NetSentron

Users' Guide

NS200

Internet Security Server
v4.0.3

NetSentron Limited Hardware Warranty

IMPORTANT – Please read carefully before using NetSentron Hardware Server.

The NetSentron Limited Hardware Warranty applies to the enclosed NetSentron hardware product. By using the Hardware Product, you agree to the terms hereof. If you do not agree to these terms, please return this package, along with proof of purchase, to the authorized dealer from whom you purchased the Hardware. THIS WARRANTY DOES NOT APPLY TO THE NETSENTRON SOFTWARE REQUIRED FOR OPERATION AND USE OF THE HARDWARE PRODUCT. PLEASE REFER TO THE ENCLOSED SFTWARE LICENCING AGREEMENT.

NOW, THEREFORE, NetSentron and you agree as follows:

1. Limited Warranty. NetSentron warrants that upon delivery and for one (1) year thereafter:

   (a.) the Hardware Product will be free from material defects in materials and workmanship, and

   (b.) the Hardware Product, when properly installed and used for its intended purpose and in its intended operating environment, will perform substantially in accordance with NetSentron applicable specifications. This warranty does not apply to any Hardware Product that has been (i) altered, repaired or modified by any party other than NetSentron or (ii) damaged or destroyed by accidents, power spikes or similar events or by any intentional, reckless or negligent acts or omissions of any party. You agree not to look to NetSentron for, and hereby release NetSentron from any liability for, performance of, enforcement of, or damage or other relief on account of, any such warranties or any breach thereof.

2. Remedies. If any Hardware Product does not comply with NetSentron warranties set forth in Section 1 above, NetSentron will, at its option, either (a) repair the Hardware Product, or (b) replace the Hardware Product; provide, that you will be responsible for returning the Hardware Product to the place of purchase and for all costs of shipping and handling. As to any Hardware Product repaired or replaced by NetSentron becomes the property of NetSentron. NetSentron shall not be responsible for return of or damage to any software, firmware, information or data contained in, stored on, or integrated with any returned Hardware Product.

3. Disclaimer and Release. The warranties, obligations and liabilities of NetSentron, and your remedies, set forth in paragraphs 1 and 2 above are exclusive and in substitution for, and you hereby waive, disclaim and release any and all other warranties, obligations and liabilities of NetSentron and all other rights, claims and remedies you may have against NetSentron, express or implied, arising by law or otherwise, with respect to any nonconformance or defect in the hardware Product (including, but not limited to, any implied warranty of merchantability or fitness for a particular purpose, any implied warranty arising from course of performance, course of dealing, or usage of trade, any warranty of non infringement, any warranty of interrupted or error-free operation, any obligation, liability, right, claim or remedy in tort, whether or not arising from the negligence (whether active,

passive or imputed) or fault of NetSentron and any obligation, liability, right, claim or remedy for loss or damage to, or caused by or contributed to by, the Hardware Product.

4. Limitation of Liability. NetSentron' liability (whether arising in contract (including warranty) tort (including active, passive or imputed negligence and strict liability and fault) or other theory) with regard to any Hardware Product will in no event exceed the purchase price paid by you for such Hardware Product. This shall be true even in the event of the failure of an agreed remedy. In no event will NetSentron be liable to you or any third party, whether arising in contract (including warranty), tort (including active, passive or imputed negligence and strict liability and fault) or other theory, for cost of cover or for any indirect, special, incidental, or consequential damages (including without limitations loss of business profits, business interruptions, or loss of business information or data) arising out of or in connection with this warranty or the use of, or inability to use the Hardware Product, even if NetSentron has been advised of the possibility of such damages. This shall be true even in the event of the failure of an agreed remedy.

5. Miscellaneous Provisions. This is the entire agreement between NetSentron and you relating to the contents of this package, and supercedes any prior purchase order, communications, advertising or representations concerning the contents of this package AND BY USING THE HARDWARE PRODUCT YOU AGREE TO THESE TERMS. No change or modification of this Agreement will be valid unless it is in writing and is signed by NetSentron.

Table of Contents

Chapter 1 Welcome

Thank you for purchasing the NetSentron NS200 – the best solution for providing network security while accessing the Internet. The NetSentron has been created in part by a group of skilled programmers, technicians and designers at Kobelt Development Inc. (KDI). Using their knowledge of security, networking and design, the team at KDI developed the NetSentron to deliver a high level of Internet security with an easy-to-use interface. Using the NetSentron will give you peace of mind when connecting to the Internet using high-speed cable or DSL modems.

The NetSentron can be used to protect an entire network, or a single computer. By default, the NetSentron is provided with two NICs: One for the LAN & the other for the WAN. Additional NICs can be purchased for Wireless & DMZ ports.

The most current information regarding the NetSentron NS200 or any other NetSentron products is available online at: http://www.netsentron.com/

Technical Support	
Telephone:	604-574-7225
Fax:	604-574-7256
Toll Free:	1-800-661-1755
Email:	support@netsentron.com

The NetSentron is supplied as a stand-alone appliance or software version. The NetSentron Software needs to be installed onto a PC with no previous operating system, as it will not install onto a PC currently running Windows.

Using This Guide

To make the text easier to read, several formatting conventions have been used throughout this guide.

Document Text

Bold	Aside from headings, **bold** text is used to highlight important text. **Bold** text is also used when asked to click on a button. Example: Click **Update**.
Italics	*Italics* are used in references. Example: *See Figure 1…*
`Courier New Font`	`Courier New Font` is used as a substitute for quotation marks because on occasion there can be some confusion as to whether or not the quotation marks are included as part of the example. Example: `Access the Internet using a proxy server.`
Bold Italics	***Bold Italics*** are used any time the user is meant to key in a stream of text. Whenever bold italics are used, the characters are meant to be keyed as shown, using the same capitalized or lower case letters as written in the instruction. Example: Type ***ABC***…

Document Symbols/Terms

⚠	Signifies precautionary advice or a warning.

NOTE	Signifies helpful information. Notes are also given in reference to additional instructions.

Default Passwords

It is important to remember the default passwords, and highly recommended to change them.

User Login	**User Password**
root	root
setup	setup
admin	admin
manager	manager

These are the default passwords and can be easily changed as explained in Chapter 4. Note: if you are purchasing the appliance, the passwords may have been changed, but a document will be shipped with the NetSentron to indicate the passwords.

Chapter 2 Installation and Configuration

Pre-installation Checklist

Before installing your NetSentron appliance, please ensure that you have the following:

□ A power cord (supplied with the NetSentron)

□ One straight through cable (supplied with the NetSentron)

□ One crossover cable (supplied with the NetSentron, required when connecting the NetSentron directly to a PC)

□ **Determine if the MAC Adapter address needs to be registered with your Internet Service Provider. If Yes, follow the instructions given by the Internet Service Provider. The MAC Adapter address is located on a white label on the back of the NetSentron, and is 12 characters long.**

□ Installed Web browser – It is recommended that you use the latest version of Firefox, Chrome, Safari or Internet Explorer. (Note: Internet Explorer is known to have some small issues with applying updates to the NetSentron).

□ A record of your TCP/IP Settings (see TCP/IP Settings)

□ Disabled the proxy in your web browser (*see Disabling Your HTTP Proxy*)

TCP/IP Settings

In order to connect to the NetSentron to administer it for the first time, you need to have your computer that is connecting to the NetSentron set up correctly. You will need an Ethernet adapter in the computer, so that you can physically connect to the NetSentron via an Ethernet cable.

Next you will need to configure the TCP/IP settings of the computer to either accept an ip address automatically (DHCP) from the NetSentron, or configure the TCP/IP settings to match those of the NetSentron.

By default, the NetSentron is configured with an ip address of 192.168.123.254 with a netmask of 255.255.255.0

So if your computer is not set to receive an ip address automatically (DHCP), you can assign your computer a static IP address in the range of 192.168.123.1 to 192.168.123.253 with a netmask of 255.255.255.0

You would set your gateway and DNS setting to be 192.168.123.254

So you should now have the settings on your computer matching those that the NetSentron requires. Next we will physically connect the computer to the NetSentron so you can administer it. You might have to disable any proxy settings that exist in your browser, the next page will tell you how to do that.

Disabling Your HTTP Proxy

To access your Administration Interface (assuming the NetSentron has been installed), you will need to disable your browser's HTTP proxy. Below are instructions on how to disable the HTTP proxy for the two most common browsers.

NOTE

If the browser you are using is not listed, click on your browser's Help menu.

Internet Explorer

Open Internet Explorer.

Click **Tools** / **Internet Options**. The Internet Options display appears.

Click the **Advanced** tab.

Scroll down the page to HTTP 1.1 Settings. Clear all check boxes.

Click **OK** to save the new settings.

Firefox

Open Firefox.
Click on **Tools**.
Click on **Options**.
Click on **Advanced** + Then **Network** Tab.
Click on **Settings**.
Select **No Proxy**.
Click **OK** to save settings.

Connecting to the NetSentron

It is recommended that you configure the NetSentron from a single computer first. Once the NetSentron has been configured, you can then add it to your network.

Configuring From a Single Computer

The following are complete step-by-step instructions on how to physically connect your NetSentron to a single computer.

1. Complete the Complete the

   located above. Once you have determined that you have what you need to install the NetSentron, continue on to step 2.

2. Unplug the network cable from your modem and then connect it to the WAN port (RED) located on the back of the NetSentron (*See Diagram 2* on the next page).

3. Plug the crossover cable that came with the NetSentron into the LAN port (GREEN) located on the back of the NetSentron.

4. Plug the other end of the crossover cable into your computer.

5. Attach the power cord to the NetSentron, and then plug it into a power outlet (*See Diagram 4* on the next page). Your NetSentron will automatically turn on. **Please allow a few minutes for the NetSentron to boot up before accessing the interface**.

> **NOTE**
>
> The first time you boot up your NetSentron it might give off an alarm-no need to panic! This occurs if you have not yet configured the external address.

6. Now that your NetSentron is connected to your computer, you will need to configure your internal and external networks before installing the NetSentron on your network.

Diagram 1

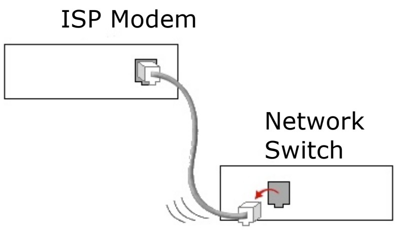


Diagram 2

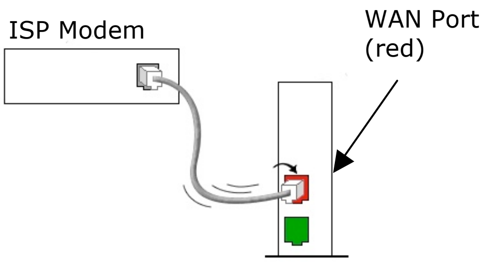


Diagram 3

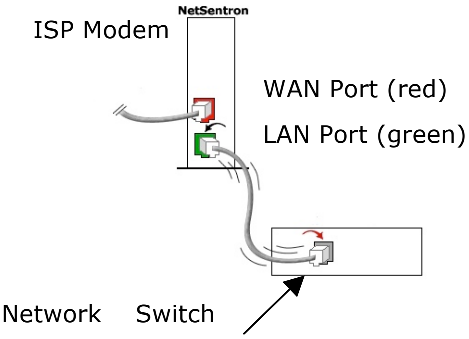
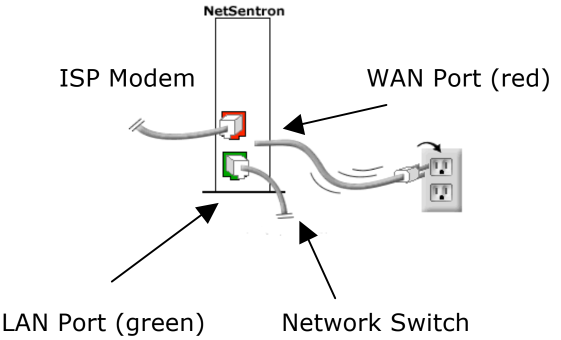


Diagram 4



Logging in to the Administration Interface

Start your browser on your computer. In the address bar, of your browser key in ***https://192.168.123.254:5445.*** The Enter Network dialog box appears.

In the User Name field key in ***admin***. In the Password field key in ***admin (r the supplied password).*** Click the **OK** button to continue. You should now be looking at the Home page of your NetSentron Administration Interface (*see Figure 3.0: Administration Interface – Home Page*).

Configuring your External Network

By configuring your external network you are giving the NetSentron the ability to communicate with your Internet Service Provider (ISP). Every networked computer around the world needs to have an IP address so that they are identifiable to other networked computers. Most ISP's assign you either a static, dynamic, or PPPoE address. When a static IP address is assigned, it will belong to your computer all the time even if you are not using it. With a dynamic IP address you are assigned a new address each time you connect to the Internet. With a PPPoE setup, you will have to provide a user name and password before your NetSentron will receive an ip address.

Determining if your Internet Service Provider (ISP) uses Dynamic or Static IP addresses or PPPoE

To allow the NetSentron to communicate with your ISP, you will need to determine whether or not you have been assigned a static or dynamic address or PPPoE. You can accomplish this by calling your ISP.

NOTE

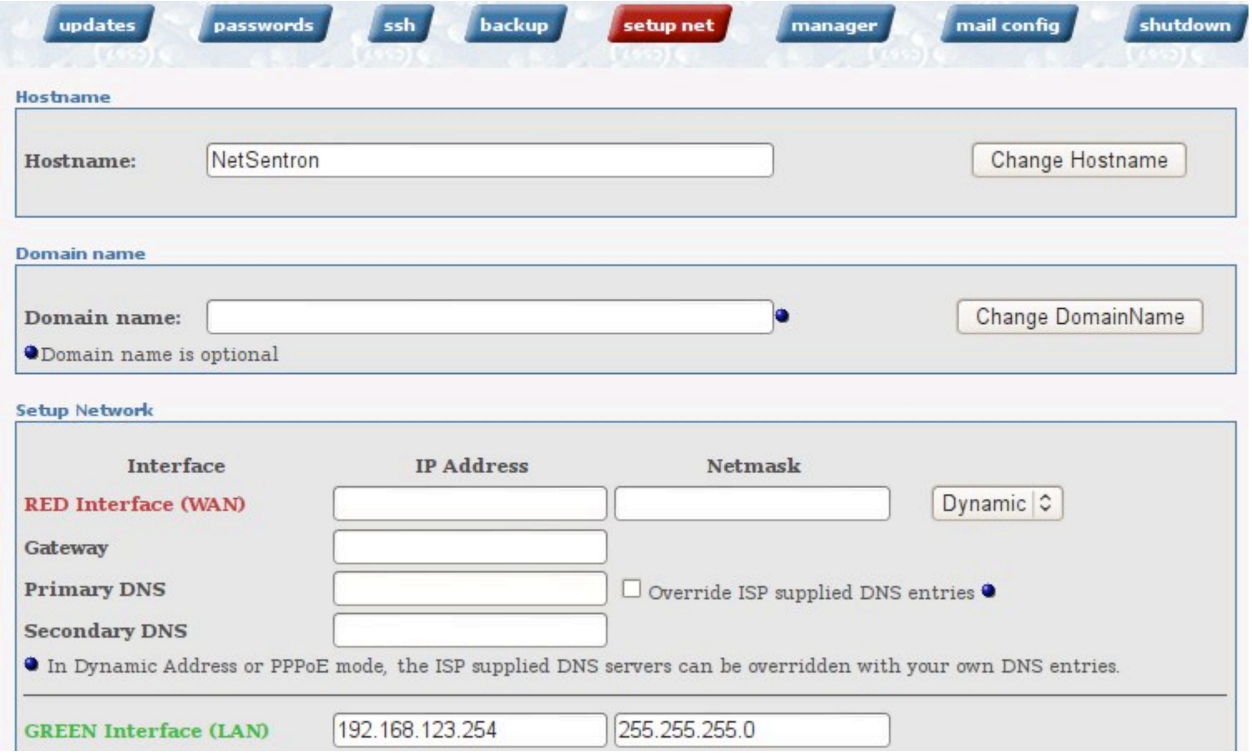
If you have a Static IP, confirm with your ISP that you are indeed receiving a true Static IP and not one that is being served through DHCP.

The next sections assume that you have logged into the NetSentron Administration GUI.

Configuring the External Network

Inside the administration guide, click on the System button. Next, click the setup net tab. You will find yourself on a screen that looks like this:

Figure2.1: Setup Net page



Hostname

Hostname: NetSentron

Domain name

Domain name: ●

● Domain name is optional

Setup Network

Interface	IP Address	Netmask	
RED Interface (WAN)			Dynamic
Gateway			
Primary DNS		□ Override ISP supplied DNS entries ●	
Secondary DNS			

● In Dynamic Address or PPPoE mode, the ISP supplied DNS servers can be overridden with your own DNS entries.

GREEN Interface (LAN)	192.168.123.254	255.255.255.0

Configuring the External Network when using a Dynamic IP

On the setup net page, choose ***Dynamic*** from the drop down list. Leave the `RED Interface (WAN)` blank, as well as the netmask.

If you wish to override the ISP supplied DNS servers, you can check the `Override ISP supplied DNS entries` and then enter a `Primary & Secondary DNS` entry.

Finally click **Update** to save the changes. The NetSentron will reset the network settings. This may take a moment or two.

Configuring the External Network when using a Static IP

On the setup net page, choose ***Static*** from the drop down list. Then enter your static IP address for the `RED Interface (WAN)` and the netmask. Then enter your gateway in the `Gateway` input field. Enter your primary and secondary DNS servers into the `Primary & Secondary DNS` input fields.

Finally click **Update** to save the changes. The NetSentron will reset the network settings. This may take a moment or two.

Configuring the External Network when using PPPoE (Point-to-Point Protocol over Ethernet)

On the setup net page, choose ***PPPoE*** from the drop down list. Next click **Update** to save the changes. The NetSentron will reset the network settings, this may take a moment or two. After the page is refreshed, there should now be a button that says **Setup PPPoE**. Click on that button to continue to configure PPPoE.
A new screen will appear that allows you to enter more settings for PPPoE, which you should have obtained from your ISP.

`Idle timeout`: The time the connection is allowed to be idle before it is reset.

`Connect on NetSentron Restart`: This should be checked for most installations.

`Connection debugging`: Leave this unchecked unless you need debugging information in the log files.

`Reconnection`: Select ***Persistent***.

`Holdoff time`: Leave at 30 seconds

`Maximum retries`: Leave at 5

`Dial on Demand for DNS`: Leave this unchecked

`Additional PPPoE Settings`: Select ***PPPoE plugin*** and leave the other input boxes empty.

`Authentication`: Enter the username that your ISP gave you.
Enter the password that your ISP gave you.
Select ***PAP or CHAP*** from the `Method` drop down list.
Leave `Script Name` blank.

`DNS`: Select ***Automatic*** unless you wish to over ride the DNS supplied by your ISP. (If you wish to enter your own DNS, select ***Manual***, then enter your DNS entries in the provided input boxes.)

Once you have everything configured, click **Save** and you will be returned to the setup net page. At this point you should click on the Home button. If everything is configured correctly, there should be Connect , Disconnect and Refresh buttons showing on the page. If you have a configuration error, you will need to go back to System -> setup net, then click on **Setup PPPoE**, make sure your settings are correct and click **Save**.

If the buttons are there, click on **Connect** and you should see the phrase Connected (0d 0h 0m ##s) – Broadband. Below that it should show an IP address. If you go back to System -> setup net, the proper IP address, gateway and DNS will now show up in the page. You can override the DNS settings in either the PPPoE setup page or the Setup net page.

If you wish to over ride the ISP supplied DNS servers, you can check the *Override ISP supplied DNS entries* and then enter a *Primary* & *Secondary DNS* entry.
If you change the DNS settings, click **Update** to save the changes. The NetSentron will reset the network settings, this may take a moment or two.

Configuring the External Network – Verifying Your Settings

After changing the external network settings, you should now reboot the NetSentron. To reboot, follow these steps:

1. From the NetSentron Interface, click the System button. Then the shutdown button and the Shutdown page appears.
2. Click the Reboot button.

Wait a few minutes for the NetSentron to restart all of its services and then log back into the administrative guide.

Verify that your NetSentron is connected to the internet by clicking on the **Home** button. You should see an IP address showing on the home page. If you have an IP address, then you can bring up a new page in your browser and try surfing the internet.
If you do not have an IP address showing, then there is probably a configuration error. Go back through your settings and double check them.

Configuring your Internal Network

Before you can use the NetSentron for the first time, you need to configure your network settings for the internal network. This requires you to gather information from your current network.

First you will need to write down the available IP address and Subnet Mask you are going to use. Use Table 2.1 New NetSentron IP Setting Reference table to record this information.

Table 2.1 New NetSentron IP Settings Reference Table

Settings	Value
Available IP Address *(Example: 192.168.123.254)*	. . .
Subnet Mask *(Example: 255.255.255.0)*	. . .

If you are configuring the NetSentron as a standalone, and not on your current network, use the crossover cable that was supplied with your hardware server. The NetSentron has DHCP Enabled and will hand out an address on the 192.168.123.xxx segment. The IP Address of the NetSentron on the Green Network Interface Controller (NIC) is 192.168.123.254. You will access the GUI on this IP.

In the address bar of your browser type in:
ht***tps://192.168.123.254:5445.*** The Enter Network dialog box appears.

In the User Name field key in ***admin***. In the Password field key in ***admin.*** Click the **OK** button to continue. You should now be looking at the Home page of your NetSentron Administration Interface (*see Figure 3.0: Administration Interface – Home Page* on page 28). Click on the

System button. Next, click the setup net tab.

Enter the `GREEN Interface (LAN)` and netmask and click **Update** to save the changes. The NetSentron will reset the network settings, this may take a moment or two. You will need to release and renew (or manually change) the IP address on the computer you are using to administer the NetSentron.

Installing to your Network

Once you have configured your internal and external networks, you can remove the NetSentron from the standalone computer and then install it onto your network. Follow the steps below.

1. Remove the one end of the crossover cable from the LAN port (GREEN) located on the back of the NetSentron and then remove the other end of the crossover cable from the computer. Put the crossover cable aside. (You will no longer need the crossover cable. It is only required when configuring from a single computer)
2. Unplug the cable on your hub/switch that goes to the cable/DSL modem (*See Diagram 5, on the next page)* and then connect it to the WAN port (RED) located on the back of the NetSentron (*See Diagram 6 on the next page)*.
3. Plug one end of the network cable that came with the NetSentron into the LAN port (GREEN) located on the back of the NetSentron.
4. Plug the other end of the cable into your hub/switch where you removed the first cable, during step 2 (*See Diagram 7* on the next page)
5. You are now ready to access the Administration interface. You will need to restart the NetSentron before you can access the GUI.

Diagram 6

ISP Modem

WAN Port
(red)

Diagram 5

ISP Modem

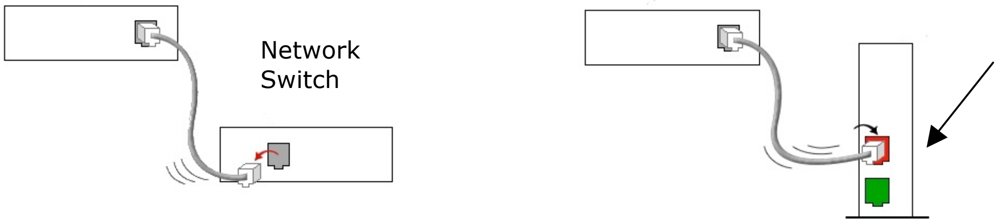
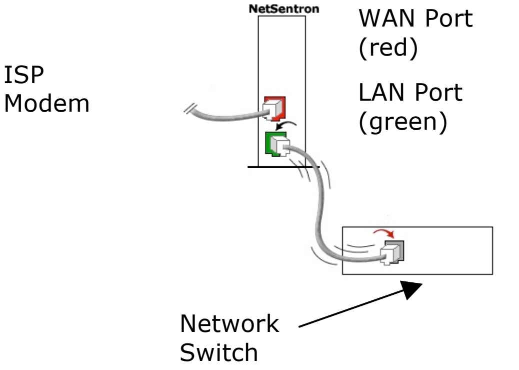


Diagram 7



NOTE

Once you have accessed the Interface, it is highly recommended that you change the default passwords. See the section on Passwords on page 30.

Chapter 3 Administration Interface

The Administration Interface gives you the ability to display, add and edit preferences and settings for your NetSentron Internet Security Server. Most of your daily administration can be accessed from the pages on this interface.

The GUI Interface Layout has been designed for easy usage. Clicking on the buttons located at the top of the page brings up different Administration pages. Each Administration Page has sub-sections, which can be accessed by clicking on the buttons below each main button. The windows that appear are the active windows, which display the currently selected information for viewing and editing. The button associated with the active window will be displayed in red. Once you are familiar with the look and the navigation of the GUI interface, you can start administering your NetSentron configurations and settings.

NOTE

Please make sure the browser you are using has Java Script Enabled.

Accessing the Administration Interface

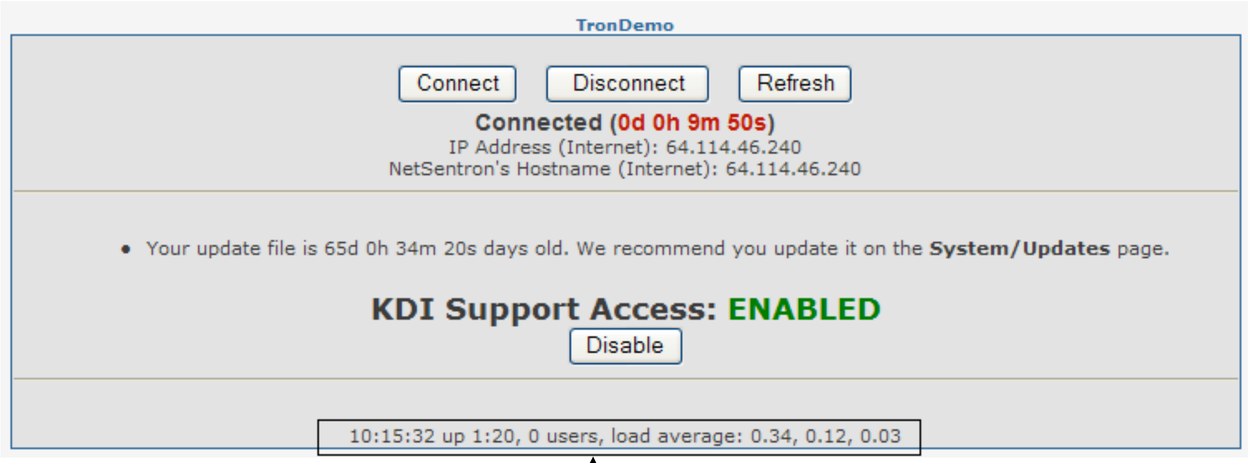
1. Open up a browser on a computer connected to the NetSentron. In the address bar:

   Key in ***https://192.168.123.254:5445*** (default) or the green IP that you previously entered. The Enter Network Dialog box appears.

2. If you are accessing the Interface for the first time, type **admin** in the User Name and Password fields. If you have already changed the default password, type in the new password in the Password field.

3. Click the **OK** button to continue. You should now be looking at the Home page of your NetSentron Administration Interface which *Figure 3.0: Administration Interface – Home Page* shows below.

Figure 3.0: Administration Interface – Home Page



Connected (0d 0h 9m 50s)
IP Address (Internet): 64.114.46.240
NetSentron's Hostname (Internet): 64.114.46.240

- Your update file is 65d 0h 34m 20s days old. We recommend you update it on the **System/Updates** page.

KDI Support Access: ENABLED

10:15:32 up 1:20, 0 users, load average: 0.34, 0.12, 0.03

Connection Status Line

Home

Once you have logged onto your NetSentron, you are automatically defaulted to the Home page of the NetSentron Administration Interface.

From here you can explore various options by clicking on the buttons located at the top of the page. You should also see a Refresh button. This button will refresh the information on the main screen.

In addition to the buttons you should also see a connection status line. (*See Figure 3.0: Administration Interface – Home Page*, on the previous page). This line is the output that displays the current time, the days/hours/minutes that your NetSentron has been running without a reboot, number of users logged in to your NetSentron, and the load average on your NetSentron Security Server.

Lastly, if there are updates available for the NetSentron that have not yet been installed, you will be informed on this page.

NOTE

Once you have accessed the Interface, it is highly recommended that you change the default passwords.

See the section on passwords in the next chapter.

Chapter 4 Administration

Once you are familiar with the look and the navigation of the Administration Interface, you can administer your NetSentron. In this chapter you will learn how to display, review and modify different settings on your NetSentron Security Server.

Passwords

Passwords are the first line of defense when using any Security Server. This section of this Users' Guide shows the administrator how to change the NetSentron passwords. This is especially important when accessing the NetSentron for the first time, as all the passwords are default passwords.

The admin, setup and manage passwords can be changed on the passwords page. Your NetSentron comes with a root password that is used for command line access to the box. This password cannot be changed through the administrative gui, it requires logging into the NetSentron using an SSH (Secure Shell) client such as putty. You can download the ssh client from the NetSentron by going to the Info -> ip utils page. The root password is usually set at the factory and is put onto a printed sheet that comes with the NetSentron.

Changing the root password

The only way to change the root password is to log in via the console with root and the existing root password. You can do this by connecting a keyboard and monitor to the NetSentron, or using the putty client that is supplied with the NetSentron. To use the putty client, double click putty.exe (the .exe file can be found in the Info > iputils section of the Administration Interface) and then enter the GREEN IP address of your NetSentron and choose port 222 for the port. You should then be asked to enter a username and password. The username is root.

Once logged in, type setup, the setup program will start.

Next cursor down to passwords and hit enter.

Hit enter again to change the root password. You can also change any of the other passwords from this program too.

NOTE

A password must be at least 8 characters long.

Once you have changed the passwords, exit the setup program, select Go Back by using the right cursor key. Then choose Exit by using the cursor keys to navigate to the button and pressing Enter.

Take steps to ensure that you do not lose the root password. Once the root password has been changed there is no way of retrieving it.

Changing Admin/Manager and Setup User Passwords

The Passwords page allows you to make changes to the Admin, Manager and Setup passwords. The Admin has full access to the GUI whereas the Manager may be allowed to manage the NetSentron, but with limited access. The access is limited by the selections on the Manager page (*see Selecting Manager Settings).* When changing the admin and setup passwords you have two options. The first option is to make the changes thru accessing SSH and then following the same instructions used when changing the root password. The second option, and much simpler option, is to use the `Passwords Administration` page. The following are instructions on changing your admin, manager and setup passwords using the GUI Administration page.

NOTE

When a setup user logs in, the setup program will run automatically, allowing the user to reconfigure the NetSentron Server. Take steps to ensure that you do not lose the setup password. Once the default password has been changed there is no way of retrieving it without a KDI Technician or you NetSentron Partner.

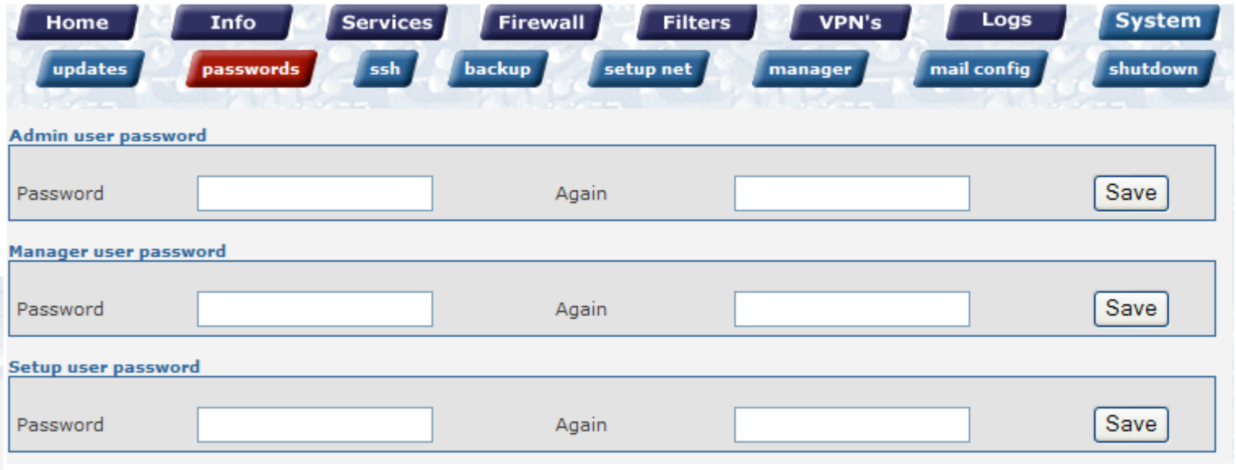
1. From the Administration Interface, click on the System button. New sets of buttons appear.

2. Click on the passwords button. The Passwords Administration Page appears (*see Figure 4.2 below*). From this page you have the option to change the password for the Admin user and the Manager users' passwords.

3. Select which user you want to change the password for and then in the Password field, key in your new password. In the Again field re-enter the new password.

4. Click the Save button to confirm the changes.

Figure 4.2: Passwords Administration Page



Admin user password

Password Again Save

Manager user password

Password Again Save

Setup user password

Password Again Save

Settings

This section of the Users' guide gives instructions on how to personalize and configure the NetSentron for your specific needs. For example you can give your NetSentron a hostname, which would appear on the top right-hand side of each page of the Administration Interface.

Assigning a Host Name to the NetSentron

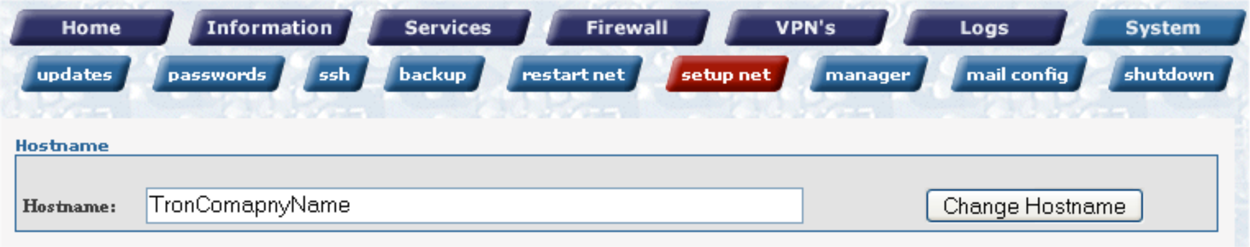
Adding a Host Name to your NetSentron is a way to personalize each NetSentron Security Server. This also allows you to distinguish between two or more NetSentrons.

1. From the Administration Interface, click on the System button. New sets of buttons appear.
2. Next, click the setup net button. The Network Settings display appears.

   Using the Hostname panel, key a name into the Hostname field.

   *(*i.e*. TronCompanyName*).

Figure 4.3: Network Settings Page – Hostname Panel



Hostname

Hostname: TronComapnyName

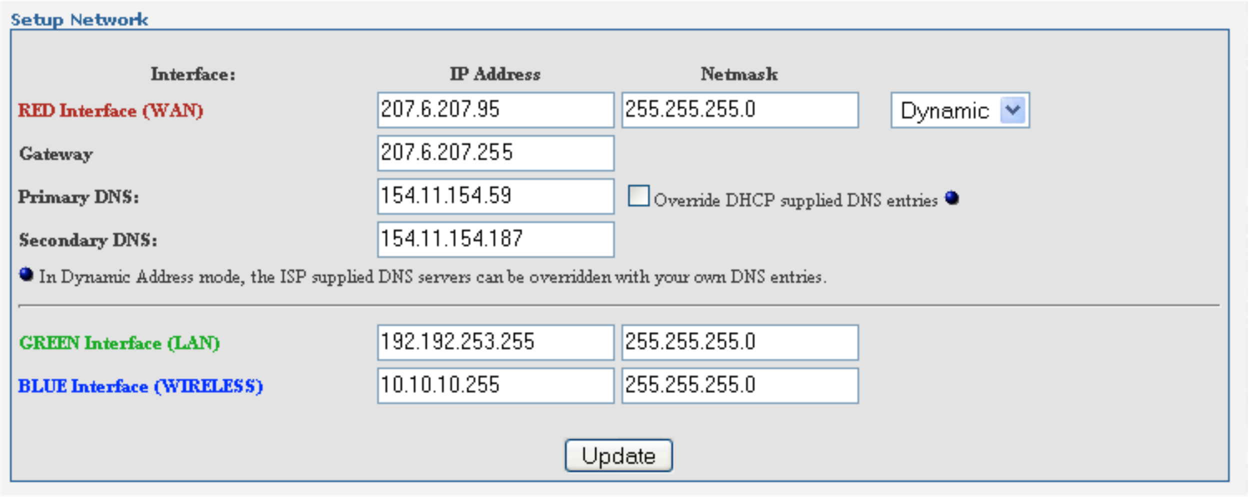
3. Click on the Change Hostname button to save the change.

Network Settings

This section of the users' guide shows you how to bring up the Network Settings display. Use this display to manage your network settings.

1. From the Administration Interface, click on the System button. New sets of buttons appear.
2. *2.* Next, click the setup net button**.** The Network Settings display appears. *See Figure 4.4: Network Settings Page* below.

Figure 4.4: Network Settings Page – Setup Network Panel



Setup Network

Interface:	IP Address	Netmask	
RED Interface (WAN)	207.6.207.95	255.255.255.0	Dynamic
Gateway	207.6.207.255		
Primary DNS:	154.11.154.59	□ Override DHCP supplied DNS entries ●	
Secondary DNS:	154.11.154.187		

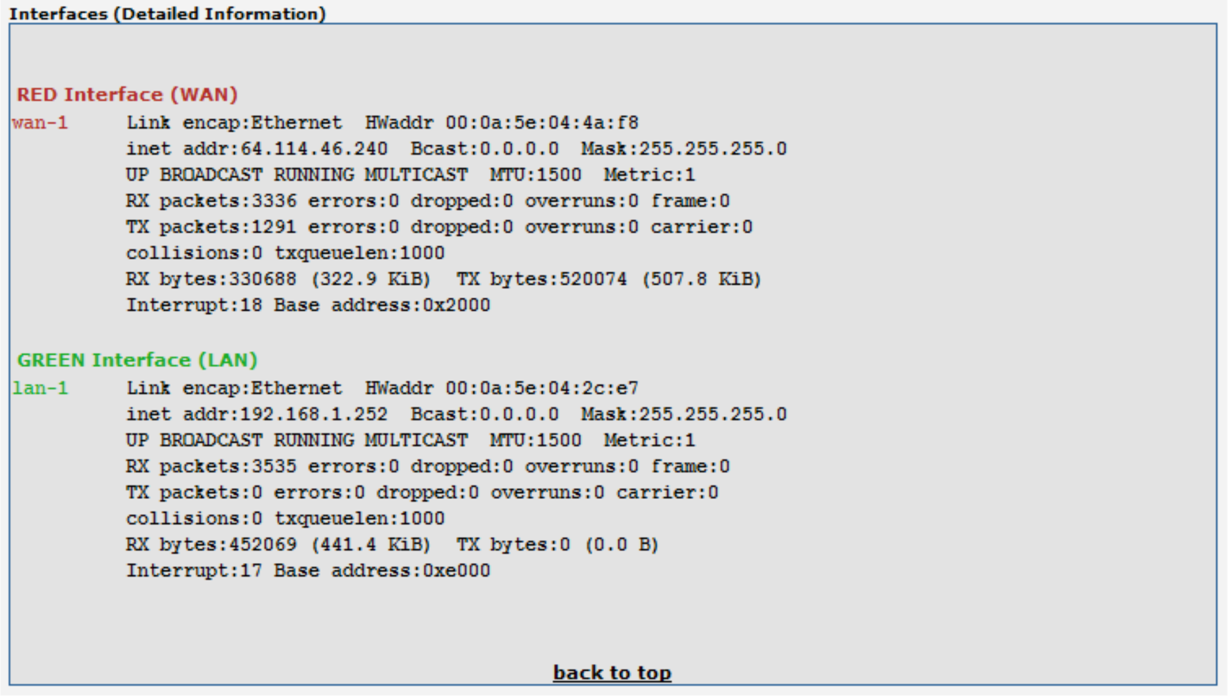
● In Dynamic Address mode, the ISP supplied DNS servers can be overridden with your own DNS entries.

Interface:	IP Address	Netmask
GREEN Interface (LAN)	192.192.253.255	255.255.255.0
BLUE Interface (WIRELESS)	10.10.10.255	255.255.255.0

*Wireless (Blue) and DMZ (Orange) Interfaces are sold as additional options.

3. Make the appropriate changes and then click on the Update button to confirm the changes.
4. You can view the details of the interface in the Interface: (Detailed Information) panel below the Setup Network panel. *See Figure 4.5: Network Settings Page,* on the next page.

Figure 4.5: Network Settings Page – Interfaces: (Detailed Information) Panel



Interfaces (Detailed Information)

RED Interface (WAN)

```
wan-1     Link encap:Ethernet  HWaddr 00:0a:5e:04:4a:f8
          inet addr:64.114.46.240  Bcast:0.0.0.0  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3336 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1291 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:330688 (322.9 KiB)  TX bytes:520074 (507.8 KiB)
          Interrupt:18 Base address:0x2000
```

GREEN Interface (LAN)

```
lan-1     Link encap:Ethernet  HWaddr 00:0a:5e:04:2c:e7
          inet addr:192.168.1.252  Bcast:0.0.0.0  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3535 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:452069 (441.4 KiB)  TX bytes:0 (0.0 B)
          Interrupt:17 Base address:0xe000
```

Information

The Info set of pages, allows the administrator to view detailed information on the status of the various sections on your NetSentron. By default, when you click on the Info button you will be given the current status of each system on your NetSentron. By clicking on the remaining buttons you can view the system graphs, network status, traffic graphs, connections, IP utilities, bandwidth monitoring, connection analysis and iptables.

Checking the Current Status of your NetSentron

The System Status Page of the NetSentron interface displays a list with information regarding the current status of the NetSentron's services. The System Status page also allows the user to view the memory, disk usage, disk log usage, uptime and users, interfaces, loaded modules, and kernel version.

From the Administration Interface, click on the Info button. By default you are on the Status Page of the NetSentron Interface. This page has been divided into separate panels. You can use the scroll bar on the side of the screen to scroll down to each panel or you can use the quick links located at the top of the page.

The following is a list of what each panel represents:

Services

Displays the current services that are active on the NetSentron. If the green light is on the service is turned on. If the red light is on the server is NOT turned on or the service is not running*. See*

Figure 4.6: Services Status on page 38.

Memory

Displays how much RAM is being used by the NetSentron Operating system. It should always be Green or Yellow: if it is Red contact a KDI Technician or your NetSentron Partner immediately. *See*

Figure 4.7: Memory status*,* on page 38.

Disk usage

Displays the Size, Used and Available amount of Hardware space on the NetSentron Security Server. If any of these bar graphs are Red call a KDI Technician or your NetSentron partner. *See*

Figure 4.8: Disk Usage*,* on page 39.

Inodes Usage

When a file is opened, the file's inode is read by the kernel. The more files/folders which are opened, the more inodes it uses. The more inodes it uses the more system resources it consumes.

Uptime and Users

Displays the Uptime details of any current user logged on to the NetSentron. *See*

Figure 4.10: Uptime And Users, on page 39. This is the same uptime as the Home page. `User` represents a user logged in through SSH (in this case there is no user shown). Log in through SSH in one browser, and then view this in a second browser to see*.*

Hardware Information

This panel displays the hardware information in the NetSentron such as processor, memory amount, hard drive size, network cards and processor speed. *See*

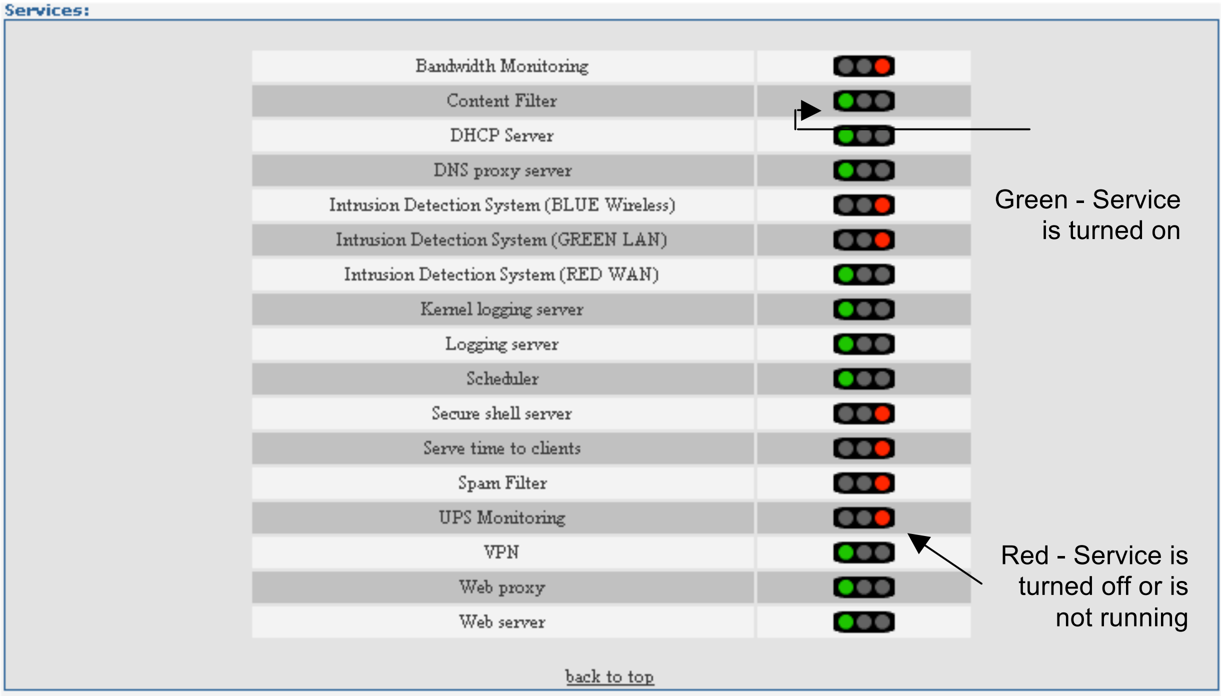
Figure 4.11: Hardware Information, on page 39.

Kernel Version

This panel displays the actual kernel information. *See*

Figure 4.12: Kernel Version*,* on page 40.

Figure 4.6: Services Status



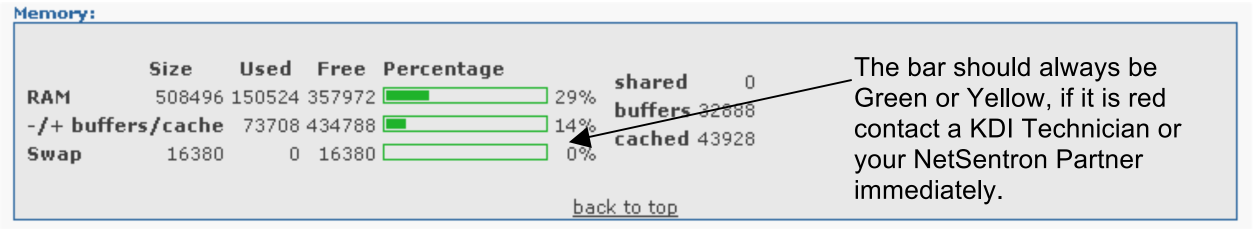
Services:

Bandwidth Monitoring	🟥
Content Filter	🟩
DHCP Server	🟩
DNS proxy server	🟩
Intrusion Detection System (BLUE Wireless)	🟥
Intrusion Detection System (GREEN LAN)	🟥
Intrusion Detection System (RED WAN)	🟩
Kernel logging server	🟩
Logging server	🟩
Scheduler	🟩
Secure shell server	🟥
Serve time to clients	🟥
Spam Filter	🟥
UPS Monitoring	🟥
VPN	🟩
Web proxy	🟩
Web server	🟩

Green - Service is turned on

Red - Service is turned off or is not running

Figure 4.7: Memory status

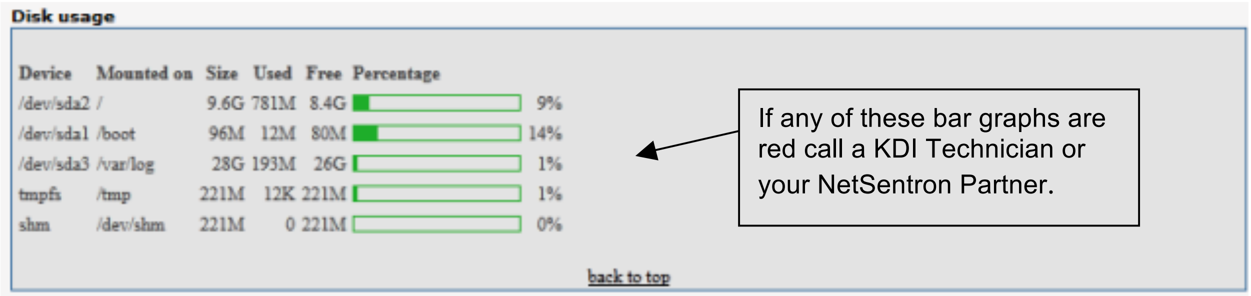


Memory:

```
                     Size   Used   Free  Percentage
RAM                508496 150524 357972  29%    shared      0
-/+ buffers/cache         73708 434788  14%    buffers 32888
Swap                16380      0  16380   0%    cached  43928
```

The bar should always be Green or Yellow, if it is red contact a KDI Technician or your NetSentron Partner immediately.

Figure 4.8: Disk Usage

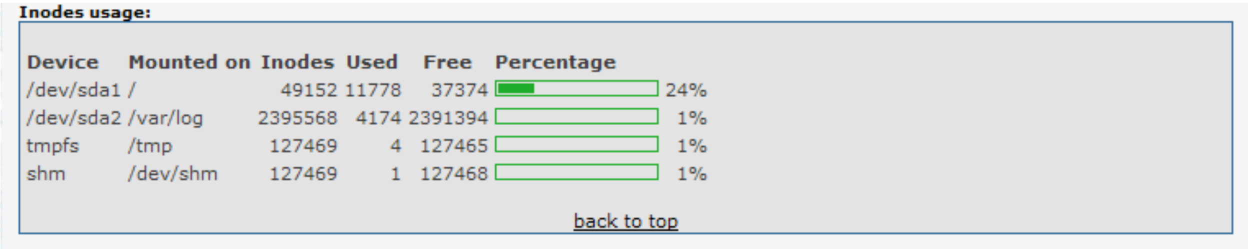


Disk usage

Device	Mounted on	Size	Used	Free	Percentage	
/dev/sda2	/	9.6G	781M	8.4G		9%
/dev/sda1	/boot	96M	12M	80M		14%
/dev/sda3	/var/log	28G	193M	26G		1%
tmpfs	/tmp	221M	12K	221M		1%
shm	/dev/shm	221M	0	221M		0%

If any of these bar graphs are red call a KDI Technician or your NetSentron Partner.

Figure 4.9: Inodes Usage

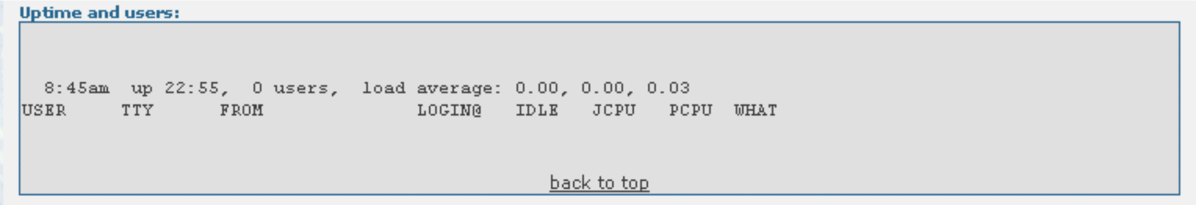


Inodes usage:

Device	Mounted on	Inodes	Used	Free	Percentage
/dev/sda1	/	49152	11778	37374	24%
/dev/sda2	/var/log	2395568	4174	2391394	1%
tmpfs	/tmp	127469	4	127465	1%
shm	/dev/shm	127469	1	127468	1%

back to top

Figure 4.10: Uptime And Users

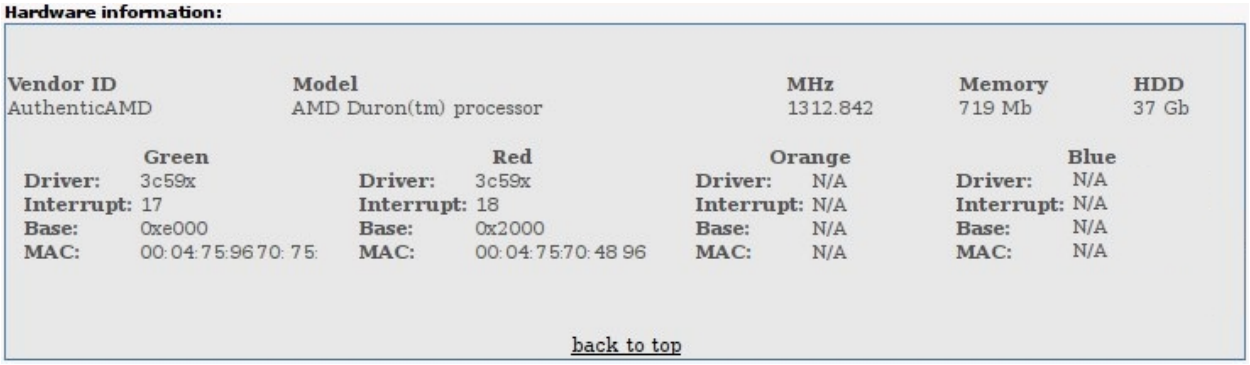


Uptime and users:

```
  8:45am  up 22:55,  0 users,  load average: 0.00, 0.00, 0.03
USER     TTY      FROM              LOGIN@   IDLE   JCPU   PCPU  WHAT
```

back to top

Figure 4.11: Hardware Information



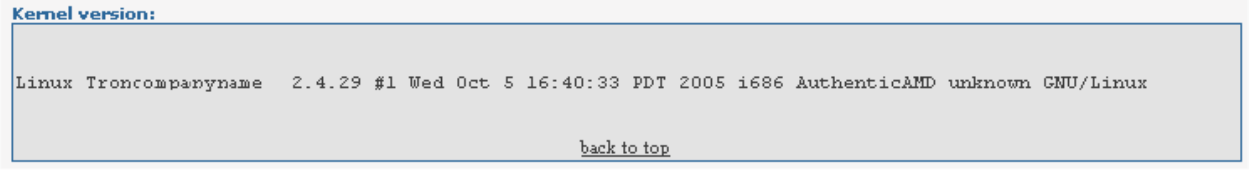
Hardware information:

Vendor ID	Model	MHz	Memory	HDD
AuthenticAMD	AMD Duron(tm) processor	1312.842	719 Mb	37 Gb

	Green		Red		Orange		Blue
Driver:	3c59x	**Driver:**	3c59x	**Driver:**	N/A	**Driver:**	N/A
Interrupt:	17	**Interrupt:**	18	**Interrupt:**	N/A	**Interrupt:**	N/A
Base:	0xe000	**Base:**	0x2000	**Base:**	N/A	**Base:**	N/A
MAC:	00:04:75:96 70: 75:	**MAC:**	00:04:75:70:48 96	**MAC:**	N/A	**MAC:**	N/A

back to top

Figure 4.12: Kernel Version



Kernel version:

```
Linux Troncompanyname  2.4.29 #1 Wed Oct 5 16:40:33 PDT 2005 i686 AuthenticAMD unknown GNU/Linux
```

back to top

Displaying System Graphs

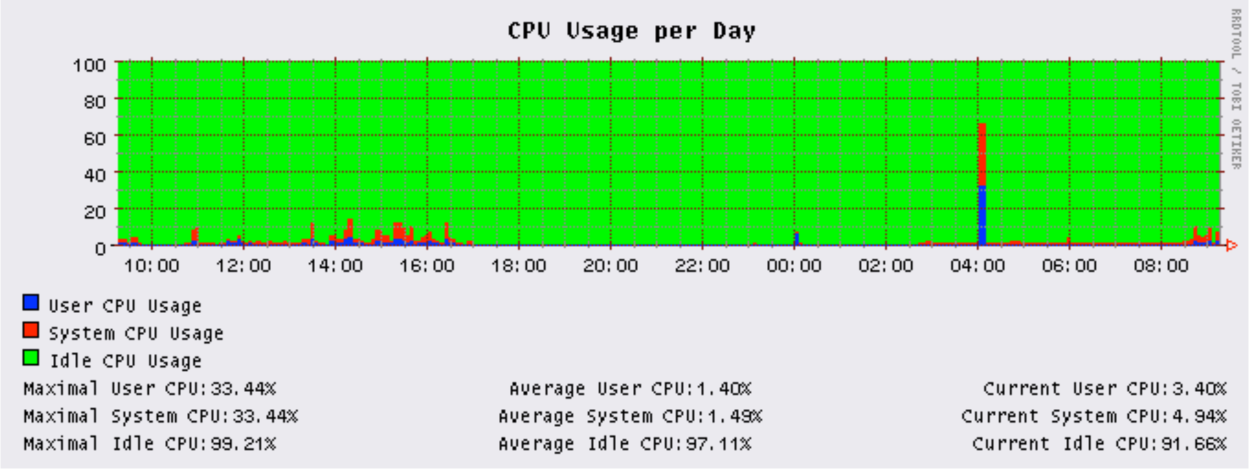
The System Graphs page on the NetSentron interface allows you to view the graphical details for CPU, Memory, Swap and Disk usage. Each system is displayed in its own graphical panel with a color-coded legend. Each graph is also date and time stamped. To view the most current time, click on the refresh button on your browser. From the Administration Interface, click on the Info button. New sets of buttons appear.

Click on the system graphs button. The System Graphs Page is displayed. You can use the scroll bar on the side of the screen to scroll down to each panel. Clicking on any of the graphs will bring up a new page for the graph in question and display the daily, weekly, monthly and yearly graphs.

The following is a list of what each panel represents, starting from top to bottom:

CPU	Displays the daily CPU usage at the time that you entered the System Graphs page*. See Figure 4.13*on page 41.
Memory	Displays the daily Memory usage at the time that you entered the System Graphs page. *See Figure 4.14* on the next page.
Disk Usage	Displays the daily Swap usage at the time that you entered the System Graphs page. *See Figure 4.15* on page 42.
Disk Access	Displays the daily disk usage at the time that you entered the System Graphs page. *See Figure 4.16* on page 42.

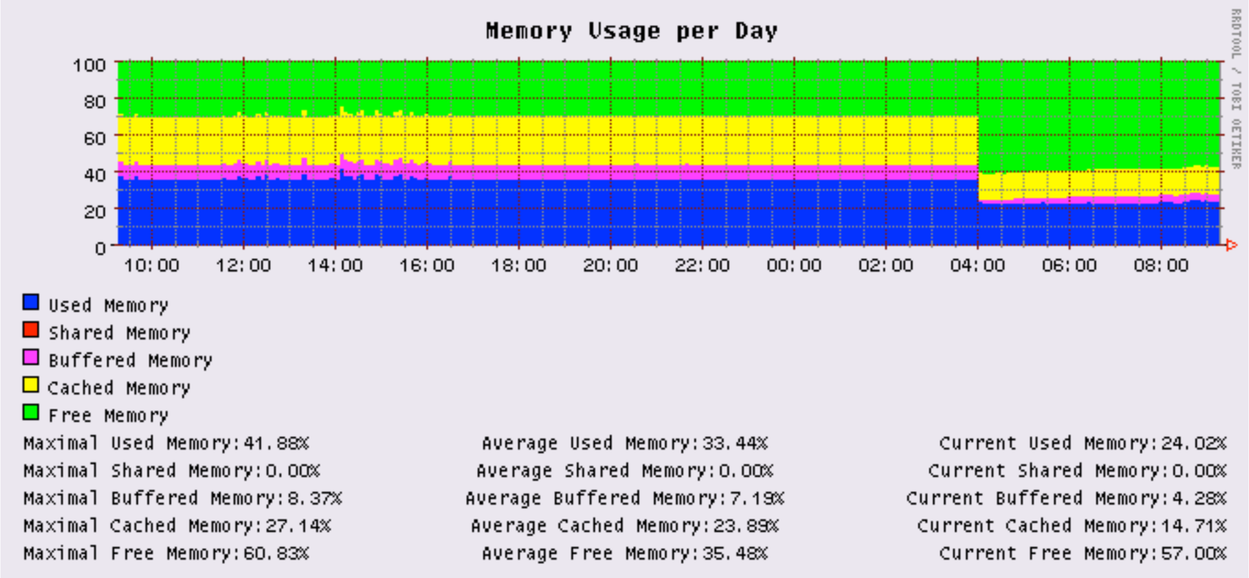
Figure 4.13: System Graphs: CPU



🟦 User CPU Usage
🟥 System CPU Usage
🟩 Idle CPU Usage

```
Maximal User CPU:33.44%        Average User CPU:1.40%       Current User CPU:3.40%
Maximal System CPU:33.44%      Average System CPU:1.49%     Current System CPU:4.94%
Maximal Idle CPU:99.21%        Average Idle CPU:97.11%      Current Idle CPU:91.66%
```

Figure 4.14: System Graphs: Memory



🟦 Used Memory
🟥 Shared Memory
🟪 Buffered Memory
🟨 Cached Memory
🟩 Free Memory

```
Maximal Used Memory:41.88%       Average Used Memory:33.44%       Current Used Memory:24.02%
Maximal Shared Memory:0.00%      Average Shared Memory:0.00%      Current Shared Memory:0.00%
Maximal Buffered Memory:8.37%    Average Buffered Memory:7.19%    Current Buffered Memory:4.28%
Maximal Cached Memory:27.14%     Average Cached Memory:23.89%     Current Cached Memory:14.71%
Maximal Free Memory:60.83%       Average Free Memory:35.48%       Current Free Memory:57.00%
```

Figure 4.15: System Graphs: Disk Usage

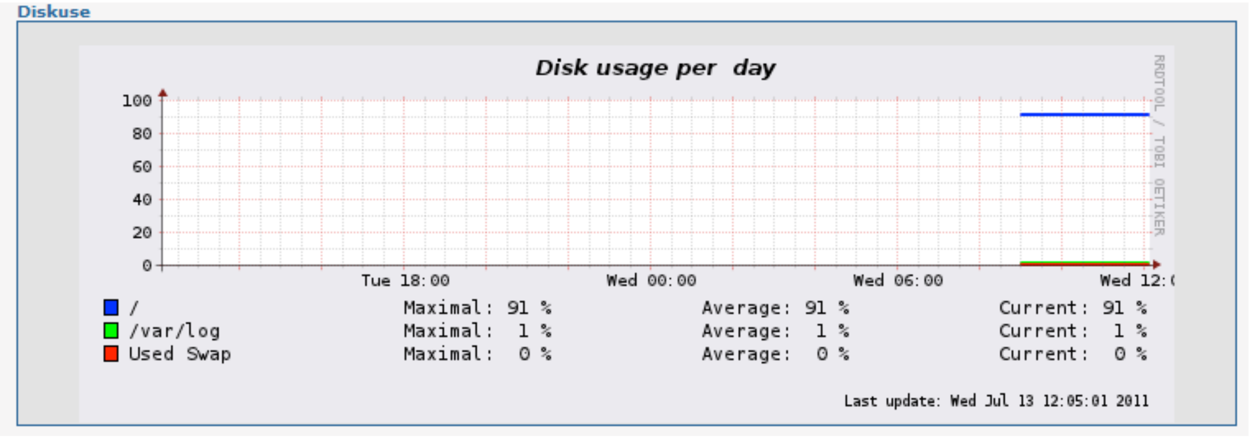
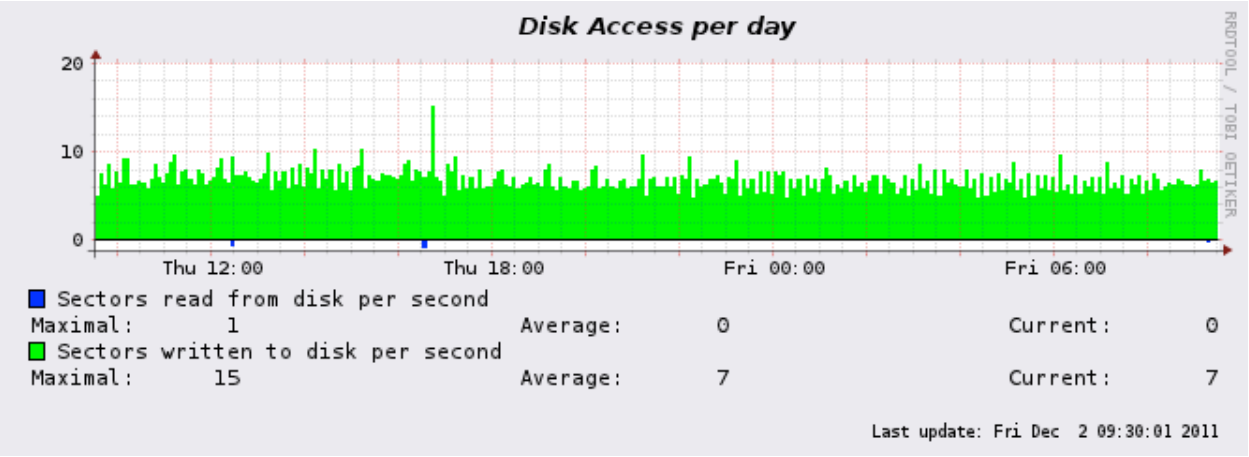


Figure 4.16: System Graphs: Disk Access



Displaying Network Status

The Network Status page on the NetSentron interface allows you to view the stats of all networks installed on the NetSentron.

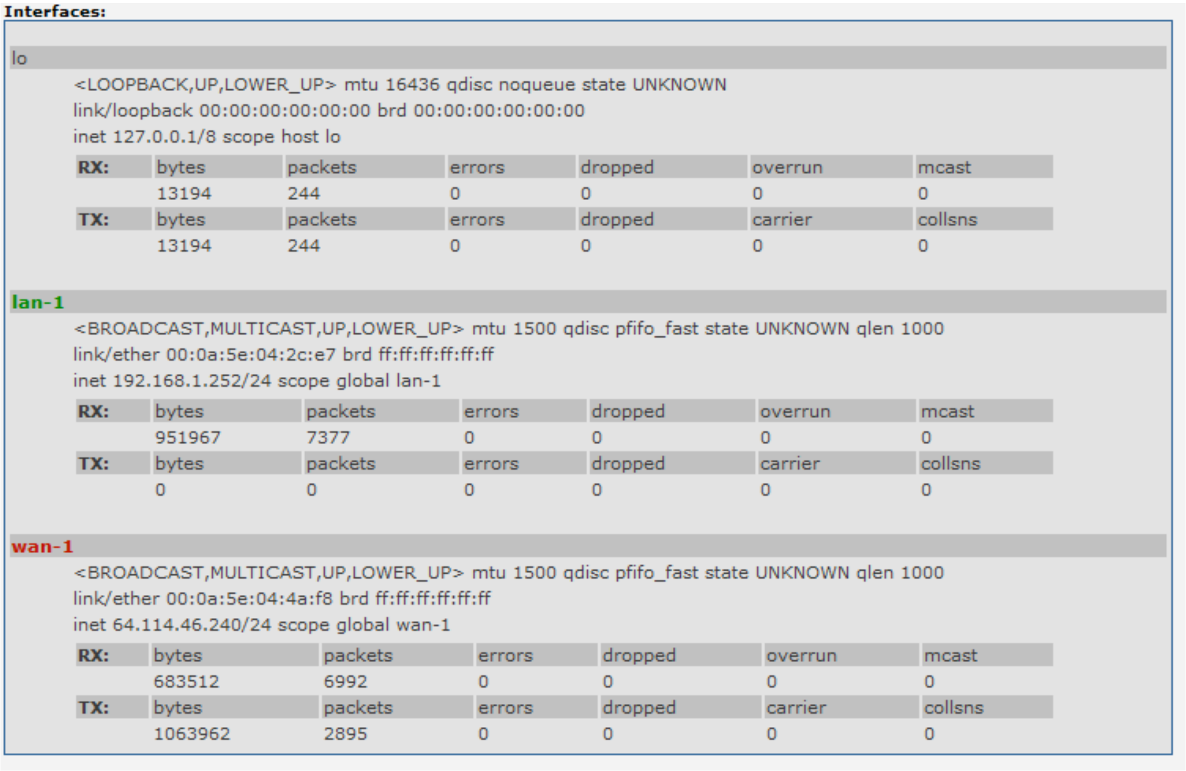
1. From the Administration Interface, click on the Info button. New sets of buttons appear.

2. Click on the network status button. The Network Status Page is displayed. This page has been divided into separate panels. You can use the scroll bar on the side of the screen to scroll down to each panel or you can use the quick links located at the top of the page.

The following is a list of what each panel represents, starting from top to bottom:

Interfaces	This panel will inform you of the IP address of each network card, the packets sent and received and also of any errors that are occurring on the network cards. *See Figure 4.17 on the next page.*
RED DHCP configuration	This panel displays the current configuration of your RED DHCP settings. *See Figure 4.18 on the next page.*
Routing Table Entries	This panel displays the routing of packets for your network. *See Figure 4.19 on the next page.*
ARP Table Entries	This panel displays the Internet protocol used to dynamically map an Internet address to a physical (hardware) address on a local area network. This is limited to networks that support hardware broadcasting. *See Figure 4.20 on the next page.*

Figure 4.17: Network Status: Interfaces



Interfaces:

lo

<LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue state UNKNOWN
link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
inet 127.0.0.1/8 scope host lo

RX:	bytes	packets	errors	dropped	overrun	mcast
	13194	244	0	0	0	0
TX:	bytes	packets	errors	dropped	carrier	collsns
	13194	244	0	0	0	0

lan-1

<BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 1000
link/ether 00:0a:5e:04:2c:e7 brd ff:ff:ff:ff:ff:ff
inet 192.168.1.252/24 scope global lan-1

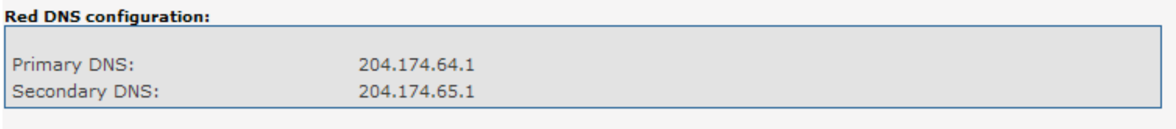
RX:	bytes	packets	errors	dropped	overrun	mcast
	951967	7377	0	0	0	0
TX:	bytes	packets	errors	dropped	carrier	collsns
	0	0	0	0	0	0

wan-1

<BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UNKNOWN qlen 1000
link/ether 00:0a:5e:04:4a:f8 brd ff:ff:ff:ff:ff:ff
inet 64.114.46.240/24 scope global wan-1

RX:	bytes	packets	errors	dropped	overrun	mcast
	683512	6992	0	0	0	0
TX:	bytes	packets	errors	dropped	carrier	collsns
	1063962	2895	0	0	0	0

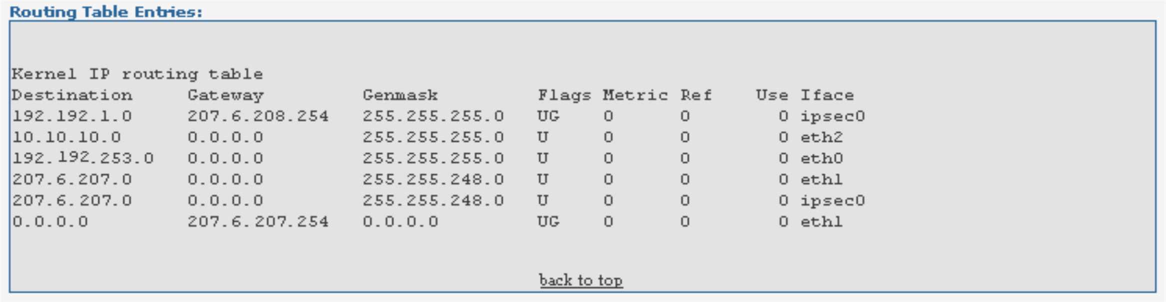
Figure 4.18: Network Status: RED DNS configuration



Red DNS configuration:

Primary DNS:	204.174.64.1
Secondary DNS:	204.174.65.1

Figure 4.19: Network Status: Routing Table Entries

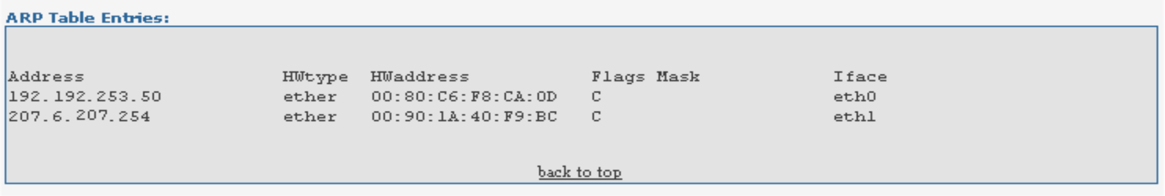


Routing Table Entries:

```
Kernel IP routing table
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.192.1.0     207.6.208.254   255.255.255.0   UG    0      0        0 ipsec0
10.10.10.0      0.0.0.0         255.255.255.0   U     0      0        0 eth2
192.192.253.0   0.0.0.0         255.255.255.0   U     0      0        0 eth0
207.6.207.0     0.0.0.0         255.255.248.0   U     0      0        0 eth1
207.6.207.0     0.0.0.0         255.255.248.0   U     0      0        0 ipsec0
0.0.0.0         207.6.207.254   0.0.0.0         UG    0      0        0 eth1
```

back to top

Figure 4.20: Network Status: ARP Table Entries



ARP Table Entries:

```
Address                  HWtype  HWaddress           Flags Mask            Iface
192.192.253.50           ether   00:80:C6:F8:CA:0D   C                     eth0
207.6.207.254            ether   00:90:1A:40:F9:BC   C                     eth1
```

back to top

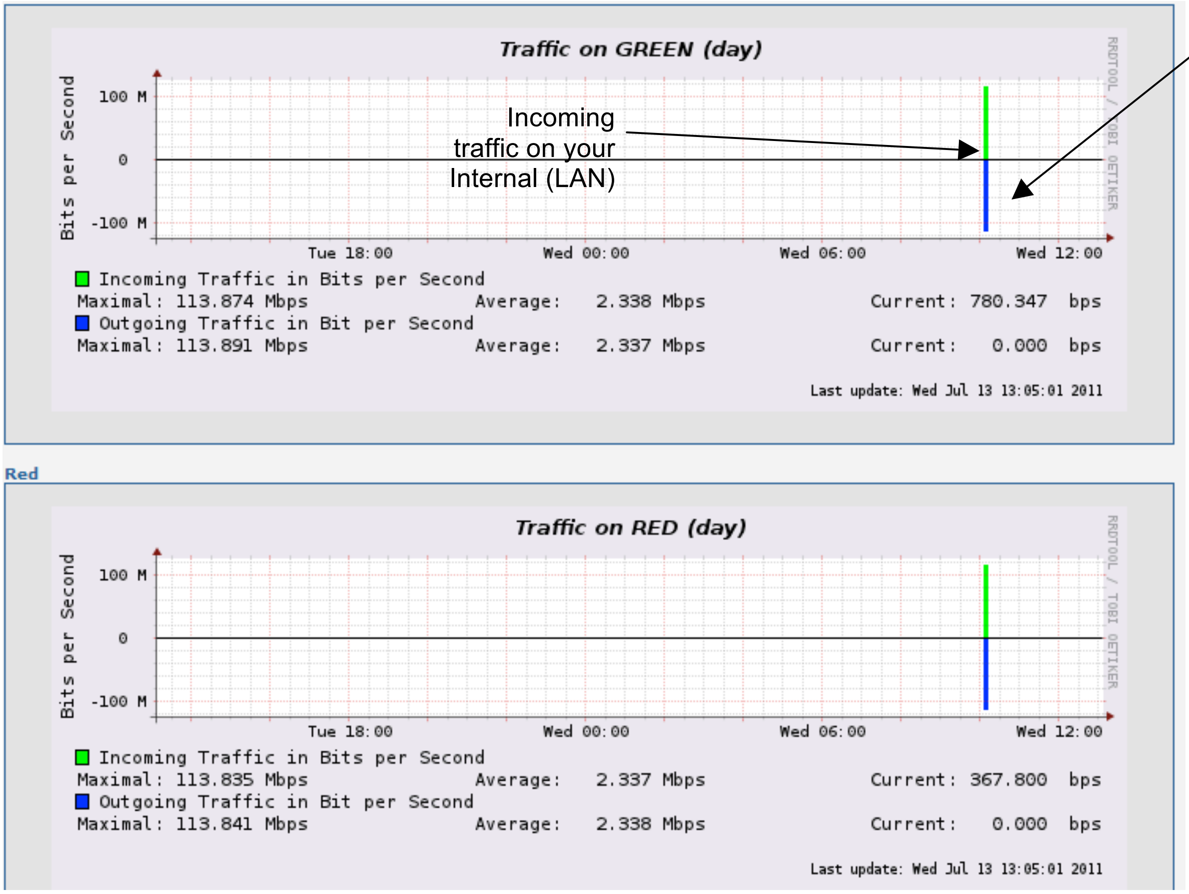
Displaying Traffic Graphs

The Traffic Graphs page on the NetSentron interface allows you to view graphical information regarding the amount of traffic that has passed through your NetSentron Security Server in the past 24 hours. All traffic including FTP is displayed on this page.

1. From the Administration Interface, click on the **Info** button. New sets of buttons appear.
2. Click on the **traffic graphs** button. The Traffic Graphs Page is displayed. There are two separate graphs one for Internal Traffic (green) and External Traffic (red). The graphs are displayed in color. The green lines represent the incoming traffic and the blue lines represent the outgoing traffic. *See Figure 4.21,* below. Additional network cards may be purchased for wireless (blue, pictured), and DMZ (orange).
3. To view the Daily, Weekly, Monthly and Yearly stats for all three graphs, simply click on the individual graph.

Figure 4.21: Traffic Graphs Page

Outgoing traffic on your Internal (LAN)



```
🟩 Incoming Traffic in Bits per Second
Maximal: 113.874 Mbps            Average:   2.338 Mbps           Current: 780.347  bps
🟦 Outgoing Traffic in Bit per Second
Maximal: 113.891 Mbps            Average:   2.337 Mbps           Current:   0.000  bps

                                                          Last update: Wed Jul 13 13:05:01 2011
```

```
🟩 Incoming Traffic in Bits per Second
Maximal: 113.835 Mbps            Average:   2.337 Mbps           Current: 367.800  bps
🟦 Outgoing Traffic in Bit per Second
Maximal: 113.841 Mbps            Average:   2.338 Mbps           Current:   0.000  bps

                                                          Last update: Wed Jul 13 13:05:01 2011
```

Click on the graphs themselves to view daily, weekly, monthly and yearly graphs.

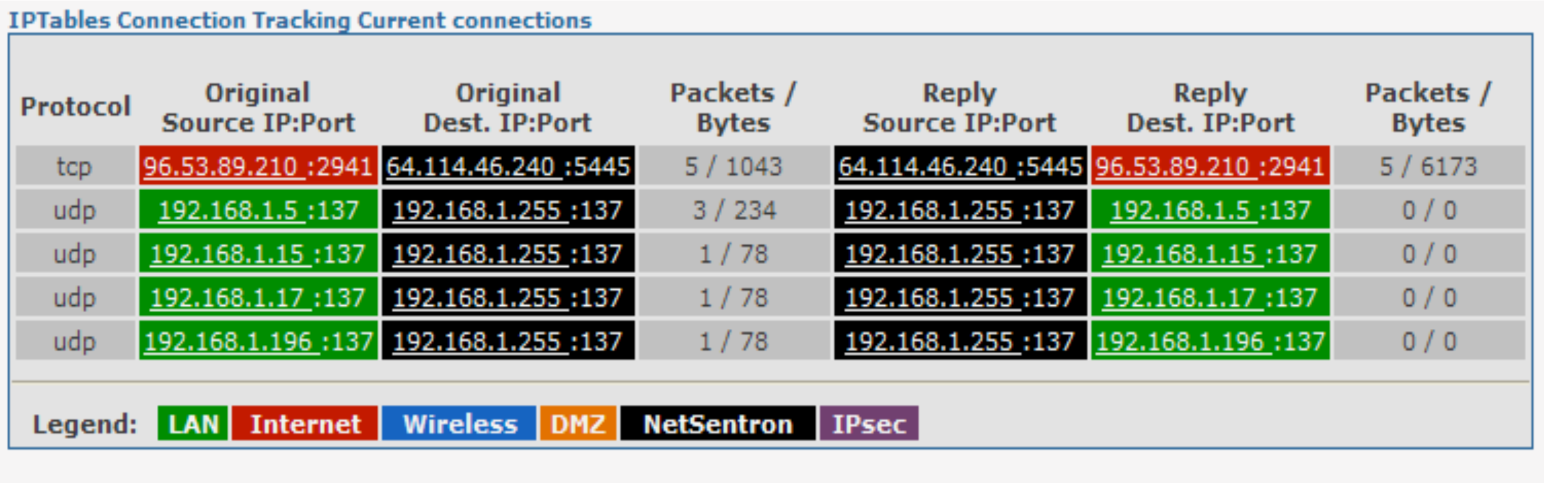
Checking Current Connections

The Connections page allows you to see who is currently connected to your NetSentron server. The page has been divided into two separate panels. If at any time you want the most current information on this page, just click the **Refresh** button on your browser.

1. From the Administration Interface, click on the Info button. New sets of buttons appear.
2. Click the connections button. The IP Tables Connection Tracking display appears. *See Figure 4.22* below. From this display you can see the current connections for the following:

LAN	Current LAN connections are displayed in GREEN.
Internet	Current Internet connections are displayed in RED.
Wireless	Current wireless connections are displayed in BLUE.
DMZ	Current DMZ connections are displayed in ORANGE.
NetSentron	Current NetSentron connections are displayed in BLACK.
VPN	Current VPN connections are displayed in PURPLE.

Figure 4.22: Connections Page



IPTables Connection Tracking Current connections

Protocol	Original Source IP:Port	Original Dest. IP:Port	Packets / Bytes	Reply Source IP:Port	Reply Dest. IP:Port	Packets / Bytes
tcp	96.53.89.210 :2941	64.114.46.240 :5445	5 / 1043	64.114.46.240 :5445	96.53.89.210 :2941	5 / 6173
udp	192.168.1.5 :137	192.168.1.255 :137	3 / 234	192.168.1.255 :137	192.168.1.5 :137	0 / 0
udp	192.168.1.15 :137	192.168.1.255 :137	1 / 78	192.168.1.255 :137	192.168.1.15 :137	0 / 0
udp	192.168.1.17 :137	192.168.1.255 :137	1 / 78	192.168.1.255 :137	192.168.1.17 :137	0 / 0
udp	192.168.1.196 :137	192.168.1.255 :137	1 / 78	192.168.1.255 :137	192.168.1.196 :137	0 / 0

Legend: LAN Internet Wireless DMZ NetSentron IPsec

Filtering Connection Results

You can filter the results of the connection page, by entering an IP address, partial IP address, port or protocol into the Filter input field. Then click on **Click to Filter** to filter the results.

Exporting Connection Results

If you wish to export the results, check the box labeled CSV Format and click on **Click to Filter**. Instead of the regular display, a text area will be created with a csv list of the results. You can then copy and paste this into excel or save it in a text file.

Connection Analysis

The Connection Analysis page allows you to view reports of abnormal connections. There are two pages associated with Connection Analyzer. The first page shows you the report. The second page is the configuration page.

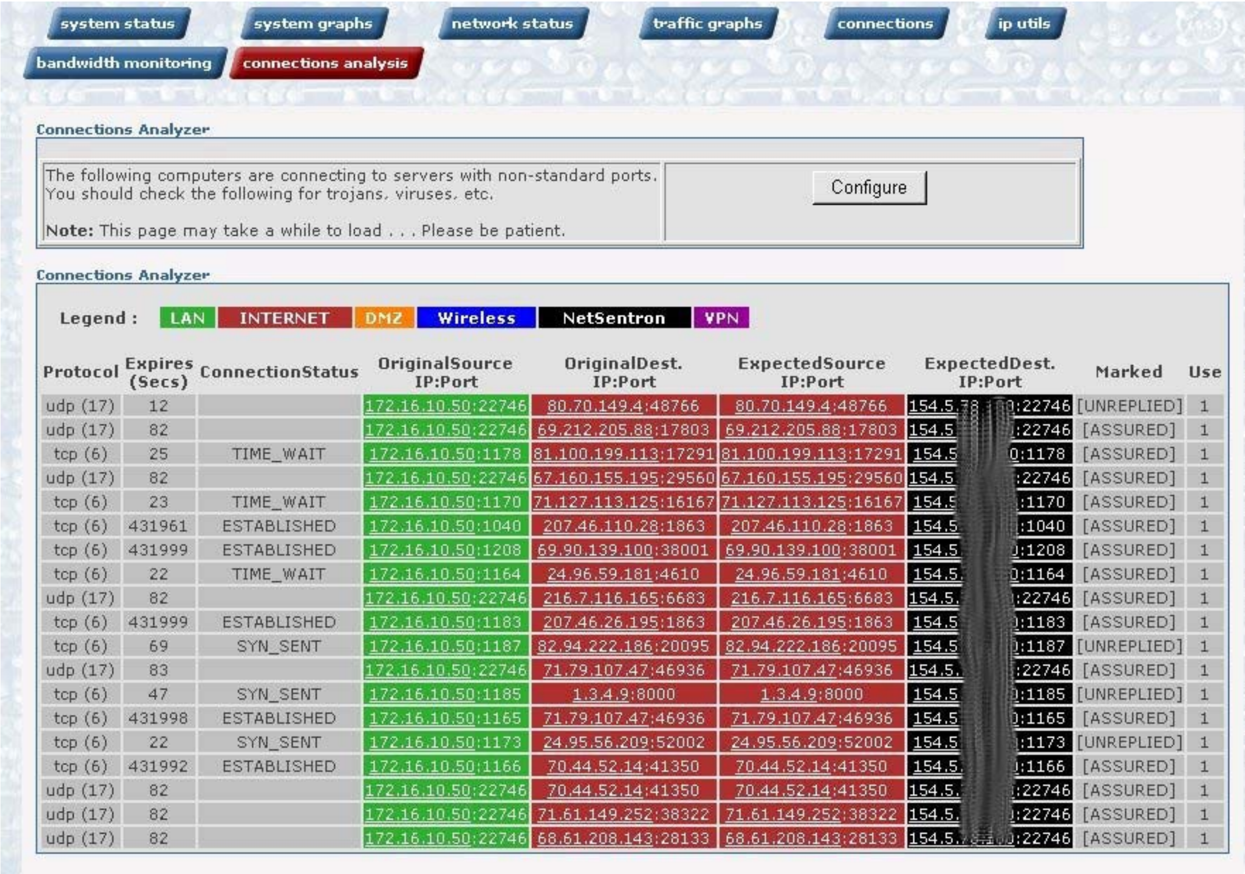
Viewing Connection Reports

From the Administration Interface, click on the Info button. New sets of buttons appear.

Click the connections analysis button. The Connections Analyzer page appears. *See Figure 4.23*, on the next page. The second panel is a report of your connections.

> **NOTE**
> The report panel only shows bad connections.

Figure 4.23: Connections Analyzer Page



Connections Analyzer

The following computers are connecting to servers with non-standard ports.
You should check the following for trojans, viruses, etc.

Note: This page may take a while to load . . . Please be patient.

Connections Analyzer

Legend : 🟩 LAN 🟥 INTERNET 🟧 DMZ 🟦 Wireless ⬛ NetSentron 🟪 VPN

Protocol	Expires (Secs)	ConnectionStatus	OriginalSource IP:Port	OriginalDest. IP:Port	ExpectedSource IP:Port	ExpectedDest. IP:Port	Marked	Use
udp (17)	12		172.16.10.50:22746	80.70.149.4:48766	80.70.149.4:48766	154.5[redacted]:22746	[UNREPLIED]	1
udp (17)	82		172.16.10.50:22746	69.212.205.88:17803	69.212.205.88:17803	154.5[redacted]:22746	[ASSURED]	1
tcp (6)	25	TIME_WAIT	172.16.10.50:1178	81.100.199.113:17291	81.100.199.113:17291	154.5[redacted]:1178	[ASSURED]	1
udp (17)	82		172.16.10.50:22746	67.160.155.195:29560	67.160.155.195:29560	154.5[redacted]:22746	[ASSURED]	1
tcp (6)	23	TIME_WAIT	172.16.10.50:1170	71.127.113.125:16167	71.127.113.125:16167	154.5[redacted]:1170	[ASSURED]	1
tcp (6)	431961	ESTABLISHED	172.16.10.50:1040	207.46.110.28:1863	207.46.110.28:1863	154.5[redacted]:1040	[ASSURED]	1
tcp (6)	431999	ESTABLISHED	172.16.10.50:1208	69.90.139.100:38001	69.90.139.100:38001	154.5[redacted]:1208	[ASSURED]	1
tcp (6)	22	TIME_WAIT	172.16.10.50:1164	24.96.59.181:4610	24.96.59.181:4610	154.5[redacted]:1164	[ASSURED]	1
udp (17)	82		172.16.10.50:22746	216.7.116.165:6683	216.7.116.165:6683	154.5[redacted]:22746	[ASSURED]	1
tcp (6)	431999	ESTABLISHED	172.16.10.50:1183	207.46.26.195:1863	207.46.26.195:1863	154.5[redacted]:1183	[ASSURED]	1
tcp (6)	69	SYN_SENT	172.16.10.50:1187	82.94.222.186:20095	82.94.222.186:20095	154.5[redacted]:1187	[UNREPLIED]	1
udp (17)	83		172.16.10.50:22746	71.79.107.47:46936	71.79.107.47:46936	154.5[redacted]:22746	[ASSURED]	1
tcp (6)	47	SYN_SENT	172.16.10.50:1185	1.3.4.9:8000	1.3.4.9:8000	154.5[redacted]:1185	[UNREPLIED]	1
tcp (6)	431998	ESTABLISHED	172.16.10.50:1165	71.79.107.47:46936	71.79.107.47:46936	154.5[redacted]:1165	[ASSURED]	1
tcp (6)	22	SYN_SENT	172.16.10.50:1173	24.95.56.209:52002	24.95.56.209:52002	154.5[redacted]:1173	[UNREPLIED]	1
tcp (6)	431992	ESTABLISHED	172.16.10.50:1166	70.44.52.14:41350	70.44.52.14:41350	154.5[redacted]:1166	[ASSURED]	1
udp (17)	82		172.16.10.50:22746	70.44.52.14:41350	70.44.52.14:41350	154.5[redacted]:22746	[ASSURED]	1
udp (17)	82		172.16.10.50:22746	71.61.149.252:38322	71.61.149.252:38322	154.5[redacted]:22746	[ASSURED]	1
udp (17)	82		172.16.10.50:22746	68.61.208.143:28133	68.61.208.143:28133	154.5[redacted]:22746	[ASSURED]	1

Adding Port Exclusion

1. From the Administration Interface, click on the Info button. New sets of buttons appear.

2. Click the connections analysis button. The Connections Analyzer page appears. *See Figure 4.23.* The third panel is a report of your connections.

3. To add a new configuration, click the Configure button located in the second panel. The Connections Analysis Configuration page appears. *See Figure 4.24: Connections Analysis Configuration,* on the next page*.* This page allows you to select which ports/protocols to ignore.
4.

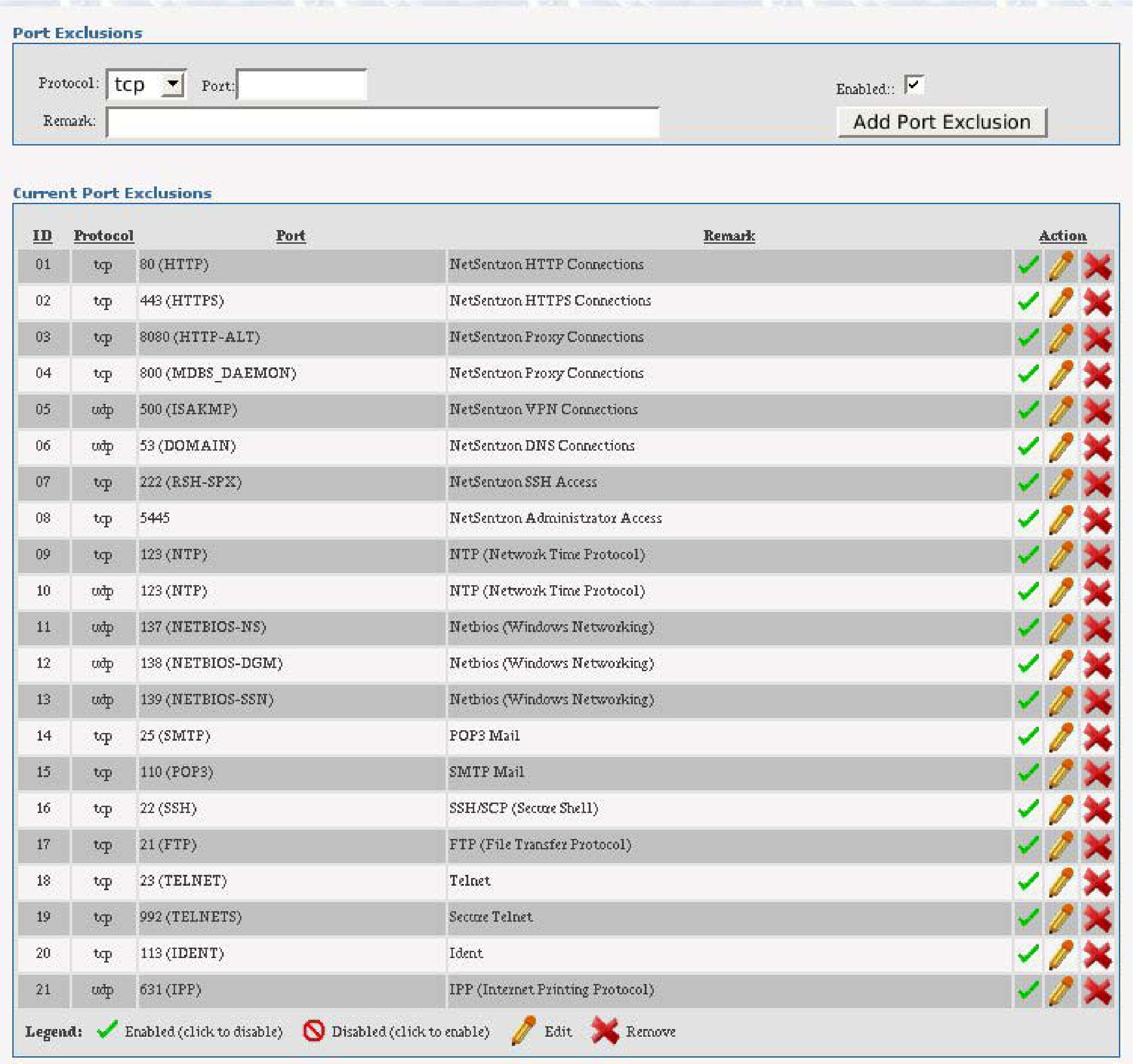
> **NOTE**
> The Current Port Exclusions list has 22 of the most common ports that a PC would normally access.

5. To add another configuration, key in the Protocol and Port.

6. In the Remark field, key in a description.

7. Click the Add Port Exclusion button. The port you added is now listed. Please ensure that Enabled has been selected.

Figure 4.24: Connections Analysis Configuration Page



Port Exclusions

Protocol: tcp ▾ Port:

Enabled:: ☑

Remark:

Current Port Exclusions

ID	Protocol	Port	Remark	Action
01	tcp	80 (HTTP)	NetSentron HTTP Connections	✓ ✎ ✖
02	tcp	443 (HTTPS)	NetSentron HTTPS Connections	✓ ✎ ✖
03	tcp	8080 (HTTP-ALT)	NetSentron Proxy Connections	✓ ✎ ✖
04	tcp	800 (MDBS_DAEMON)	NetSentron Proxy Connections	✓ ✎ ✖
05	udp	500 (ISAKMP)	NetSentron VPN Connections	✓ ✎ ✖
06	udp	53 (DOMAIN)	NetSentron DNS Connections	✓ ✎ ✖
07	tcp	222 (RSH-SPX)	NetSentron SSH Access	✓ ✎ ✖
08	tcp	5445	NetSentron Administrator Access	✓ ✎ ✖
09	tcp	123 (NTP)	NTP (Network Time Protocol)	✓ ✎ ✖
10	udp	123 (NTP)	NTP (Network Time Protocol)	✓ ✎ ✖
11	udp	137 (NETBIOS-NS)	Netbios (Windows Networking)	✓ ✎ ✖
12	udp	138 (NETBIOS-DGM)	Netbios (Windows Networking)	✓ ✎ ✖
13	udp	139 (NETBIOS-SSN)	Netbios (Windows Networking)	✓ ✎ ✖
14	tcp	25 (SMTP)	POP3 Mail	✓ ✎ ✖
15	tcp	110 (POP3)	SMTP Mail	✓ ✎ ✖
16	tcp	22 (SSH)	SSH/SCP (Secure Shell)	✓ ✎ ✖
17	tcp	21 (FTP)	FTP (File Transfer Protocol)	✓ ✎ ✖
18	tcp	23 (TELNET)	Telnet	✓ ✎ ✖
19	tcp	992 (TELNETS)	Secure Telnet	✓ ✎ ✖
20	tcp	113 (IDENT)	Ident	✓ ✎ ✖
21	udp	631 (IPP)	IPP (Internet Printing Protocol)	✓ ✎ ✖

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) ✎ Edit ✖ Remove

Disabling/Enabling a Port Exclusion

1. From the Administration Interface, click on the **Info** button. New sets of buttons appear.

2. Click the **connections analysis** button. The Connections Analyzer page appears.

3. Next, click the **Configure** button located in the second panel. The Connections Analysis Configuration page appears. *See Figure 4.24.*

4. Click the ✓ icon on the same line of the port you want to disable. The icon is changes to the 🚫 icon. To re-enable the port click on the 🚫 icon and the ✓ re-appears.

Editing a Port Exclusion

1. From the Administration Interface, click on the Info button. New sets of buttons appear.
2. Click the connections analysis button. The Connections Analyzer page appears. *See Figure 4.23,* on page 48. The second panel is a report of your connections.
3. Next, click the Configure button located in the second panel. The Connections Analysis Configuration page appears. *See Figure 4.24,* on page 50.
4. Click the ✎ icon on the same line of the port you want to edit. The details for that port are placed in the Edit a Port Exclusion rule panel.

> **NOTE**
> The port rule you are editing is highlighted yellow.

Removing a Port Exclusion

1. From the Administration Interface, click on the Info button. New sets of buttons appear.
2. Click the connections analysis button. The Connections Analyzer page appears. *See Figure 4.23* on page 48. The second panel is a report of your connections.
3. Next, click on the Configure button located in the second panel. The Connections Analysis Configuration page appears. *See Figure 4.24* on

page 49.

4. Click the ✖ icon on the same line of the port you want to remove. **Note:** Once you click the delete icon, the port rule is removed automatically.

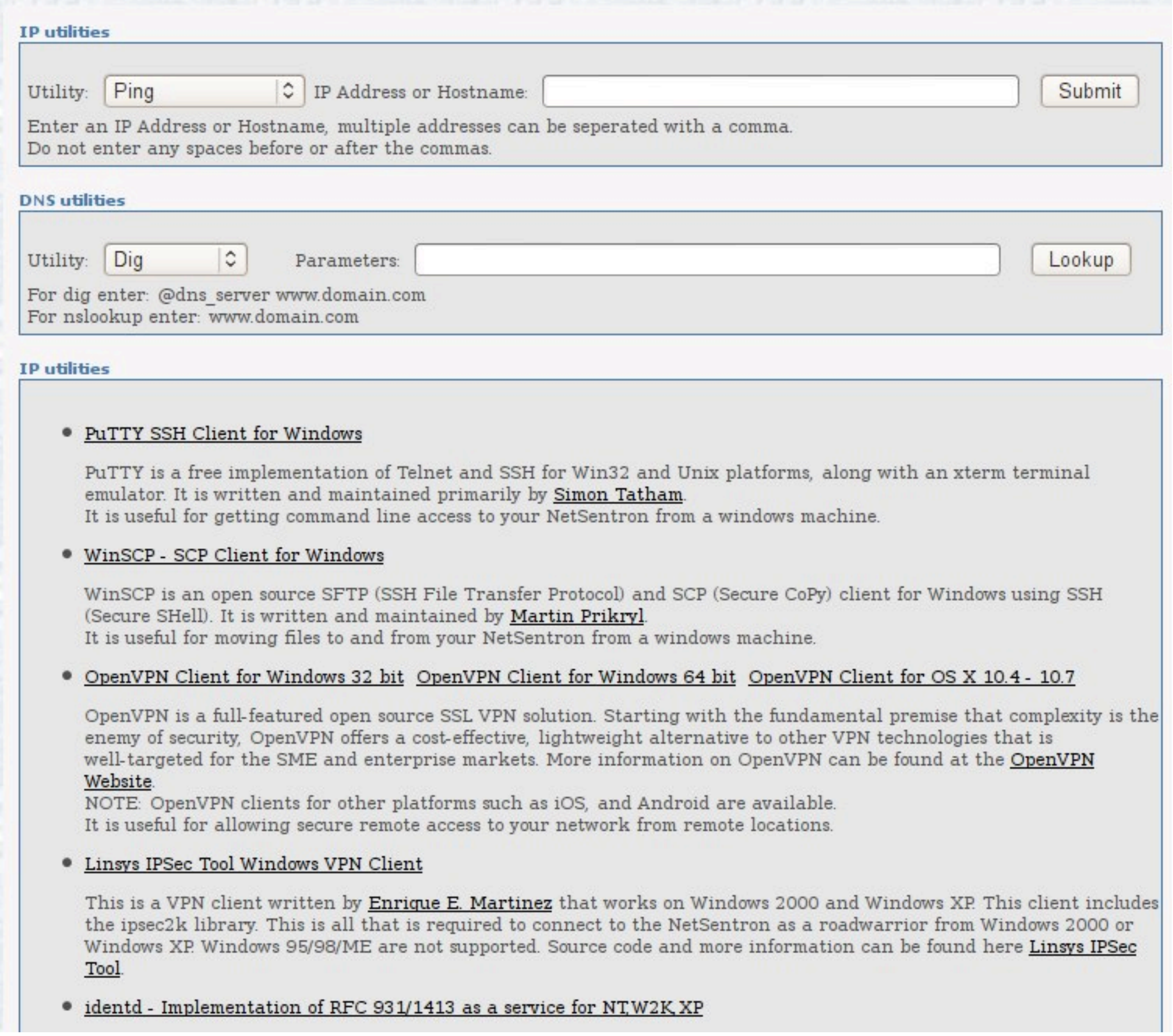
Filtering and Exporting Connection Analysis

The filtering and exporting on the Connection Analysis page works exactly the same as the one for the connections page seen in Figure 4.24.

IP Utilities

1. From the Administration Interface, click on the Info button. New sets of buttons appear.
2. Click the ip utils button. The IP Utilities page appears. *See Figure 4.25 - IP Utilities Page* on the next page.

Figure 4.25: IP Utilities Page



IP utilities

Utility: Ping IP Address or Hostname:

Enter an IP Address or Hostname, multiple addresses can be seperated with a comma.
Do not enter any spaces before or after the commas.

DNS utilities

Utility: Dig Parameters:

For dig enter: @dns_server www.domain.com
For nslookup enter: www.domain.com

IP utilities

- PuTTY SSH Client for Windows

  PuTTY is a free implementation of Telnet and SSH for Win32 and Unix platforms, along with an xterm terminal emulator. It is written and maintained primarily by Simon Tatham.
  It is useful for getting command line access to your NetSentron from a windows machine.

- WinSCP - SCP Client for Windows

  WinSCP is an open source SFTP (SSH File Transfer Protocol) and SCP (Secure CoPy) client for Windows using SSH (Secure SHell). It is written and maintained by Martin Prikryl.
  It is useful for moving files to and from your NetSentron from a windows machine.

- OpenVPN Client for Windows 32 bit OpenVPN Client for Windows 64 bit OpenVPN Client for OS X 10.4 - 10.7

  OpenVPN is a full-featured open source SSL VPN solution. Starting with the fundamental premise that complexity is the enemy of security, OpenVPN offers a cost-effective, lightweight alternative to other VPN technologies that is well-targeted for the SME and enterprise markets. More information on OpenVPN can be found at the OpenVPN Website.
  NOTE: OpenVPN clients for other platforms such as iOS, and Android are available.
  It is useful for allowing secure remote access to your network from remote locations.

- Linsys IPSec Tool Windows VPN Client

  This is a VPN client written by Enrique E. Martinez that works on Windows 2000 and Windows XP. This client includes the ipsec2k library. This is all that is required to connect to the NetSentron as a roadwarrior from Windows 2000 or Windows XP. Windows 95/98/ME are not supported. Source code and more information can be found here Linsys IPSec Tool.

- identd - Implementation of RFC 931/1413 as a service for NT,W2K,XP

The IP Utilities Page contains several useful built in tools:

A. PING

PING is a computer network tool used to test if a particular host is reachable across an IP network.

Using interval timing and response rate, PING estimates the round-trip and rate of packet loss between hosts. You can enter an IP Address or URL and click submit (separate multiples with commas).

B. Trace Route

Trace Route is a computer network tool used to determine the route taken by packets across an IP network.

You can enter an IP Address or URL and click submit (separate multiples with commas).

C. Lookup Machine
This is used if you have an IP address and would like to know the MAC address + Machine name.

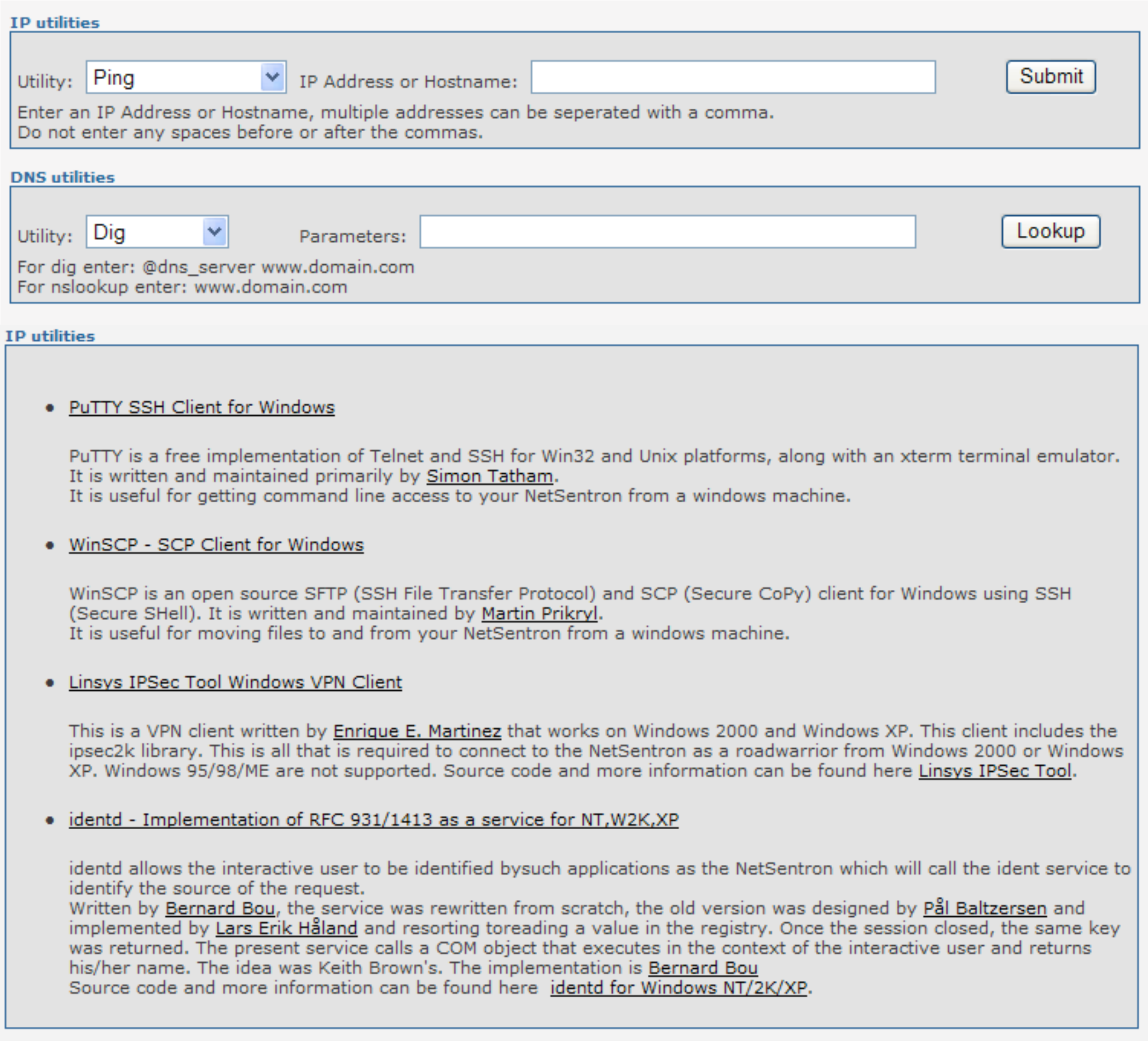
D. IP Info
This is used if you have an IP address or domain name and would like to know who owns the IP address or block of IP Addresses associated with the original IP or domain name.

E. DIG
DIG (Domain Information Groper) is a network tool that requires DNS Name Servers. It can be used to simulate a name resolver or a name server. This will verify that a DNS Server is working as expected.

F. NS Lookup

This is used to find the IP Address of a particular computer using DNS Lookup. It also verifies that DNS is working properly.

Figure 4.26: IP Utilities



IP utilities

Utility: Ping IP Address or Hostname:

Enter an IP Address or Hostname, multiple addresses can be seperated with a comma.
Do not enter any spaces before or after the commas.

DNS utilities

Utility: Dig Parameters:

For dig enter: @dns_server www.domain.com
For nslookup enter: www.domain.com

IP utilities

- PuTTY SSH Client for Windows

  PuTTY is a free implementation of Telnet and SSH for Win32 and Unix platforms, along with an xterm terminal emulator.
  It is written and maintained primarily by Simon Tatham.
  It is useful for getting command line access to your NetSentron from a windows machine.

- WinSCP - SCP Client for Windows

  WinSCP is an open source SFTP (SSH File Transfer Protocol) and SCP (Secure CoPy) client for Windows using SSH (Secure SHell). It is written and maintained by Martin Prikryl.
  It is useful for moving files to and from your NetSentron from a windows machine.

- Linsys IPSec Tool Windows VPN Client

  This is a VPN client written by Enrique E. Martinez that works on Windows 2000 and Windows XP. This client includes the ipsec2k library. This is all that is required to connect to the NetSentron as a roadwarrior from Windows 2000 or Windows XP. Windows 95/98/ME are not supported. Source code and more information can be found here Linsys IPSec Tool.

- identd - Implementation of RFC 931/1413 as a service for NT,W2K,XP

  identd allows the interactive user to be identified bysuch applications as the NetSentron which will call the ident service to identify the source of the request.
  Written by Bernard Bou, the service was rewritten from scratch, the old version was designed by Pål Baltzersen and implemented by Lars Erik Håland and resorting toreading a value in the registry. Once the session closed, the same key was returned. The present service calls a COM object that executes in the context of the interactive user and returns his/her name. The idea was Keith Brown's. The implementation is Bernard Bou
  Source code and more information can be found here identd for Windows NT/2K/XP.

There are also several downloadable tools:

A. Putty - Secure shell client for Windows (SSH) allows you to connect to the NetSentron using the command line from a Windows PC. This runs on Port 222 on the NetSentron.

B. WinSCP - SFTP Client (FTP over SSH) is useful for downloading logs or files from the NetSentron. This runs on Port 222 on the NetSentron.

C. OpenVPN Client – This is a free client that allows you to create a VPN to the LAN behind your NetSentron. It is a free and open source solution. It is actually an SSL VPN. Clients are included for Windows 7 32 & 64 bit as well as Macintosh OSX 10.4 to 10.7. There are versions of openvpn clients available elsewhere for iOS devices and Android devices.

D. Linsys ISPec Client - IPSec UPN Client for Windows 2000 XP, 2003, is used to create a VPN from a Windows PC to the NetSentron. **Note:** Linsys will NOT work with some installations of Windows XP and Windows Vista. It also will not work on Windows 7 or 8. For those operating systems we suggest Greenbow.

E. Identd – This is a small service that you can install on older Windows machines that will pass the logged on user name of the machine to the NetSentron so that it can be used in the logging.

Identd Instructions

Download identd for Windows NT/2000/XP

identdnt-setup.exe This can be found on your NetSentron under Info -> ip utils or on the NetSentron web site at: http://www.netsentron.com/utilities.html

Installation & Configuration instructions NT/2000/XP

Double click the identnt-setup.exe to install the software just like any other Windows application.

Then open up a DOS box and change to the directory where you installed identd. (Start menu -> Run -> cmd)

Install Identd as a Service

- Type: ***identd.exe -install***
- To verify it is installed as a service, go to Control Panel and select Services, you should see ***Identd RFC931/1413 service -(bb)*** installed as an automatic service.

Remove Identd as a Service

- Type: ***identd.exe –remove***

NOTE

On Windows XP you will need to adjust the Windows Firewall to allow identd.exe to be an exception. If you are running another third party firewall such as ZoneAlarm, you will need to allow identd.exe to bypass the firewall.

Configure the NetSentron to use Identd

- Click on the **Filters** button in the menu across the top.
- Enable the check box labeled: ***Enable Ident Authentication***

You should now start seeing the logged in user show up in the Web Access Logs.

NOTE

Machines that do not have the identd service running will experience extremely slow Internet access as the identd service will have to time out for every request before sending information to the browser.

Bandwidth Monitoring

The Bandwidth Monitoring page allows you to monitor all traffic on your network and see a table as well as a graphical representation of how much each machine on your LAN is using.

NOTE

A machine does not actually have to use the NetSentron as a gateway for its bandwidth usage to appear on this page.

Bandwidth Monitoring is particularly useful for spotting P2P activity, gaming activity and also can be used as an indicator of spyware/malware/trojans running on your PCs. *See Figure 4.27: Bandwidth Monitoring Page on the next page to see an example of P2P traffic, as well as some other interesting occurrences in the graph.*

From the Administration Interface, click on the Info button. New sets of buttons appear.

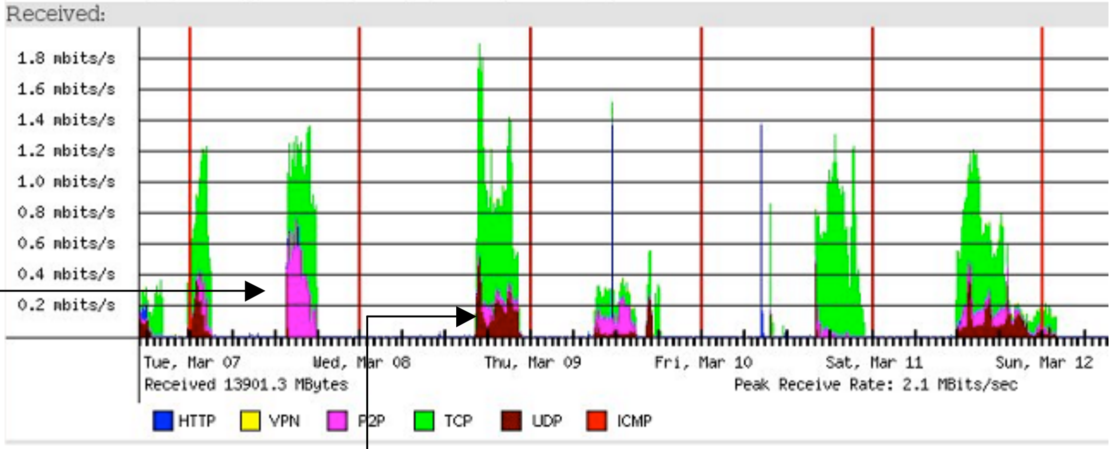
Click the bandwidth monitoring button. The Bandwidth Monitoring page appears. *See Figure 4.27: Bandwidth Monitoring Page,* on the next page*.* The Bandwidth Monitoring page is a read only page, which shows the Top 20 bandwidth users.

Check the Enabled box, and click the Save button. The Bandwidth Monitoring is now configured.

NOTE

It will take several minutes to accumulate some stats. It will also take corresponding time to generate daily, weekly, and monthly stats; be patient, and the stats will be displayed.

Figure 4.27: Bandwidth Monitoring Page



As you can see, on Wednesday at about 2PM there was a large spike in P2P. Again on Thursday, Friday, Saturday and Sunday

The brown UDP spike on Wednesday and Saturday can be an indicator of several things. One is gaming activity, most on line multi-player games are using UDP to communicate with the other peers. The other thing this could be is a trojan/malware/spyware. Many of these programs use UDP as a transport protocol

NOTE

If you are seeing many green spikes from PCs on your LAN, this can be an indicator of an infected machine, which may have some form of trojan/malware/spyware on it.

In a classroom environment, most of your PCs should have about the same bandwidth usage if they are all being used for their intended purpose. Watch for spikes and abnormally high bandwidth usage to find potentially inappropriate usage or infected PCs.

Chapter 5 Services

Services gives the administrator the ability to configure and administer the many service options provided with the NetSentron. By default, when you click on the Services button you will be given the Web Proxy administration page. By clicking on the remaining buttons, you bring up the other service administration pages.

Web Proxy

The NetSentron runs a caching web proxy. This process provides a cache of items available on a server, which accepts URLs with a special prefix. When it receives a request for such a URL, it strips off the prefix and looks for the resulting URL in its local cache. If found, it returns the document immediately or it fetches it from the remote server, saves a copy in the cache and returns it to the requester. The cache will usually have an expiry algorithm, which flushes documents according to their age, size, and access history. The proxy supports http, https, and ftp proxy caching. The following are step-by-step instructions on how to configure your NetSentron web proxy setting.

From the Administration Interface, click on the Services button. By default you are on the Web Proxy Page of the NetSentron Interface. *See Figure 5.1 Web Proxy .* NetSentron has given you default settings, allowing for the best service. This page has been divided into 3 separate panels: Web Proxy, Authentication options and Domain information. The following is a description of the settings provided in each section on this page. **Fields with a ● may be left blank**

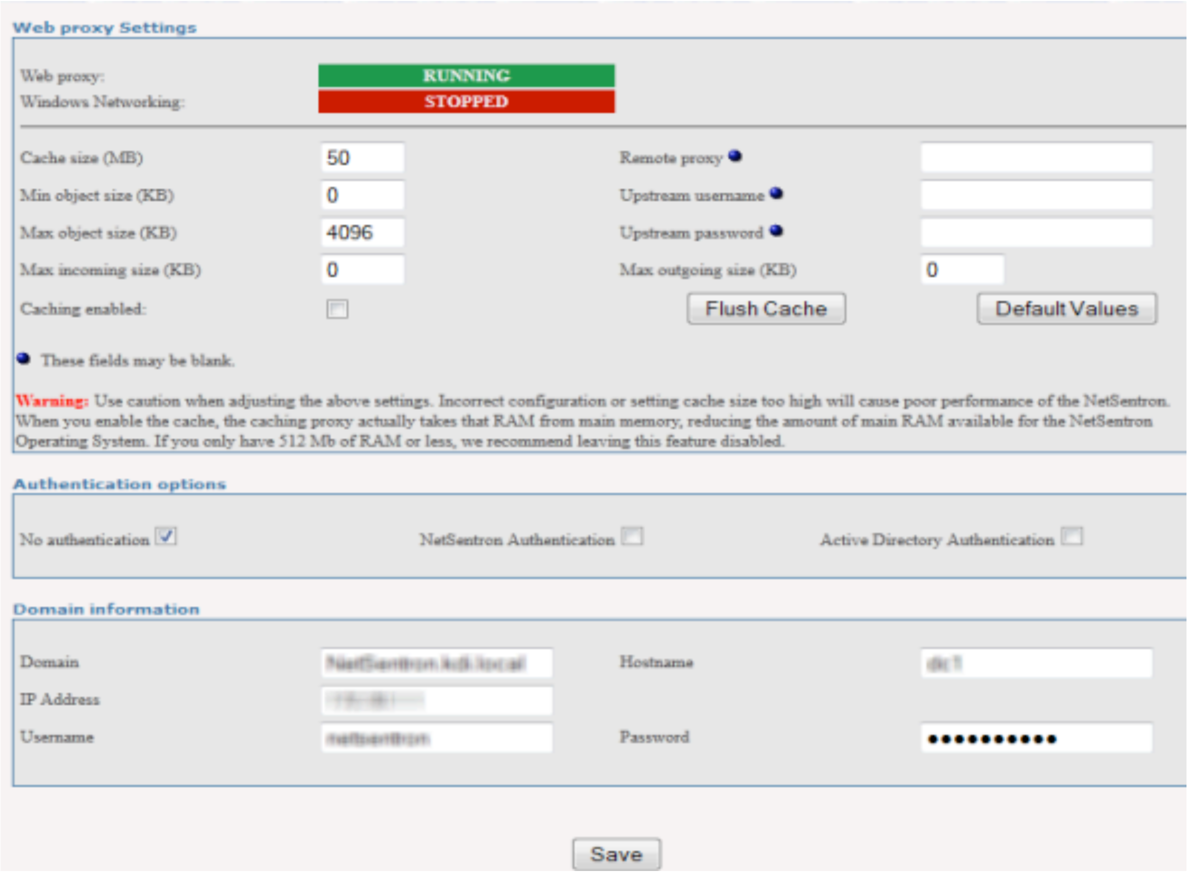
NOTE

Unless you are familiar with proxy settings it is in your best interest to keep the default settings.

Configuring Web Proxy Settings

Cache size (MB)	Allows the user to set the maximum size of the cache, in megabytes. The default is set to 50 MB.
Min object size (KB)	Sets the smallest object size that will enter the cache. This allows the user to force the proxy to only cache objects that are larger that the size entered.
Max object size (KB)	Sets the largest object size that will enter the cache. This allows the user to force the proxy to only cache objects that are smaller than the size entered.
Max incoming size (KB)	The amount entered will be the maximum download size for a file that the proxy will allow through. This stops people from downloading large files that would slow your network down.
Caching Enabled	This is really useful for low speed connections such as dial up and ISDN. With more than 50 users on the network you will require a memory upgrade to the NetSentron. Please contact a KDI Technician or your NetSentron Partner for more information.
Remote Proxy	Selecting this option allows NetSentron to use another web proxy from a remote location.
Upstream username	If you are using a third party proxy such as your ISP's sometimes you have to supply a username for it.
Upstream password	If you are using a third party proxy such as your ISP's sometimes you have to supply the password associated with the Upstream username.
Max outgoing size (KB)	Sets the size of the date that a browser is allowed to send through the proxy, whether or not it is cached.
Flush Cache	Click this button to flush out contents of the cache. This will only work if `Caching Enabled` is checked.
Default Values	Click this button to reset your web proxy back to the default settings.

Figure 5.1 Web Proxy Page



Web proxy Settings

Web proxy:	RUNNING
Windows Networking:	STOPPED

Cache size (MB)	50	Remote proxy ●	
Min object size (KB)	0	Upstream username ●	
Max object size (KB)	4096	Upstream password ●	
Max incoming size (KB)	0	Max outgoing size (KB)	0
Caching enabled:	□	Flush Cache	Default Values

● These fields may be blank.

Warning: Use caution when adjusting the above settings. Incorrect configuration or setting cache size too high will cause poor performance of the NetSentron. When you enable the cache, the caching proxy actually takes that RAM from main memory, reducing the amount of main RAM available for the NetSentron Operating System. If you only have 512 Mb of RAM or less, we recommend leaving this feature disabled.

Authentication options

No authentication ☑ NetSentron Authentication □ Active Directory Authentication □

Domain information

Domain	[redacted]	Hostname	[redacted]
IP Address	[redacted]		
Username	[redacted]	Password	●●●●●●●●●●●

Authentication Options

No Authentication

1. To select no authentication simply check the `No authentication box` located in the Authentication options panel.

   See *Figure 5.1 Web Proxy above*.

2. Click the Save button to confirm.

NetSentron Authentication

1. NetSentron Authentication makes the browser query each user for a username and password. The list of users is maintained on the NetSentron via the users and groups pages.
2. In the Authentication options panel of the Web Proxy page, select the NetSentron Authentication box.

> **NOTE**
>
> Selecting this setting will prompt each user for a user name and password when opening a browser. For the NetSentron Authentication setting to work you will need to give each user a name and password. These can be entered in the Users administration area on *page 86 of the NS200 Users' Guide*. Next, you will need to change the proxy server settings on each PC attached to the NetSentron. To make changes to your browsers Proxy Server settings go to *Changing Your Browsers Web Proxy Settings to allow for User Authentication* on page 89 of the *NS200 Users' Guide.*

3. Click the Save button to confirm.

Active Directory Authentication

The following are step-by-step instructions on adding Active Directory Authentication.

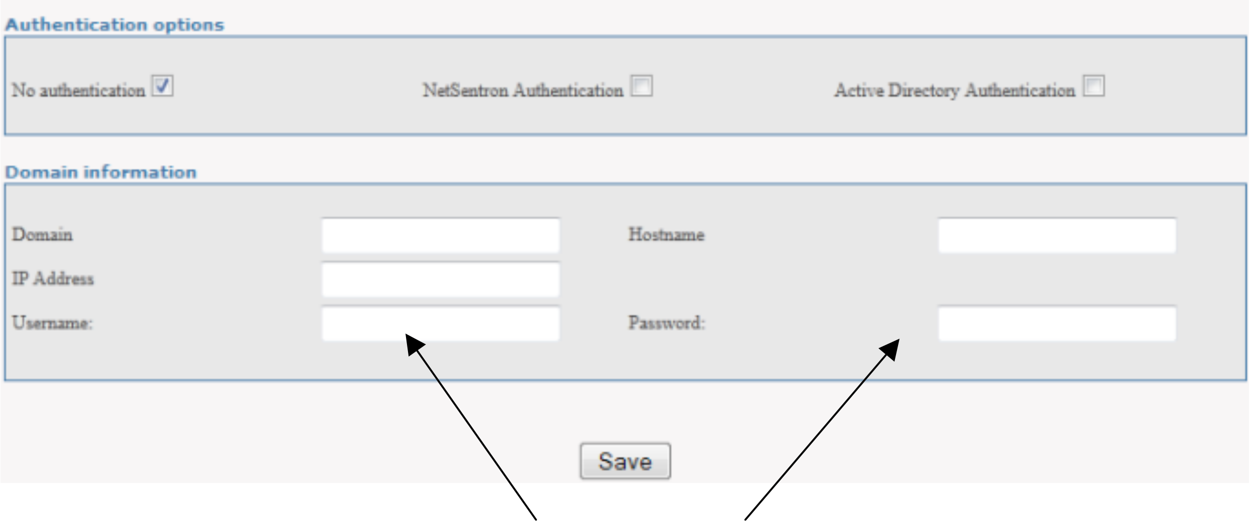
1. In the Authentication options panel of the Web Proxy page, select the Active Directory Authentication box.
2. In the Domain information panel you will need to enter the ***domain name*** in the domain field.
3. Key in the ***IP address*** of the windows server in the IP Address field.
4. Next, You will need to create a user on the Windows server, which is part of the domain, and that the NetSentron can use to authenticate the individual users.
5. Take the same ***username*** and ***password*** that you created on the Windows server and enter them in the username and password fields located in the Domain information panel. *See Figure 5.2: Active Directory Authentication* on the next page.

6. Click the Save button to confirm.

NOTE

The user needs to be created on Domain Controller so that the NetSentron can authenticate with Active Directory.

Figure 5.2: Active Directory Authentication



Authentication options

No authentication ☑ NetSentron Authentication □ Active Directory Authentication □

Domain information

Domain:
Hostname:
IP Address:
Username:
Password:

Save

Use the same ***username*** and ***password*** used
when creating the user on your windows server.

Active Directory Authentication with NetSentron

The NetSentron is capable of authenticating users against an Active Directory server to validate their username and password. It is supported on Windows server 2000, 2003 and 2008. This can be done in two ways: single sign on where any machine already logged on to the Domain will automatically pass its credentials on to the NetSentron, or, if not logged in, a dialog will come up asking for a valid username and password.

NOTE

The time on the NetSentron and the time on the Active Directory Server cannot be more than five minutes apart or this will **NOT** work. See p. 81.

To enable Active Directory Authentication with the NetSentron, you need to collect some information and also create an Administrative user on the Active Directory Server.

Log into your Active Directory server and create a new user account for the NetSentron to use. This account must have administrative rights for this to work. This is mandatory for Active Directory Authentication. Once you have done that, write it down here:

Username: ______________________ Password: ___________________

Then get the following information from the Active Directory Server:

IP Address of the Server: _________________________

Hostname of the Server: __________________________

Domain of the Server: ____________________________

Once you have recorded that information, you can now enter it into the NetSentron to enable Active Directory Authentication.

Log into the web based interface for the NetSentron and go to Firewall -> Hosts . Make an entry into the hosts table so that the NetSentron can find the Active Directory Server.

- For Host IP: enter the IP Address of the Active Directory Server
- For Hostname: enter the Hostname of the Active Directory Server
- For Domain name: enter the Domain of the Active Directory Server

Click on **Add** to save your entry. Ensure that a new entry appears below in the Current Hosts section of the Hosts page, then click on the Services menu entry and scroll down to Domain information.

There you will see five fields that need to be filled to enable Active Directory Authentication. **DO NOT** click on Active Directory Authentication in the Authentication options section until we have completed the entries in this section.

- For Domain, enter the Domain of the Active Directory Server
- For Hostname, enter the Hostname of the Active Directory Server
- For IP Address, enter the IP Address of the Active Directory Server
- For Username, enter the username you created on the Active Directory Server
- For Password, enter the password you created on the Active Directory Server

Double check that everything is correct.

NOTE

Hosts and Domains are case sensitive.

Click on the Save button. If the information has no errors, then it should be saved. Next go to the Authentication options section and click on Active Directory Authentication and then click on Save again. When the page reloads, you should see some new items in the Domain information section. It should show Active Directory Status, with some buttons after it.

Click on the Join Domain button and wait for the page to reload. Upon reloading, if everything has been entered correctly, then the Active Directory Status should change to `Joined to Domain` . . . . in green writing. If it is still in Red writing, then click on Services menu item again and see if it has changed to Green writing.

If it still is showing as not connected, then you have made an error and will need to recheck your settings.

Once the NetSentron has successfully joined the domain, it will show up in your Windows Active Directory Server as the hostname you created for the NetSentron when you installed the software.

Changing Your Browsers Web Proxy Settings to allow for User Authentication

For User Authentication to work, you will need to change the Web Proxy settings on your web browser.

Changing Web Proxy Settings on Internet Explorer

1. Open up your Internet Explorer. Click on Tools / Internet Options / Connections.
2. Click on the LAN Settings button. Check Use a proxy serverand then key in the Address (this is the green address of the NetSentron).
3. Next, key in the port (Use Port 8080). Click the OK button to confirm.

Changing Web Proxy Setting on Mozilla Firefox

1. Open up your Firefox browser.
2. Click on Tools / Options. The Options dialog box appears.
3. In the top panel, click on **Advanced**. A new pane will appear.
4. Next, click on the **Network** tab, The Connections panel appears.
5. Click on the **Settings** button and a new dialog will pop up.
6. Select **Manual proxy** configuration.
7. In the `HTTP:` field, key in the Address (this is the green address of the NetSentron).

Under the `Port` field key in the port (Use Port 8080). Click on the OK button to confirm.

DHCP Settings

Dynamic Host Control Protocol (DHCP) allows you to automatically assign IP addresses to computers on your network. The DHCP Administration Page allows the administrator to configure your Dynamic Host Control Protocol as well as add fixed leases.

Configuring DHCP Settings

The following are instructions on how to configure your DHCP settings.

1. From the Administration Interface, click on the Services button. New sets of buttons appear.
2. Click the dhcp button. The DHCP Administration Page appears. *See Figure 5.3: DHCP Settings* on page 67*.* For configuring your DHCP setting you will be using the DCHP panel. You will need to fill in the following fields.

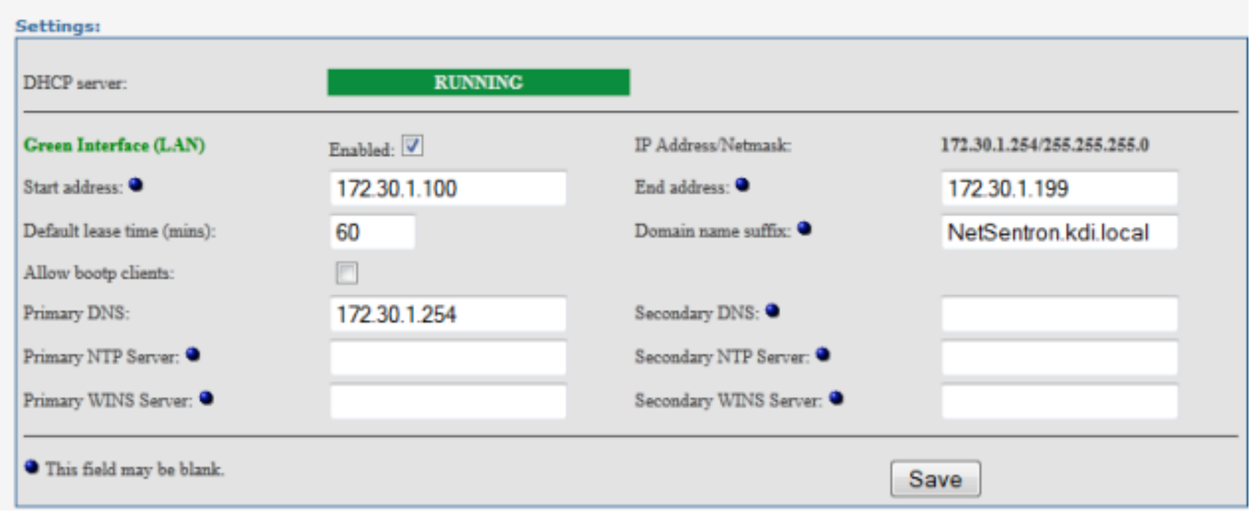
Fields with a ● may be left blank

Start Address	Key in the specific starting address of your DHCP IP address range that you want the DHCP server to supply. Make sure that the address range you have chosen does not contain the IPs of other machines on your LAN with Static IP assignments.
End Address	Key in the specific ending address of your DHCP IP range that you want the DHCP server to supply. Just like the starting address, make sure that the address range you have chosen does not contain the IPs of other machines on your LAN with Static IP assignments.
Primary DNS	Key in the address that the DHCP server should tell its clients to use for their Primary DNS server. By default, this is usually set as the green address. For the best results leave it on the default setting.
Secondary DNS	If you are running a local DNS server and want your desktops to use it, set the Secondary DNS to its address.
Default lease time	Should be left at the default setting.

NTP Server address	If you are running an NTP server and wish to pass that along to your clients via DHCP, then enter the primary and secondary NTP addresses here.
Domain name suffix	Key in the domain name that the DHCP server will give to the client. There should not be a leading period in this box. This setting is optional.
Wins Server address	If you are running a WINS server on your LAN or at the end point of your VPN, then the IP Address of your WINS server should be entered here. (WINS) Windows Internet Name Service.

3. Once you have entered the information in the required fields, click the Save button.

Figure 5.3: DHCP Settings



Settings:

DHCP server: RUNNING

Green Interface (LAN)	Enabled: ☑	IP Address/Netmask:	172.30.1.254/255.255.255.0
Start address: ●	172.30.1.100	End address: ●	172.30.1.199
Default lease time (mins):	60	Domain name suffix: ●	NetSentron.kdi.local
Allow bootp clients:	□		
Primary DNS:	172.30.1.254	Secondary DNS: ●	
Primary NTP Server: ●		Secondary NTP Server: ●	
Primary WINS Server: ●		Secondary WINS Server: ●	

● This field may be blank.

Adding a New Fixed Lease

Fixed leases allow you to serve the same IP address to the same machine on your network. This is handy if you have a server or a particular machine that you always want at the same address.

1. From the Administration Interface, click on the Services button. New sets of buttons appear.

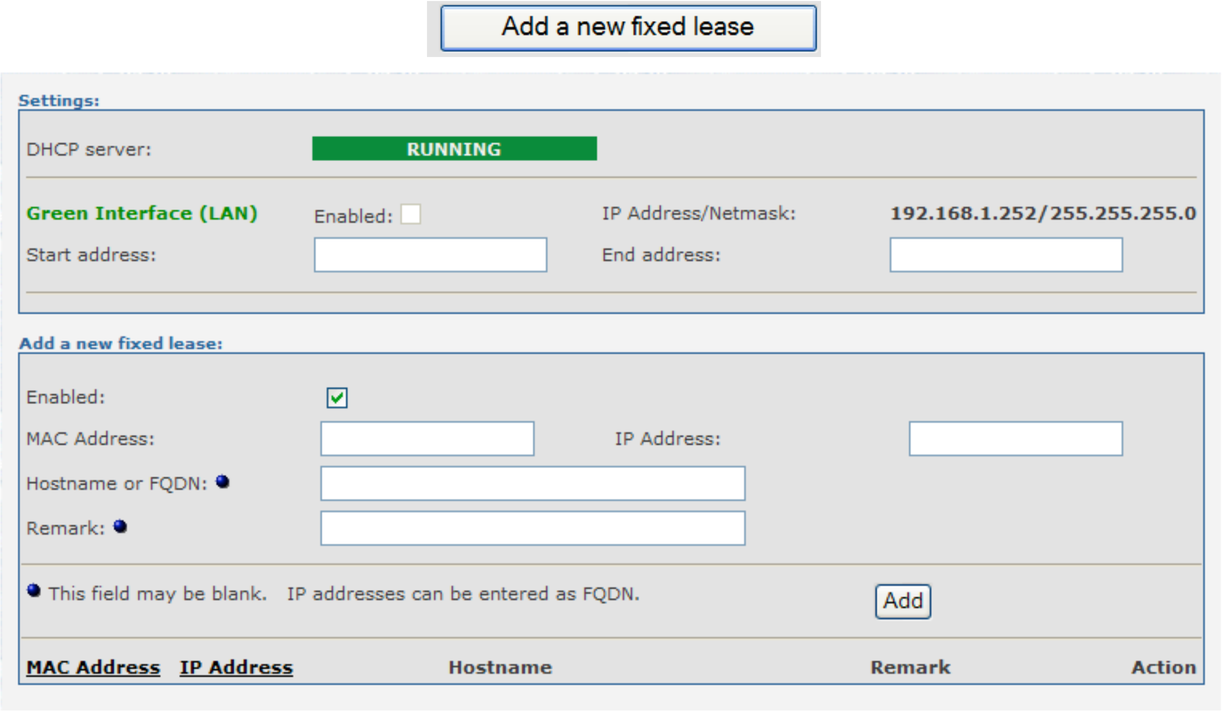
2. Click the dhcp button. The DHCP Administration Page appears. *See Figure 5.4: Add a New Fixed Lease;* this page has been divided into to four separate panels. To add a new fixed lease you will be using the Add a new fixed lease panel. There are only two fields you will need to fill in. The instructions are as follows:

MAC Address	Type in the MAC address provided on your network interface card.
IP Address	Key in the IP address.
Remark	Key in a description of the new fixed lease.
Enabled	Enable the fixed lease by ticking the *Enabled* checkbox.

3. Once you have entered the information in the fields, click the Add button.

4. The new fixed address has been added. You can view this in the Current fixed leases panel on the same page. See Figure 5.5 on the next page.

Figure 5.4: Add A New Fixed Lease



Add a new fixed lease

Settings:

DHCP server: RUNNING

Green Interface (LAN) Enabled: □ IP Address/Netmask: 192.168.1.252/255.255.255.0

Start address: End address:

Add a new fixed lease:

Enabled: ☑

MAC Address: IP Address:

Hostname or FQDN: ●

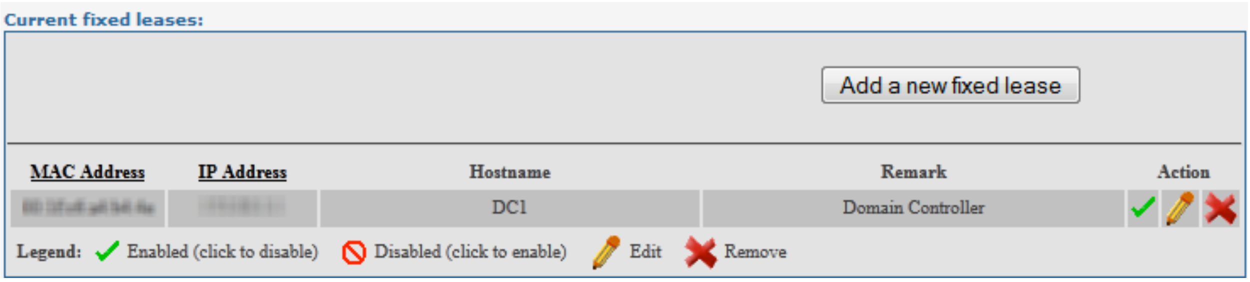
Remark: ●

● This field may be blank. IP addresses can be entered as FQDN.

Add

MAC Address	IP Address	Hostname	Remark	Action

Figure 5.5: Current Fixed Leases



Current fixed leases:

Add a new fixed lease

MAC Address	IP Address	Hostname	Remark	Action
[redacted]	[redacted]	DC1	Domain Controller	✓ ✎ ✖

Legend: ✓ Enabled (click to disable) 🚫 Disabled (click to enable) ✎ Edit ✖ Remove

External Aliases

External Aliases allow you to assign multiple IP addresses to the RED interface. The purpose of these interfaces is to combine them with port forwarding to allow mail and web servers to be protected by the NetSentron using a real Internet address. This can be useful for combining a few web/ftp servers behind a NetSentron and forwarding their ports through with their own Internet address on the NetSentron.

NOTE

External Aliases only works if you have a static IP address on RED.

Adding an External Alias

The following are instructions on how to add external aliases.

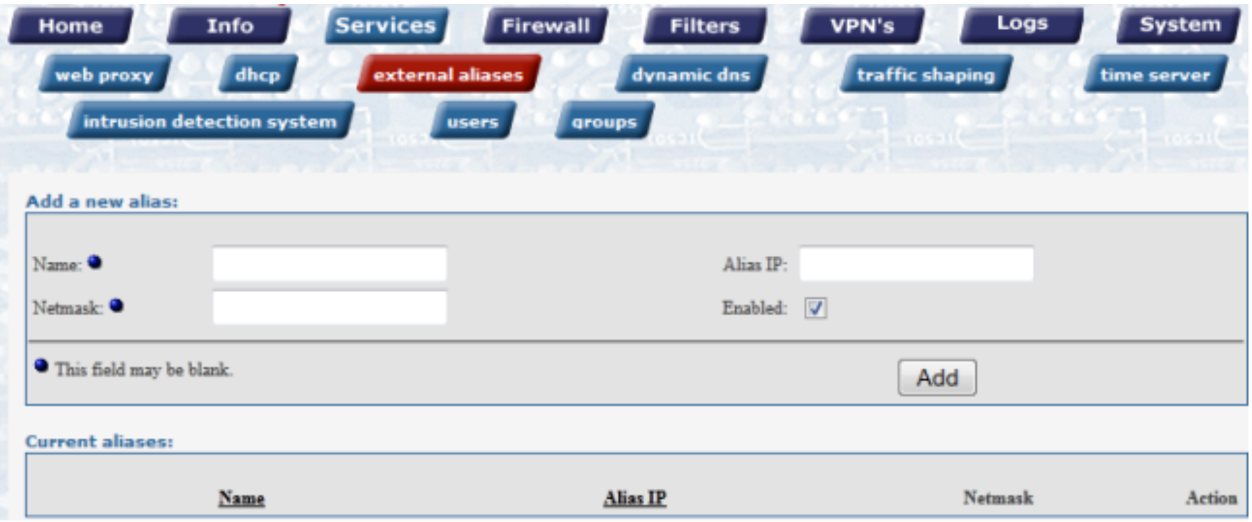
1. From the Administration Interface, click on the Services button. New sets of buttons appear.

2. Click the external aliases button. The External Aliases Page appears*.* *See 5.6:Exteral Aliases Page* on the next page.

3. Key in a name in the Name field. The Name is used to identify what the alias is used for. This field is optional**.**

4. Next, type the alias IP address in the Alias IP field. Click the Add button. Make sure `Enabled` has been checked. You can view the aliases on the same page in the Current aliases panel.

Figure 5.6: External Aliases Page



Add a new alias:

Name: ●

Alias IP:

Netmask: ●

Enabled: ☑

● This field may be blank.

Current aliases:

Name	Alias IP	Netmask	Action

Dynamic DNS

Dynamic DNS allows the administrator to assign a Fully Qualified Domain Name to the NetSentron using a third party Dynamic DNS service. This makes it easier to find the NetSentron using its name instead of an IP Address. There is a small program on the NetSentron that will send a message to the DNS service each time the NetSentron receives a new address. In turn the DNS service will update DNS servers on the Internet with the new address of the NetSentron. This is a handy tool for remote administration or creating VPNs on a NetSentron with dynamic addresses.

Setting up a Dynamic DNS Name (Hostname)

1. Starting from the Administration Interface, click on the Services button. New sets of buttons appear.

2. Click the dynamic dns button.
   The Dynamic DNS page appears (*See Figure 5.7: Dynamic DNS* – The Dynamic DNS page has been divided into two separate panels. The top panel, `Add a Host`, is used to add a new host name. The lower

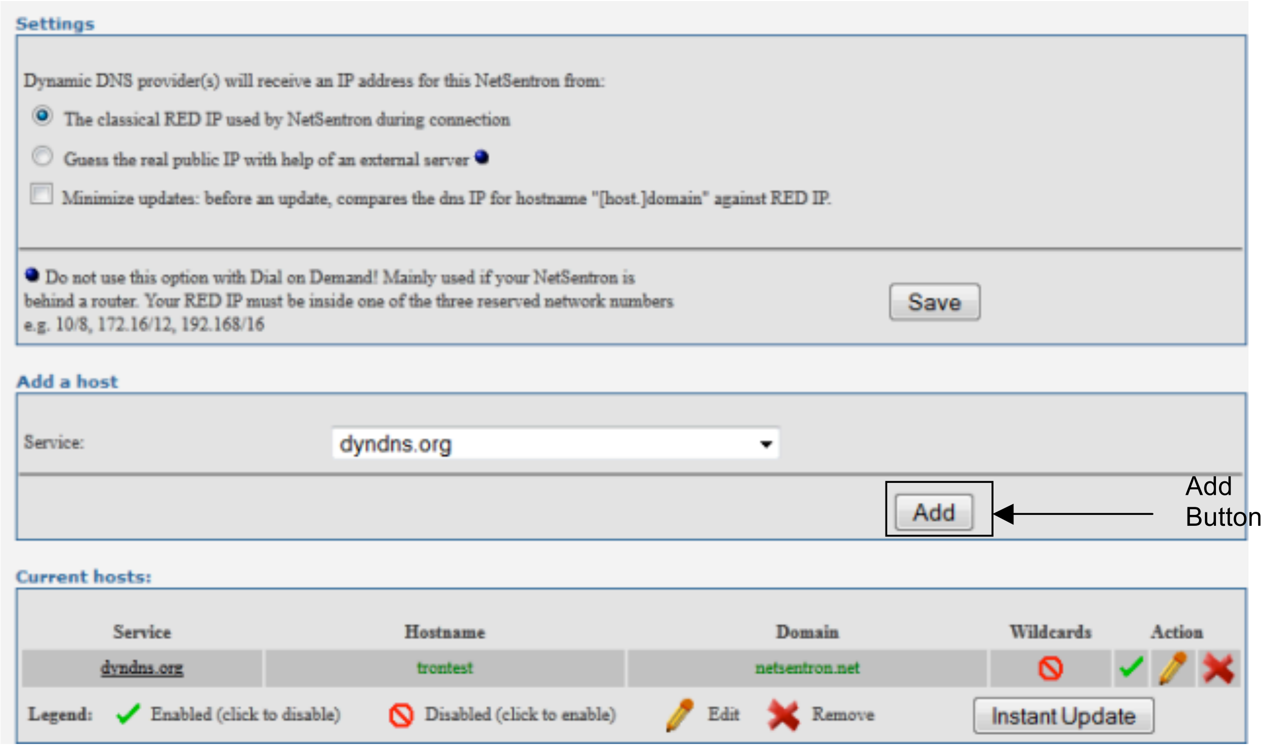
section is used to view, edit and remove existing host names. To add a new host you will be using the Add a host panel.

3. Fill in the following fields: Service, Hostname, Domain, Wildcards.

Service	Click on the drop down menu. You are given a list of Dynamic DNS Service Providers. Select the one you have an active account with.
Hostname	The name of the account. i.e. YourCompanyName
Domain	Key in the domain you selected when you set up your account with your Dynamic DNS Service Provider.
Wildcards	Checking this option will allow for the acceptance of any hostname requests for your account.

You can view your host name in the Current Hosts panel located on the same page. *See Figure 5.8: Dynamic DNS- Current Hosts Display* on the next page.

Figure 5.7: Dynamic DNS – Adding A Host



Settings

Dynamic DNS provider(s) will receive an IP address for this NetSentron from:

● The classical RED IP used by NetSentron during connection

○ Guess the real public IP with help of an external server ●

□ Minimize updates: before an update, compares the dns IP for hostname "[host.]domain" against RED IP.

● Do not use this option with Dial on Demand! Mainly used if your NetSentron is behind a router. Your RED IP must be inside one of the three reserved network numbers e.g. 10/8, 172.16/12, 192.168/16

Add a host

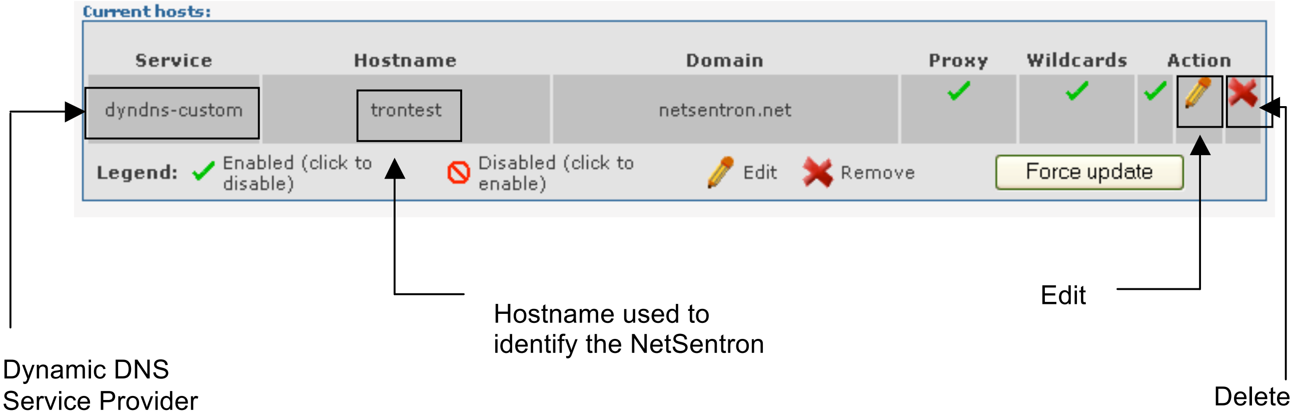
Service: dyndns.org

Current hosts:

Service	Hostname	Domain	Wildcards	Action
dyndns.org	trontest	netsentron.net	⦸	✓ ✎ ✖

Legend: ✓ Enabled (click to disable) ⦸ Disabled (click to enable) ✎ Edit ✖ Remove

Figure 5.8: Dynamic DNS – Current Hosts Display



Current hosts:

Service	Hostname	Domain	Proxy	Wildcards	Action
dyndns-custom	trontest	netsentron.net	✓	✓	✓ ✎ ✗

Legend: ✓ Enabled (click to disable) 🚫 Disabled (click to enable) ✎ Edit ✗ Remove

Dynamic DNS Service Provider

Hostname used to identify the NetSentron

Edit

Delete

Editing a Hostname

1. Starting from the Administration Interface, click on the Services button. New sets of buttons appear.

2. Click the dynamic dns button. The Dynamic DNS page appears. Click on the ✎ icon located next to the hostname you want to edit. The details for hostname are listed above (similar to adding).

NOTE

The address you are editing is highlighted yellow.

3. Make the required changes and then click the Update button. You can view the changes in the Current Hosts panel.

Removing a Hostname

1. Starting from the Administration Interface, click on the Services button. New sets of buttons appear.

2. Click the dynamic dns button. The Dynamic DNS page appears. Click on the ✗ icon located next to the hostname you want to remove.

Traffic Shaping

Traffic shaping allows one to control the amount of bandwidth that the different kinds of traffic use on the NetSentron. To enable this feature, you first need find out what your upstream and downstream bandwidth is on your DSL modem or Cable modem and subtract 5% from those values.

The following is an example of how you would configure your Upstream and Downstream bandwidth:

You are using a modem that has 640 Kbits Upload speed, and 2.5 Megabit download speed.

Subtract 5% from your upstream bandwidth and your downstream bandwidth.

NOTE
You must convert the Megabits into Kilobits.
1 Megabit= 1000 Kilobits
(The 2.5 Megabits comes out to approximately 2500 Kbits)

You have 608Kbits upload speed (640Kbit x 0.05= 32; 640-32= 608) and 2375 Kbits downstream speed (2500 x0.05= 125; 2500-125=2375).

These are the Kbits that you enter in the Settings panel on the Traffic Shaping page seen in Figure 5.9.

(You took 5% off the maximum, as a rough number to make up for inaccuracies such as slow modems.)

Adding A Service

1. From the Administration Interface, click on the Services button. New sets of buttons appear. Click on the traffic shaping button. The Traffic Shaping page appears. *See Figure 5.9: Traffic Shaping Page* on the next page.

2. In the setting panel key in the Downlink speed and Uplink speed. (Use the example of settings up bandwidth constraints on the previous page to configure your upstream and downstream bandwidth)

3. Once you have entered the settings check the enable box and then click SAVE button.

4. Next, you will need to define the traffic that is allowed, and how much priority to give each type of traffic. See the example of distributing bandwidth priority below.

Example of Distributing Bandwidth Priority

If you had a bunch of people surfing the web (http port 80), an FTP server (port 21), and some VOIP phones (port 1720) and you wanted a nice clear conversations on the VOIP phone you will assign most bandwidth to the VOIP phone. Then you would assign some bandwidth to web surfing. You would want to keep the FTP to a minimal amount, as you do not want all of the bandwidth chewed up

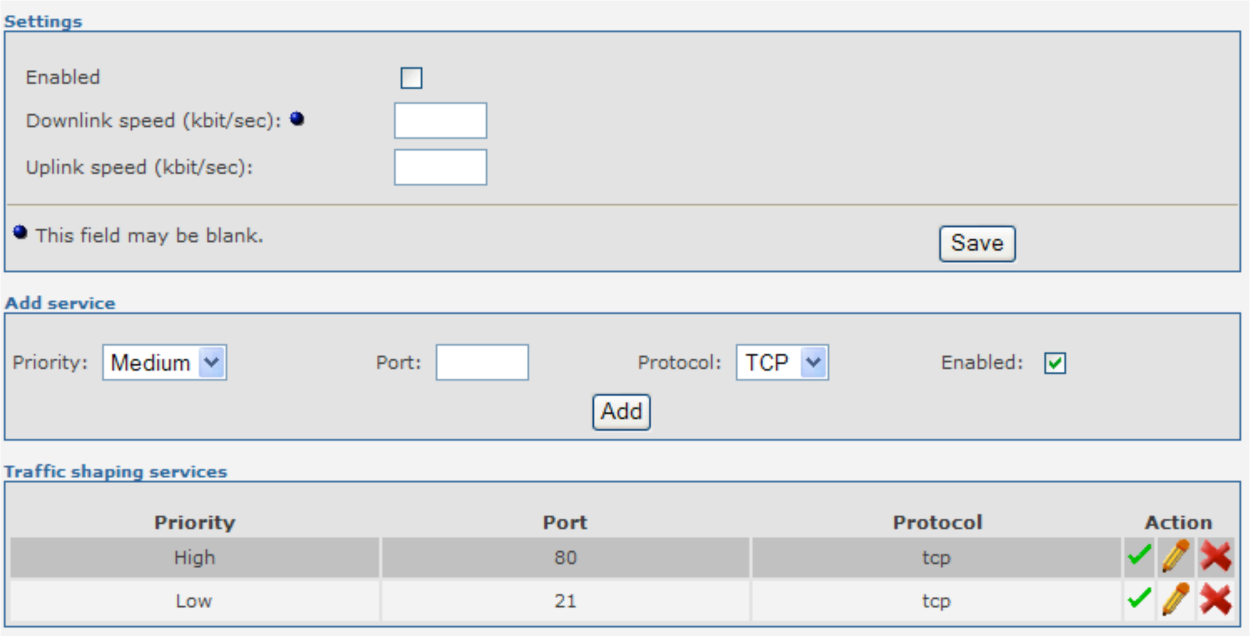
NOTE: The following instructions are using the setting for the above example.

5. In the `Add Service` panel, using the drop down menu select ***TCP*** for Protocol. From the Priority menu select ***High.*** In the Port field enter ***1720*** for port, and then click the Add button. This will give port 1720 a higher priority than any other entries. Next, select ***TCP*** again from the drop down menu***.*** This time select ***Medium*** from the Priority menu and enter ***80*** in the Port field. Click the Add button. This would give your surfers a decent amount of bandwidth, but the VOIP phone on port 1720 would get priority over surfing, keeping the phone conversation nice and clear.

6. Finally you want to limit FTP (port 21) and make sure that it has the lowest priority. Again, select ***TCP*** from the drop down menu. Now, select ***Low*** from the Priority menu and then enter ***21*** in the Port field. Click the Add button. You have now given web surfing and VOIP connections a higher priority than FTP.

8. You can use the Edit button to make changes or use the Remove button to remove a service.

Figure 5.9: Traffic Shaping



Settings

Enabled	□
Downlink speed (kbit/sec): ●	
Uplink speed (kbit/sec):	

● This field may be blank.

Add service

Priority: Medium Port: Protocol: TCP Enabled: ☑

Traffic shaping services

Priority	Port	Protocol	Action
High	80	tcp	✓ ✎ ✗
Low	21	tcp	✓ ✎ ✗

Time Server

The Time Server Administration page gives you the ability to set up the NetSentron internal clock. Setting up the Time Server allows the NetSentron to go to a known Time Server on the Internet. From there the NetSentron can adjust its internal clock accordingly. Making sure the NetSentron internal clock is set correctly gives the administrator the ability to view all of the logs correctly.

1. From the Administration Interface, click on the Services button. New sets of buttons appear.

2. Click the time server button. The Time Server page appears. *See Figure 5.10: Time Server* Page on page 79. The Time Server page has been divided into four separate panels, Time zone, Time and Date, Network time retrievals and Network timeservers. See the list below for a description of the fields provided on this page.

Timezone:

Timezone	Select the time zone you are working in by clicking the drop box. You are given a list of different time zones to choose from.

Time and Date:

Set	Check set to enable the time and date changes.
Time	Use the drop down menus to select your current time.
Date	Use the drop down menu to select the month, day and year.

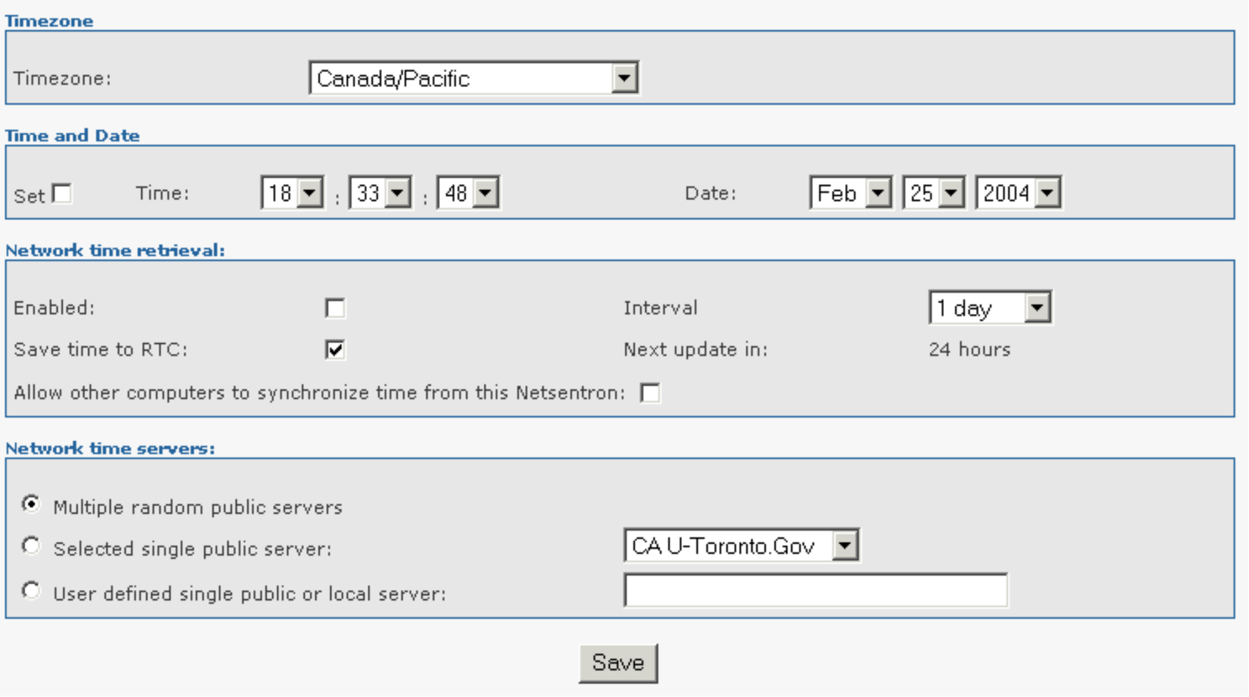
Network time retrieval:

Enabled	If selected network time retrieval is turned on.
Interval	Allows the administrator to specify the instances for time retrieval. Use the drop down menu to make the selection.
Save time to RTC	Enabling these features allows the time to be saved to the hardware clock when updating.
Allow other computers to synchronize time from this NetSentron	Checking this box allows the NetSentron to act as a timeserver for computers on the internal (green) network. For this to work you will need an NTP client installed on each computer.

Network time servers:

Multiple random public servers	Allows the NetSentron to choose from a variety of public servers. It is recommended to use this setting.
Selected single public server	Gives you the option to choose a single server from the drop down menu.
User defined single public or local server	Allows the administrator to enter a defined time server. Key in the server IP address or the FQDN.

Figure 5.10: Time Server Page



Timezone

Timezone: Canada/Pacific

Time and Date

Set □ Time: 18 : 33 : 48 Date: Feb 25 2004

Network time retrieval:

Enabled: □ Interval 1 day

Save time to RTC: ☑ Next update in: 24 hours

Allow other computers to synchronize time from this Netsentron: □

Network time servers:

● Multiple random public servers

○ Selected single public server: CA U-Toronto.Gov

○ User defined single public or local server:

Save

Intrusion Detection System (IDS)

The Intrusion Detection System page gives the administrator the option to have either the internal (LAN) or external (WAN) Intrusion Detection Systems turned on or off. To view any logs generated by the IDS go to *Viewing Intrusion Detection System Logs*.

Turning IDS On/Off

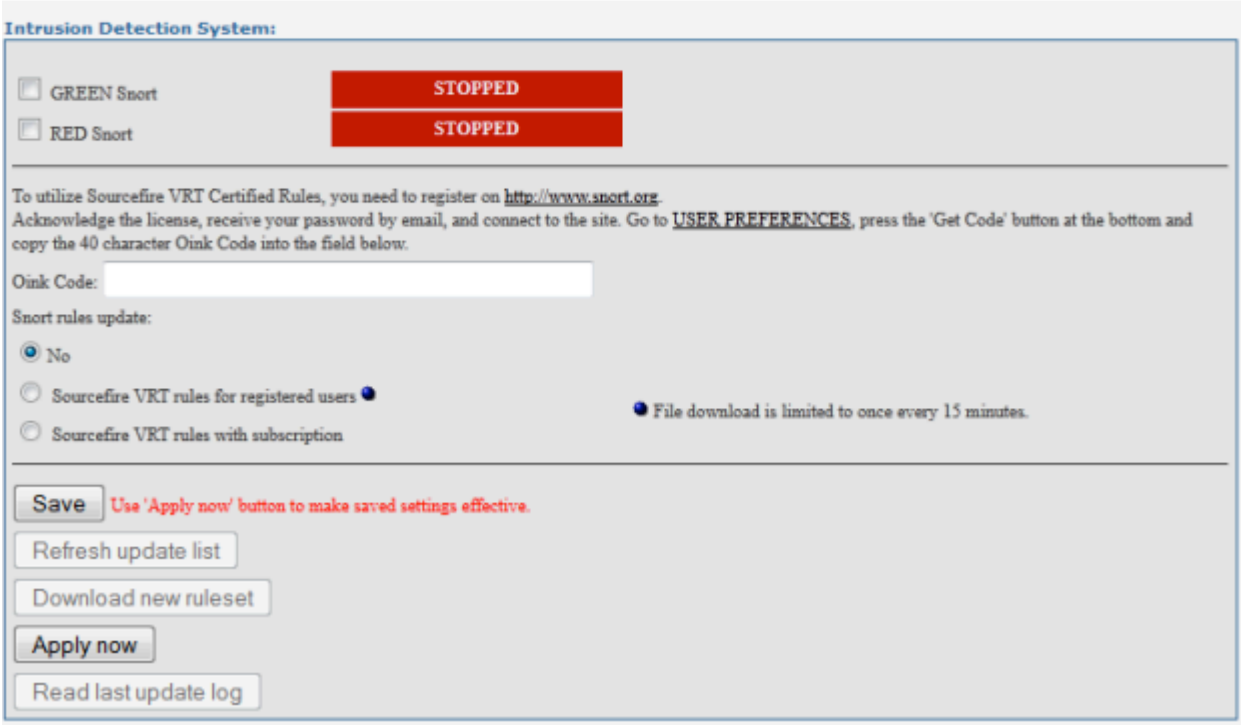
1. From the Administration Interface, click on the Services button. New sets of buttons appear.

2. Click the intrusion detection system button. The Intrusion Detection System page appears as Figure 5.11 shows on the next page.

3. Put a check mark next to the system you want turned on, and then click the Save button. You also have the option to update the sort rules. Follow the instructions listed in the Intrusion Detection System

panel.

Figure 5.11: Intrusion Detection System Page



Intrusion Detection System:

☐ GREEN Snort STOPPED

☐ RED Snort STOPPED

To utilize Sourcefire VRT Certified Rules, you need to register on http://www.snort.org. Acknowledge the license, receive your password by email, and connect to the site. Go to USER PREFERENCES, press the 'Get Code' button at the bottom and copy the 40 character Oink Code into the field below.

Oink Code:

Snort rules update:

● No

○ Sourcefire VRT rules for registered users ●

○ Sourcefire VRT rules with subscription

● File download is limited to once every 15 minutes.

Use 'Apply now' button to make saved settings effective.

Users

The NetSentron Users administration page gives the administrator the ability to give each user attached to the network a user name and password that would allow them access to the Internet (the user would be prompted for a user name and password when opening up a browser). Using this feature gives the administrator the ability to see where and when each user is surfing the net.

If someone has abused their Internet privileges the administrator can deny them access. For this feature to work the NetSentron Authentication must be enabled, the user must be assigned to a group and the web proxy settings for the browser need to be changed to allow for User Authentication.

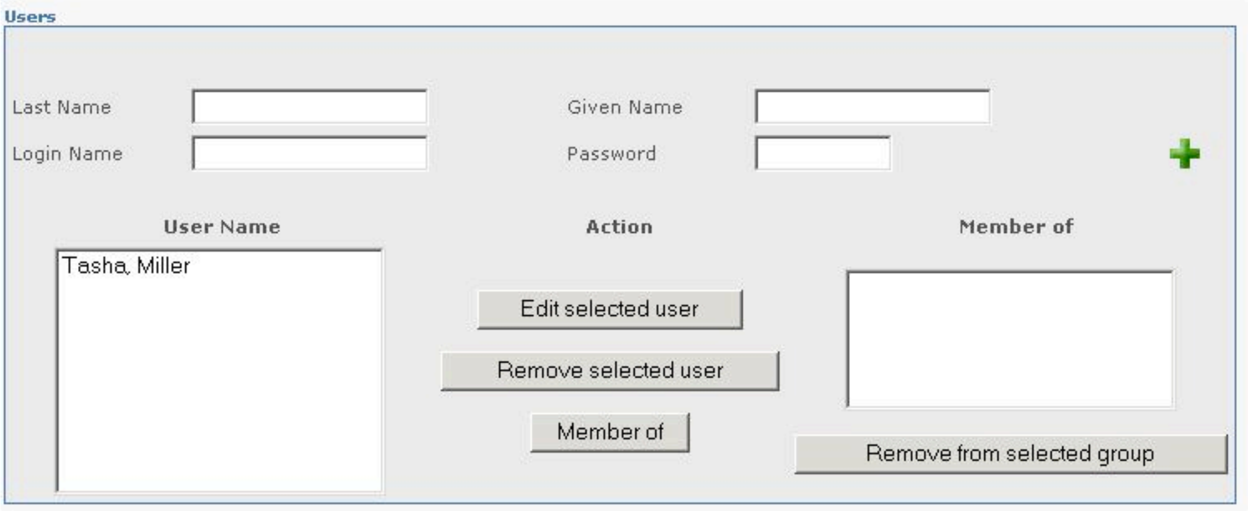
Creating a new User

The following are instructions on how to add a new user to the Authentication list.

1. From the Administration Interface, click on the Services button. New sets of buttons appear.

2. Click on the users button. The `Users` Administration page appears. *See Figure 5.12: Users Administration page below*.

Figure 5.12: Users Administration page



3. In the `Last Name` field, key in the last name of the user (using lower

case).

4. In the `Given Name` field, key in the first name of the user (using lower case).

5. In the `Login Name` field, key in a name the user will be using when logging onto the Internet (using lower case).

6. In the `Password` field, key in a password (using lower case).

7. Once all the fields have been keyed in, click the ✚ icon. A message panel appears at the top of the page and the new user should be listed in the `User Name` box. *See Figure 5.13 below*.

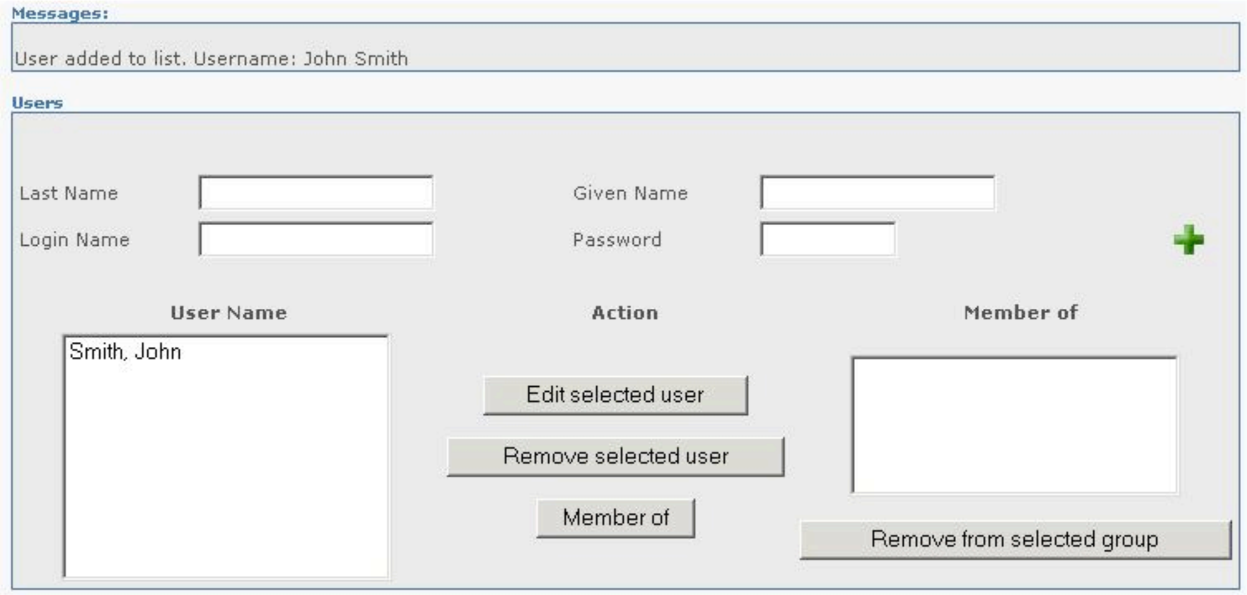
NOTE

For User Authentication to work you must do the following:

- Make sure the User has been assigned to a group. See *Adding a User to a Group on page 90*
- NetSentron Authentication has been enabled. See *Configuring Web Proxy located on page 67.*
- Change the browsers Proxy Server settings for each pc. *See Changing Your Browsers Web Proxy Settings to allow for User on page 88.*

To view the web access logs for individual users see the section on *Viewing the Web Access Logs on page 209.*

Figure 5.13: User Added



Messages:

User added to list. Username: John Smith

Users

Last Name		Given Name	
Login Name		Password	

User Name: Smith, John

Editing a User

1. From the Administration Interface, click on the Services button. New sets of buttons appear.

2. Click on the users button. The Users Administration page appears.

3. In the User Name box click on the user you want to make the changes to. Once the user name is highlighted click the Edit selected user button. The name has been removed from the box and all the fields above have been filled.

4. Make the appropriate changes. For example if you want to change the password, clear the field and key in a new password.

5. Once the changes have been made, click on the ✚ icon. The changes have been recorded and the name is re-entered in the User Name box. The message panel will appear stating that the User has been updated.

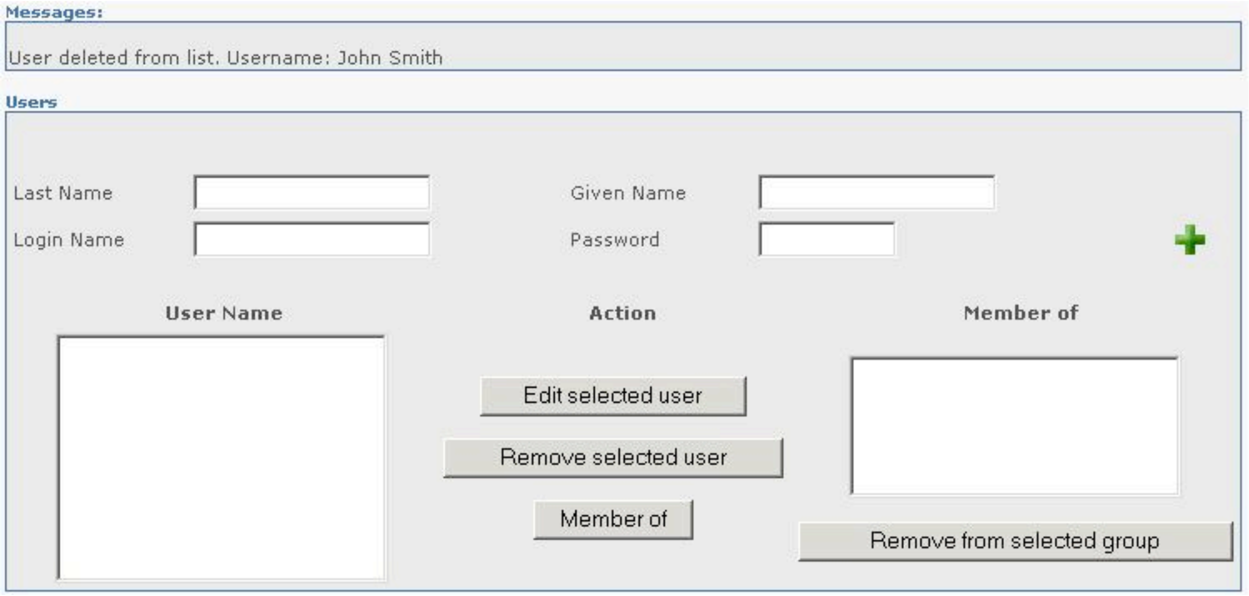
Removing a User

1. From the Administration Interface, click on the Services button. New sets of buttons appear.

2. Click on the users button. The Users Administration page appears.

3. In the User Name box click on the user you want to make remove. Once the user name is highlighted click the Remove selected user button. A message panel appears at the top of the page stating that the user has been removed from the list. *See Figure 5.14 on the next page.*

Figure 5.14: User Deleted



Messages:

User deleted from list. Username: John Smith

Groups

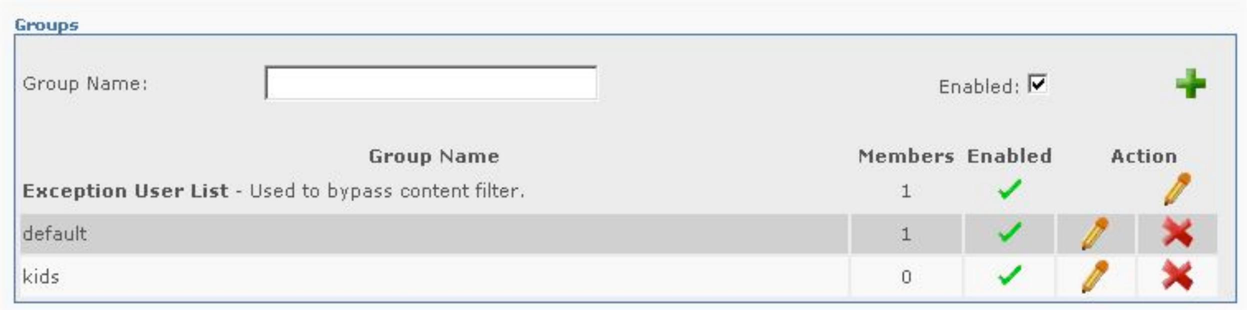
The Groups Administration page allows the Administrator to group together users. Using groups makes it easier to the administrator to maintain all the users. If a user has not been assigned to a group User Authentication will not work.

Creating Groups

1. From the Administration Interface, click on the Services button. New sets of buttons appear.

2. Click on the groups button. The Groups Administration page appears. *See Figure 5.15:Groups Administration page below.*

Figure 5.15 Groups Administration page



Groups

Group Name: Enabled: ☑ ✚

Group Name	Members	Enabled	Action	
Exception User List - Used to bypass content filter.	1	✓		✎
default	1	✓	✎	✗
kids	0	✓	✎	✗

3. In the Group Name field, key in a name for the group you are creating. Note: If you don't want the new group enabled, just de-select the enabled box.

4. Click on the ✚ icon to add the group. The new Group Name has been added to the list

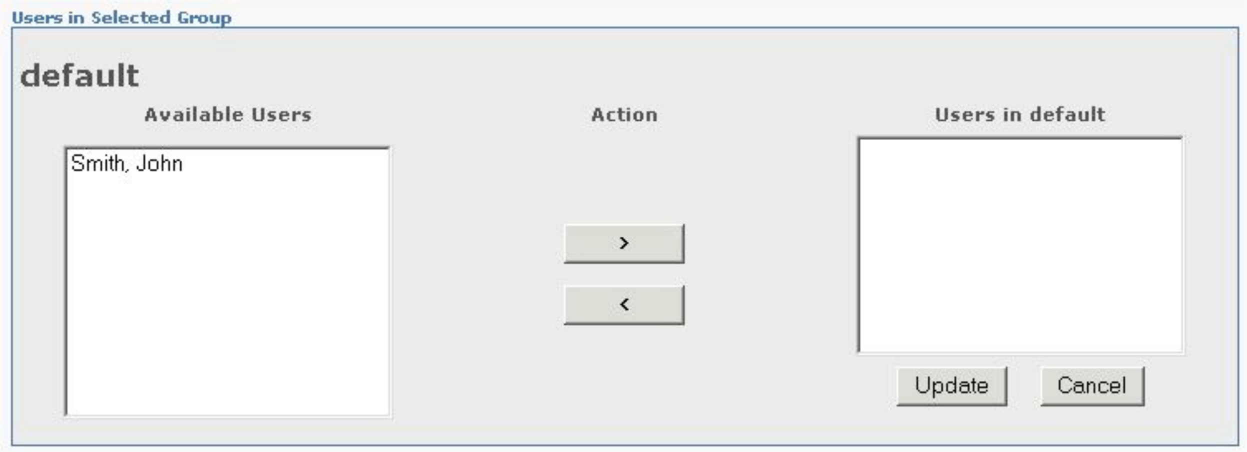
Adding a User to a Group

1. From the Administration Interface, click on the Services button. New sets of buttons appear.

2. Click on the groups button. The Groups Administration page appears. See *Figure 5.15: Groups Administration.*

3. Click on the ✎ icon associated with the group you want to add the user to. The Users in `Selected Group` panel appears. See *Figure 5.16: Users in Selected Group panel below.*

Figure 5.16: Users in Selected Group panel



Users in Selected Group

default

Available Users	Action	Users in default
Smith, John		

4. Click on the user you want to add located in the `Available Users` box. The user name should be highlighted.

5. Next, click on the > button. The user you selected has been moved to the `Users` in '`groupname`' box.

6. Click on the Update button to confirm. You are returned to the Group Administration page. You should see a message confirming that the group has been updated.

Removing a User from a Group

1. From the Administration Interface, click on the Services button. New sets of buttons appear.

2. Click on the groups button. The Groups Administration page appears. *See Figure 51: Groups Administration page above.*

3. Click on the ✎ icon associated with the group you want to remove the user from. The `Users in Selected Group` panel appears. *See Figure 52: Users in Selected Group panel above.*

4. Click on the user you want to remove in the located in the `Users` in '`groupname`' box. The user name should be highlighted.

5. Next, click on the < button. The user you selected has been moved from the `Users` in '`groupname`' box to the `Available Users` box.

6. Click on the Update button to confirm. You are returned to the Group Administration page. You should see a message confirming that the group has been updated.

Removing a Group

1. From the Administration Interface, click on the Services button. New sets of buttons appear.

2. Click on the groups button. The Groups Administration page appears. *See Figure 5.15: Groups Administration* on page 85.

3. Click on the ✖ icon associated with the group you want to remove.

Chapter 6 Filters

Content Filtering

The NetSentron can filter language and phrases that are often associated with pornography and objectionable subject matter. The URL and domain filtering is able to handle huge lists and is significantly faster than other filtering systems.

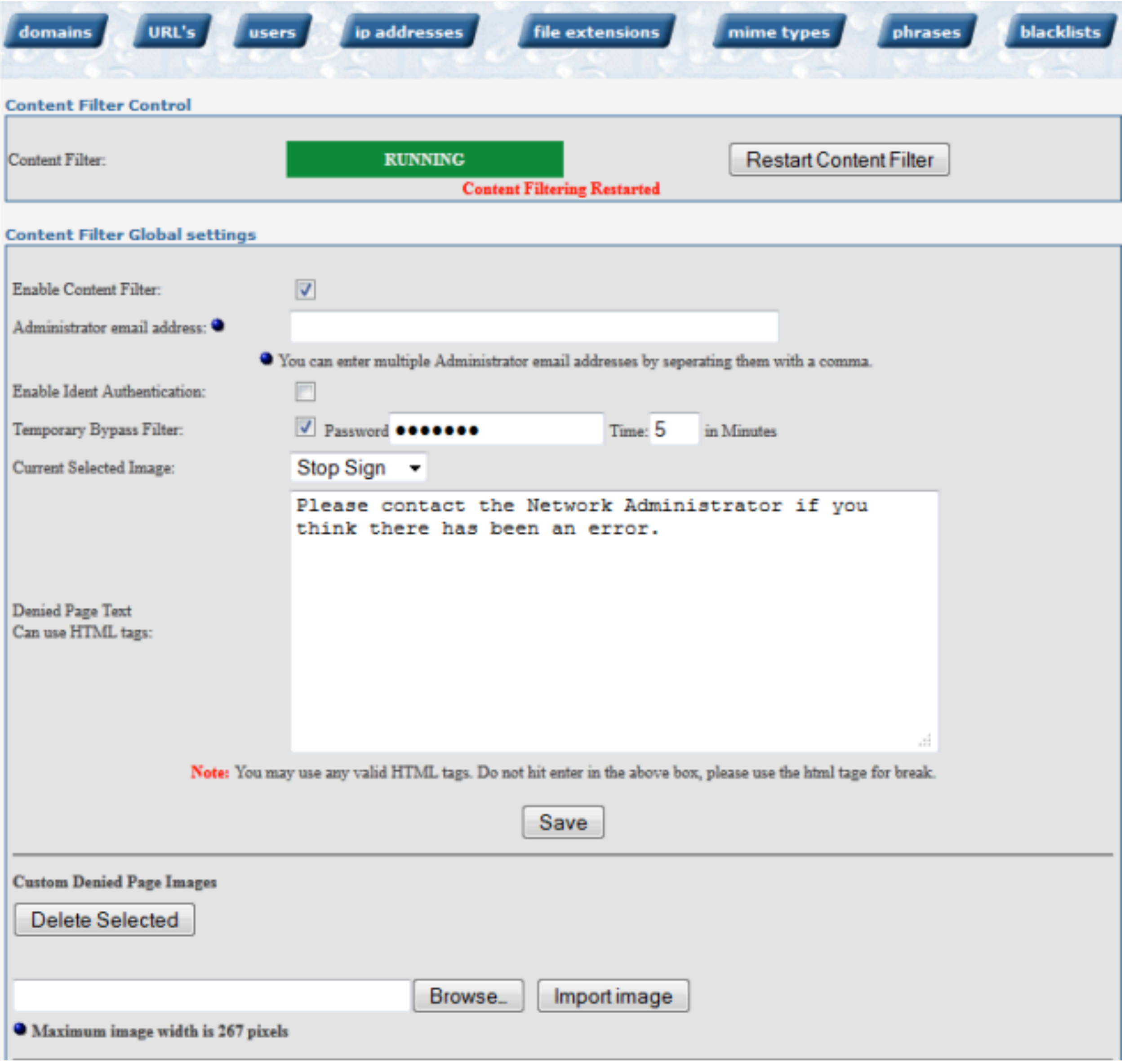
This system is designed to be completely flexible to allow the administrator to adjust the settings to suit their filtering requisites. The administrator can also set the parameters as severe or as unobtrusive as needed.

The default settings for the NetSentron filtering program filters the actual content of pages based on several methods, which include phrase matching, PICS filtering and URL filtering. The content phrase filtering checks for pages that may have foul words (which have been pre-configured for what a primary school may require); however, the administrator has the option to alter these settings.

Global Settings

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the content filter page appears. To make changes to the global settings you will be using the Content Filter Global Settings panel. *See Figure 6.1: Content Filter – Content Filter Global Settings panel* on the next page.

Figure 6.1 : Content Filter – Content Filter Global Settings Panel



Content Filter Control

Content Filter: RUNNING

Content Filtering Restarted

Content Filter Global settings

Enable Content Filter: ☑

Administrator email address: ●

● You can enter multiple Administrator email addresses by seperating them with a comma.

Enable Ident Authentication: □

Temporary Bypass Filter: ☑ Password ••••••• Time: 5 in Minutes

Current Selected Image: Stop Sign

Denied Page Text
Can use HTML tags:

```
Please contact the Network Administrator if you
think there has been an error.
```

Note: You may use any valid HTML tags. Do not hit enter in the above box, please use the html tage for break.

Custom Denied Page Images

● **Maximum image width is 267 pixels**

2. Make your changes to the following fields:

Enable Content Filter	Check the box to turn on the Content Filter system. Uncheck to turn off.
Administrators email address	The email address keyed in here, will be displayed on the blocked page.
Enable Ident Authentication	Select this option if you are running Ident Client. This allows the NetSentron to identify the users on the LAN by their login name. The username will then show up in the Web Access Logs *(See Viewing the Web Access Logs on page* ***201****)* making is simpler for the administrator to match user names rather than matching IP addresses to a computer.
Temporary Bypass Filter	Check the box to turn on Temporary Bypass Filter. Key in a password and select the length of time that the bypass will work for. The Bypass gives the administrator the ability to allow a certain IP address to bypass the Content Filter System for the selected time limit.
Current Selected Image	When a site has been denied access the user will see a picture. This option allows the administrator to use their own images. By default you are given two images to choose from. You also have the option to upload your own image to display. Use the [Browse...] button to select an image and then use the [Import image] button to upload it to the NetSentron. To make sure the Custom Denied image is selected click on the check box next to it.

3. Once you have selected your settings, click on the [Save] button. The

Content Filter is automatically restarted.

Adding Content Filter Rules

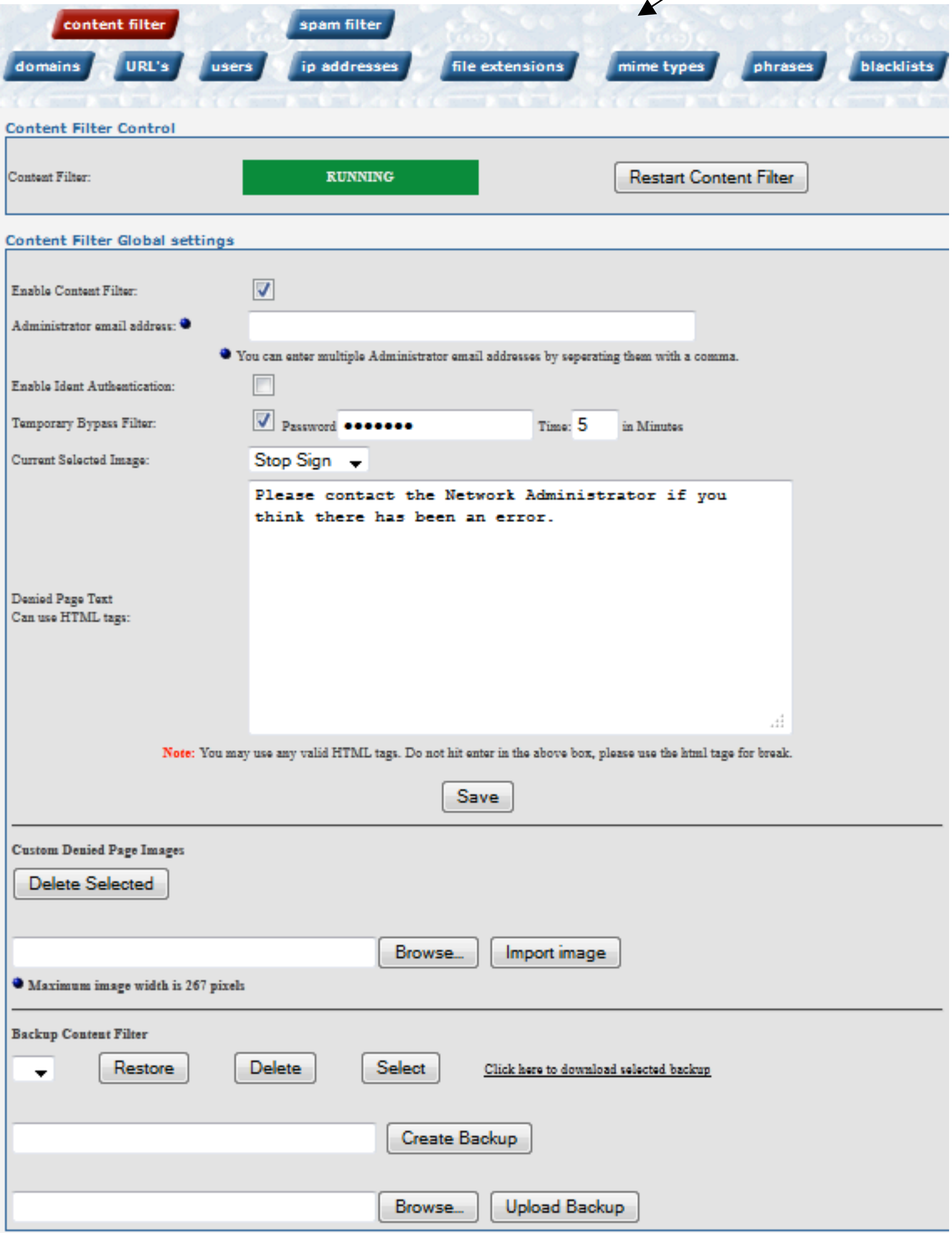
1. From the Administration Interface, click on the Filters button. New sets of buttons appear.

2. Click the content filter button. The Content Filter Administration page appears*. See Figure 6.2: Content Filter Page.* Simply click the button to enable the content filter system. The Content Filter Control gives the administrator the ability to restart content filtering

3. To make any changes to the filter settings, click the button of a category to the top of the page. A new page will open allowing the administrator edit the existing data.

Figure 6.2 : Content Filter Page

Click the appropriate link to make any changes



Content Filter Control

Content Filter: RUNNING

Content Filter Global settings

Enable Content Filter: ☑

Administrator email address: ●

● You can enter multiple Administrator email addresses by seperating them with a comma.

Enable Ident Authentication: □

Temporary Bypass Filter: ☑ Password ●●●●●●● Time: 5 in Minutes

Current Selected Image: Stop Sign

Denied Page Text
Can use HTML tags:

```
Please contact the Network Administrator if you
think there has been an error.
```

Note: You may use any valid HTML tags. Do not hit enter in the above box, please use the html tags for break.

Custom Denied Page Images

● Maximum image width is 267 pixels

Backup Content Filter

Click here to download selected backup

Editing Banned URL Expressions

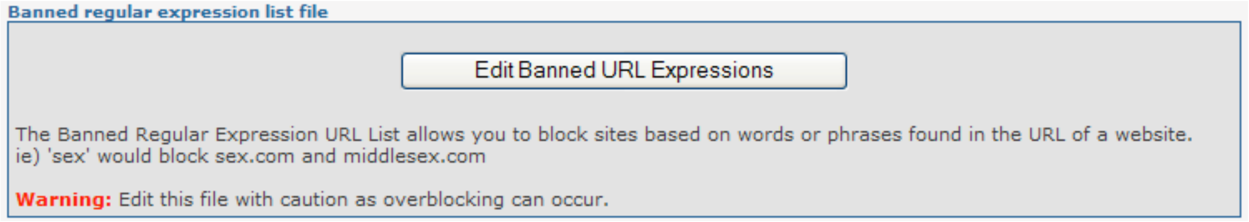
Banned URL Expressions are expressions or words found in the URL of a website. If a word is present, then the entire site is blocked. Ie) if you wanted to block proxy sites, you would add the word proxy to the banned URL expressions. If any page came up with the word proxy anywhere in the URL, the page would be blocked.

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the content filter page appears. To edit banned URL Expressions, click on the Edit Banned URL Expressions button located in the Banned regular expression list file panel. *See Figure 6.3: Content Filter – Banned regular expression list file panel below.*

2. Make your changes. **Warning**: Edit this file with caution as over blocking can occur.

3. Click on the Update Banned URL Expressions button to save your changes. The content filter restarts automatically.

Figure 6.3: Content Filter – Banned Regular Expression List File Panel



Banned regular expression list file

Edit Banned URL Expressions

The Banned Regular Expression URL List allows you to block sites based on words or phrases found in the URL of a website.
ie) 'sex' would block sex.com and middlesex.com

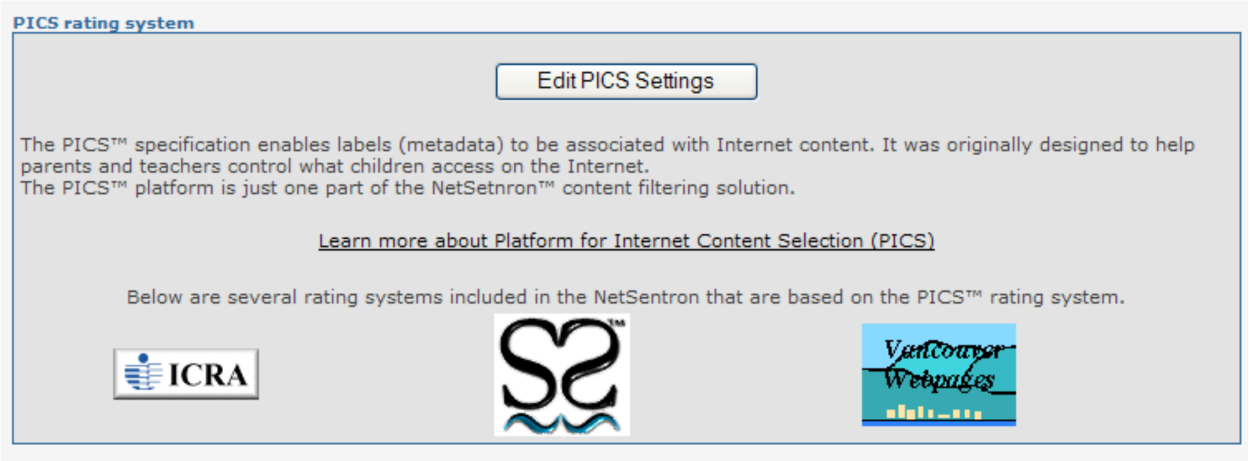
Warning: Edit this file with caution as overblocking can occur.

Editing PICS Settings

PICS—Platform for Internet Content Selection—is an Internet protocol to allow ratings to be transferred and understood across the Internet. This is an older rating system that is not always followed by websites.

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the Content Filter Control page appears. To edit PICS settings, click on the Edit PICS Settings button located in the PICS rating system panel. *See Figure 6.4: Content Filter – PICS rating system panel.*
2. Make your changes. To learn more about PICS click on the link in the center of the panel.

Figure 6.4: Content Filter – PICS Rating System Panel



PICS rating system

Edit PICS Settings

The PICS™ specification enables labels (metadata) to be associated with Internet content. It was originally designed to help parents and teachers control what children access on the Internet.
The PICS™ platform is just one part of the NetSetnron™ content filtering solution.

Learn more about Platform for Internet Content Selection (PICS)

Below are several rating systems included in the NetSentron that are based on the PICS™ rating system.

3. Click on the Update PICS Settings button to save your changes. The content filter restarts automatically.

Backing Up the Content Filter

You can back up the content filter separately from the main backup of the NetSentron. The purpose of this is to allow you to copy one filter setup from a NetSentron to another or set up a restore point if you want to experiment with settings.

Creating A Backup

To create a back up, enter a name (with no spaces) in the input box and then click on the **Create Backup** button. The NetSentron will start backing up your content filter. This may take a minute or two, before the page refreshes. When it does you should see the message "Backup file ##### CREATED" in red at the top of the page. Note ##### is actually the name of your file.

You should now see that the drop down list in the Backup Content Filter area has the filename you entered followed by .tgz in it. Make sure the back up file you just created is selected, and then click on the **Select** button. When screen refreshes, you should see the message indicating that you are now working with the file. You can now click on the **Click here to download selected backup** link to download your backup to your computer. Store it somewhere safe.

Restoring a Backup

To restore a backup, if it is from another NetSentron (or stored off of the NetSentron), you will need to upload it first. To do that, click on the Browse button, select your backup file and click on **Upload Backup**. Once uploaded, you should see the backup file listed in the drop down list.

To restore a backup file, make sure it is selected from the drop down list and then click on the **Select** button. You will see a message indicating the file you are now working with.

Then click on the **Restore** button. It will take a few moments to restore and you should see a message at the top of the page indicating it has been restored when done.

It is a good idea to restart the NetSentron after restoring a backup.

Deleting a Backup

To delete a backup file, first select it by clicking on the **Select** button. You will see a message indicating which file you are working with. Then click on the **Delete** button. You will see a message indicating that the selected file was deleted.

Domain Names

You can block an entire domain name such as www.proxy.net by simply entering the proxy.net part of things into the NetSentron. Any page from www.proxy.net would then be blocked. You can also whitelist, or allow unfiltered access to an entire domain in the same manner that you can block a domain.

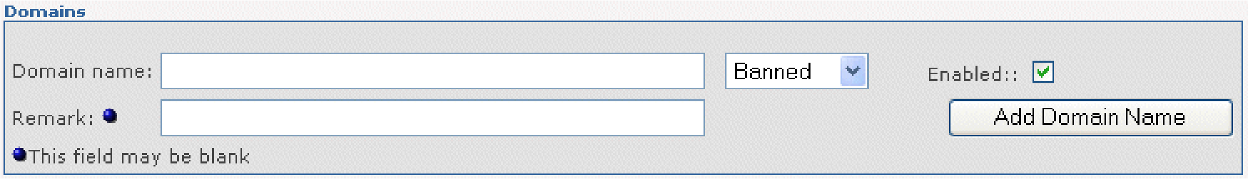
Adding Domain Names

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the content filter page appears*.*

2. Next, you will need to click on the domains button. The Domains panel appears. *See Figure 6.5: Content Filter – Domains panel.*

3. In the Domain name field, key in the domain name you want to add to the Content Filter Domain list.

Figure 6.5: Content Filter – Domains Panel



Domains

Domain name: Banned Enabled:: ☑

Remark: ● Add Domain Name

●This field may be blank

4. Next, click on the drop down menu to the right of the `Domain name` field. You are given three options: `Banned, Filtered, Exception`. See the following page for a description of each status option in the table.

NOTE

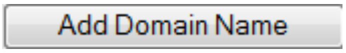
You should not put the http:// or the www at the beginning of the entries.

Banned Blocks access to the whole site.

Filtered Used for partly unblocking ALL of a site.

> **NOTE**
>
> The 'filtered' lists override the 'banned' lists. The
>
> 'exception' lists override the 'banned' lists also. The difference is that the 'exception' lists completely switches off *all* other filtering for the match. 'filtered' lists only stop the URL filtering and allow the normal filtering to work. An example off a filtered list is when in Blanket Block (whitelist) mode and you want to allow some sites but still filter as normal on their content Another example of when a filtered list used is when you ban a site but want to allow part of it.

Exception Allows access to whole site.

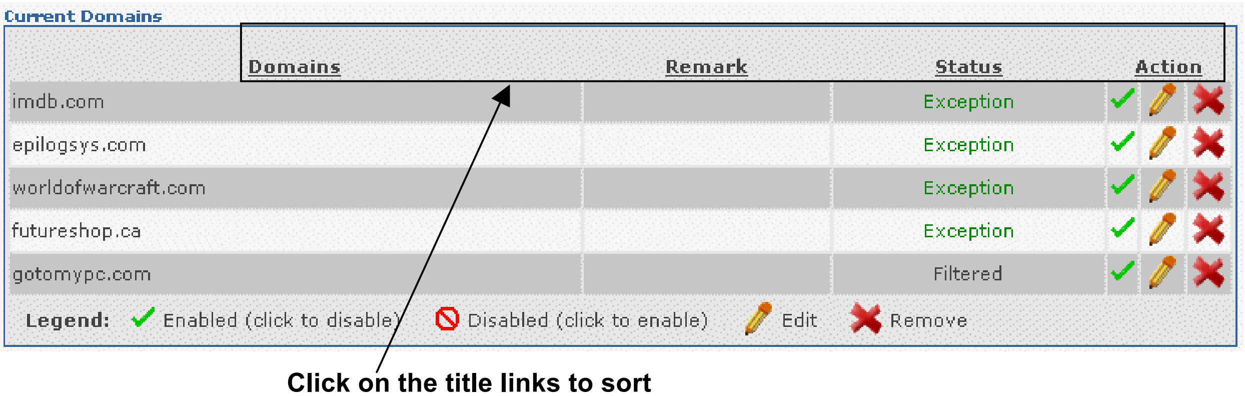
5. In the remark field you can add a comment to describe the filter you added.
6. Lastly, check the `Enabled` box. You are now ready to save the domain filter setting.
7. Click the  Add Domain Name button. The setting you added is listed in the Current Domains panel. The content filter restarts automatically.

Viewing the Current List of Domain Names

1. From the Administration Interface, click on the **Filters** button. New sets of buttons appear. By default the Content Filter Control page appears.

2. Next you will need to click on the **domains** button. The Domains page appears. See *Figure 6.6 - Content Filter - Current Domains panel* below. This panel allows you to edit, disable and delete any domain name settings. For easy look up, simply click on the title links above each column to sort alphabetically. For example to sort the list by domains, click on the Domains link.

Figure 6.6: Content Filter – Current Domains Panel



Current Domains

Domains	Remark	Status	Action
imdb.com		Exception	✓ ✎ ✗
epilogsys.com		Exception	✓ ✎ ✗
worldofwarcraft.com		Exception	✓ ✎ ✗
futureshop.ca		Exception	✓ ✎ ✗
gotomypc.com		Filtered	✓ ✎ ✗

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) ✎ Edit ✗ Remove

Click on the title links to sort each column alphabetically

Editing Domain Names

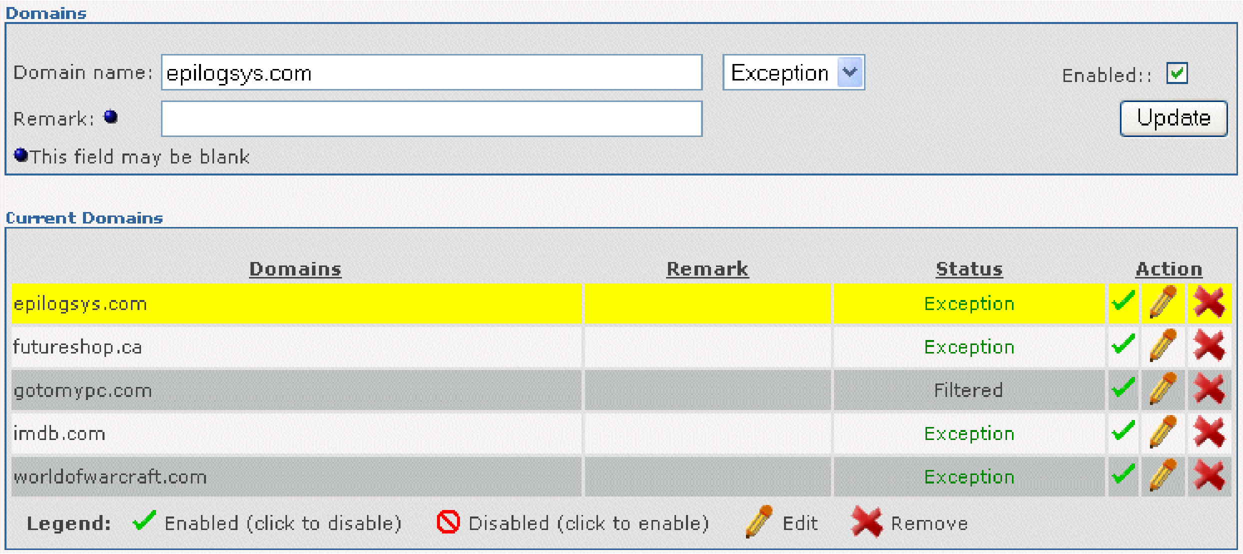
1. From the Administration Interface, click on the **Filters** button. New sets of buttons appear. By default the `Content Filter Control` page appears.

2. Next, you will need to click on the **domains** button. The `Domains` page appears. The second panel is the `Current Domains` panel.

> **NOTE**
>
> For easy look up, simply click on the title links above each column to sort alphabetically.

3. Click the ✎ icon associated with the domain name you want to edit. The details for that domain are placed in the `Domains` panel. *See Figure 6.7: Content Filter – Edit Domain Names, below.* The domain you are editing is highlighted yellow.

Figure 6.7: Content Filter – Edit Domain Names



Domains

Domain name: epilogsys.com | Exception | Enabled:: ☑

Remark: ● | Update

●This field may be blank

Current Domains

Domains	Remark	Status	Action
epilogsys.com		Exception	✓ ✎ ✖
futureshop.ca		Exception	✓ ✎ ✖
gotomypc.com		Filtered	✓ ✎ ✖
imdb.com		Exception	✓ ✎ ✖
worldofwarcraft.com		Exception	✓ ✎ ✖

Legend: ✓ Enabled (click to disable) ⃠ Disabled (click to enable) ✎ Edit ✖ Remove

4. Make the appropriate changes and then click the Update button. You can view the changes you made in the `Current Domains` panel.

Removing Domain Names

1. From the Administration Interface, click on the **Filters** button. New sets of buttons appear.

2. Next, you will need to click on the **domains** button. The `Domains` page

appears. The second panel is the `Current Domains` panel. *See Figure 6.6: Content Filter – Current Domains*. For easy look up, simply click on the title links above each column to sort alphabetically.

3. Click the ✖ icon associated with the domain name you want to remove. Once you click the `delete` icon, the domain name is removed automatically.

Disabling/Enabling Domain Names

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.

2. Next, you will need to click on the domains button. The `Domains` page appears. The second panel is the `Current Domains` panel. *See Figure 6.6: Content Filter – Current Domains panel,* on page 82. **Note:** For easy look up, simply click on the title links above each column to sort alphabetically.
3. Click the ✓ icon associated with the domain name you want to disable. The ✓ icon as been replaced with a 🚫. To enable the domain name, simply click on the 🚫 icon and the ✓ icon is returned and your domain name is enabled.

URLs

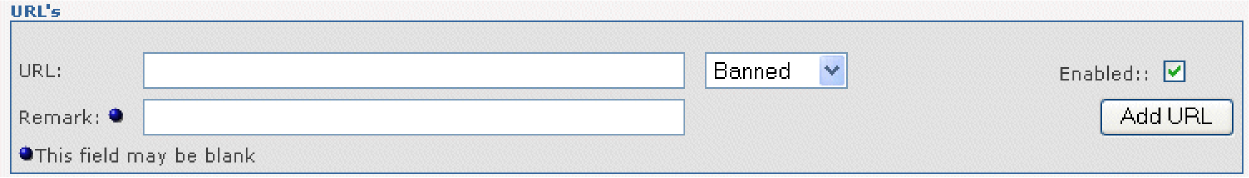
The URLs page allows you to enter specific URLs or pages into the NetSentron that can be blocked or whitelisted. This is handy for allowing access (or denying access) to specific pages in a website.

Adding URLs

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the `Content Filter Control` page appears.

2. Next, you will need to click on the URL's button. The `URLs` panel appears. *See Figure 6.8: Content Filter – URLs panel*.

Figure 6.8: Content Filter – URLs Panel



Banned

Enabled:: ☑

3. In the URL field, key in the URL name you want to add to the Content Filter URL list.

4. Next, click on the drop down menu to the right of the URL field. You are given three options: Banned, Filtered, Exception. See below for a description of each status option.

Banned

This allows you to block specific parts of a site rather than the whole site.

Filtered

Used for partly unblocking *part* of a site.

> **Note:** The 'filtered' lists override the 'banned' lists. The 'exception' lists override the 'banned' lists also. The difference is that the 'exception' lists completely switches off **all** other filtering for the match. 'Filtered' lists only stop the URL filtering and allow the normal filtering to work. An example off a filtered list is when in Blanket Block (whitelist) mode and you want to allow some sites but still filter as normal on their content. Another example of when a filtered list used is when you ban a site but want to allow part of it.

Exception

URLs that have particular pages that you allow access to.

5. In the remark field you can add a comment to describe the filter you added.

6. Lastly, check the enabled box. You are now ready to save the URL filter setting.

7. Click the Add URL button. The setting you added is listed in the `Current URLs` panel.

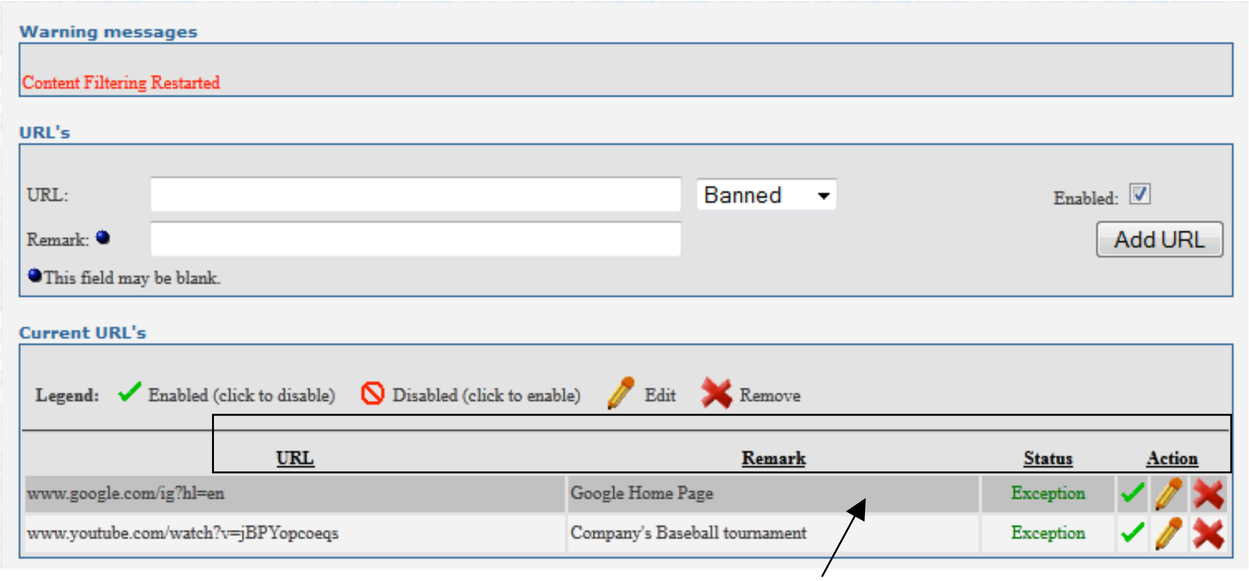
Viewing the Current List of URLs

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the `Content Filter Control` page appears*.*

2. Next, you will need to click on the URL's button. The URLs page appears. The second panel is the `Current URLs` panel. *See Figure 6.9: Content Filter page – Current URLs panel.* This panel allows you to edit, disable and delete any URL settings.

> **NOTE**
>
> For easy look up, simply click on the title links above each column to sort alphabetically. For example to sort the list by URL click on the URL link.

Figure 6.9: Content Filter page – Current URLs panel



Warning messages

Content Filtering Restarted

URL's

URL: Banned ▾ Enabled: ☑

Remark: ● Add URL

●This field may be blank.

Current URL's

Legend: ✓ Enabled (click to disable) ⦸ Disabled (click to enable) ✎ Edit ✗ Remove

URL	Remark	Status	Action
www.google.com/ig?hl=en	Google Home Page	Exception	✓ ✎ ✗
www.youtube.com/watch?v=jBPYopcoeqs	Company's Baseball tournament	Exception	✓ ✎ ✗

Click on the title links to sort each column alphabetically

Editing URLs

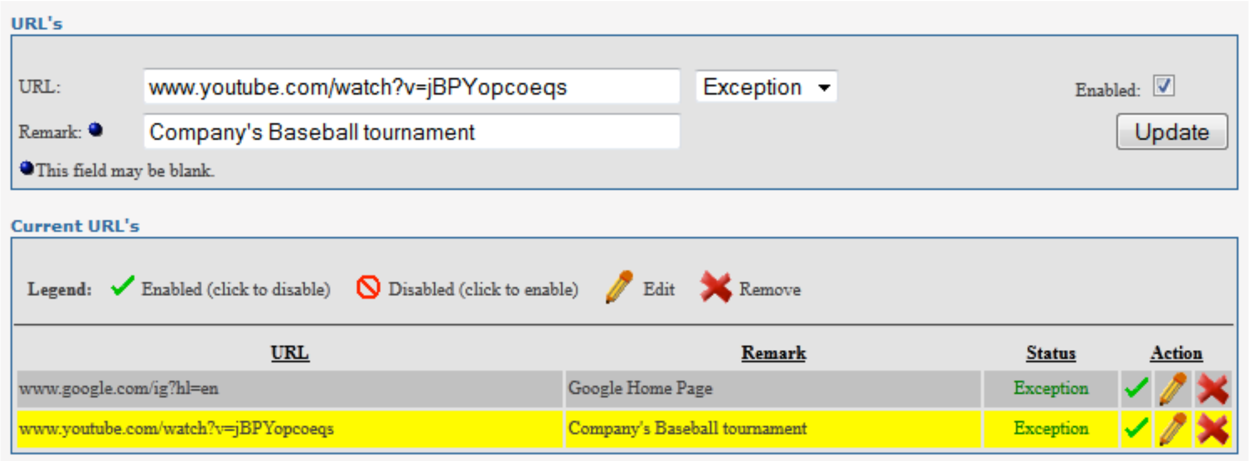
1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the Content Filter Control page appears.

2. Next, you will need to click on the URL's button. The `URLs` page appears. The second panel is the Current URLs panel. **Note:** For easy look up, simply click on the title links above each column to sort alphabetically.

3. Click the ✎ icon associated with the URL you want to edit. The details for that URL are placed in the URLs panel. *See Figure 6.10: Content Filter page – Edit URLs,* on the next page.

4. Make the appropriate changes and then click the Update button. You can view the changes you made in the Current URLs panel.

Figure 6.10: Content Filter Page – Edit URLs



URL's

URL: www.youtube.com/watch?v=jBPYopcoeqs | Exception ▾ | Enabled: ☑

Remark: ● Company's Baseball tournament | Update

● This field may be blank.

Current URL's

Legend: ✓ Enabled (click to disable) ⃠ Disabled (click to enable) ✎ Edit ✖ Remove

URL	Remark	Status	Action
www.google.com/ig?hl=en	Google Home Page	Exception	✓ ✎ ✖
www.youtube.com/watch?v=jBPYopcoeqs	Company's Baseball tournament	Exception	✓ ✎ ✖

Removing URLs from the Content Filter List

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.

2. Next, you will need to click on the URL's button. The `URLs` page appears. The second panel is the Current URLs panel. *See Figure 6.9: Content Filter page – Current URLs panel,* on page 87. For easy look up, simply click on the title links above each column to sort alphabetically*.*

3. Click the ✖ icon associated with the URL you want to remove. Once you click the `delete` icon, the URL is removed automatically.

Disabling/Enabling URLs

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.

2. Next, you will need to click on the URL's button. The `URLs` page

appears. The second panel is the Current URLs panel. *See Figure 6.9: Content Filter page on page 103 – Current URLs panel* on the next page. For easy look up, simply click on the title links above each column to sort alphabetically*.*

3. *Click the ✓icon associated with the URL you want to disable. The ✓ icon as been replaced with a ⊘. To enable the URL setting, simply click on the ⊘icon and the ✓ icon is returned and your URL setting will be enabled.*

Users

The NetSentron Users administration page gives the administrator the ability to give each user attached to the network a user name and password that would allow them access to the Internet (the user would be prompted for a user name and password when opening up a browser). Using this feature gives the administrator the ability to see where and when each user is surfing the net. If someone has abused their Internet privileges the administrator can deny them access. For this feature to work the NetSentron Authentication must be enabled, the user must be assigned to a group and the web proxy settings for the browser need to be changed to allow for User Authentication.

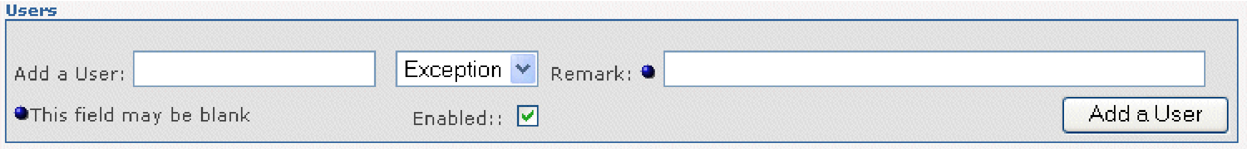
Adding Users

1. From the Administration Interface, click on the **Filters** button. New sets of buttons appear. By default the Content Filter Control page appears*.*
2. Next, you will need to click on the **users** button. The Users panel appears. *See Figure 6.11: Content Filter – Users panel* on the next page.

> **NOTE**
>
> Basic proxy authentication must be enabled for this feature to work. *See Configuring Web Proxy Settings, above.*

3. In the `Add a User` field, key in the name of the person you want to add to the Content Filter User list.

Figure 6.11: Content Filter – Users Panel



Users

Add a User: 　 Exception ▾ 　 Remark: ●

●This field may be blank 　 Enabled:: ☑ 　 Add a User

4. Next, click on the drop down menu to the right of the Add a User field. You are given two options: `Banned and Exception`. See below for a description of each status option.

Banned 　 User, if basic proxy authentication is enabled, will automatically be denied, web access.

Exception 　 User, if basic proxy authentication is enabled, will not be filtered automatically.

5. In the remark field you can add a brief description. This field is optional.

6. Check the enabled box. You are now ready to save the user to the `Content Filter List`.

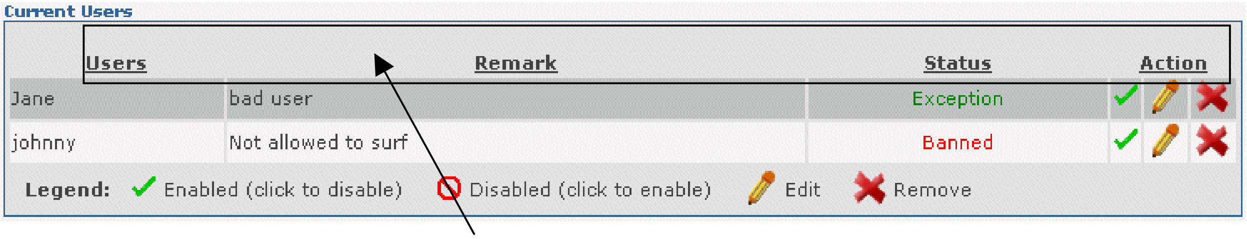
7. Click the Add a User button. The setting you added is listed in the `Current Users` panel.

Viewing the Current List of Users

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the Content Filter Control page appears.

2. Next, you will need to click on the users button. The `Users` page appears. The second panel is the `Current Users` panel. *See Figure 6.12: Content Filter page – Current Users panel, below.* This panel allows you to edit, disable and delete any of the users on the list. For easy look up, simply click on the title links above each column to sort alphabetically. For example to sort the list by users click on the `Users` link.

Figure 6.12: Content Filter Page – Current Users Panel



Current Users

Users	Remark	Status	Action
Jane	bad user	Exception	✓ ✎ ✖
johnny	Not allowed to surf	Banned	✓ ✎ ✖

Legend: ✓ Enabled (click to disable) ⦸ Disabled (click to enable) ✎ Edit ✖ Remove

Click on the title links to sort each column alphabetically

Editing Users

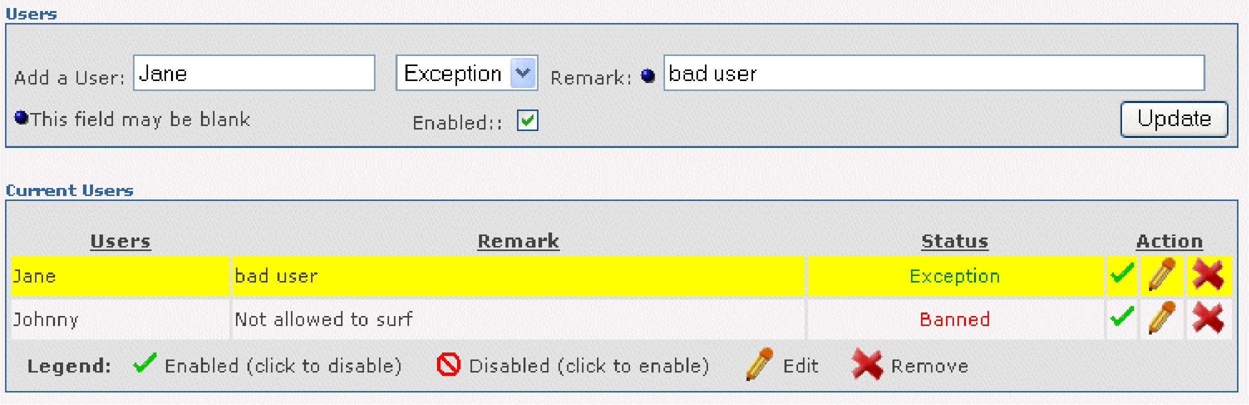
1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the `Content Filter Control` page appears.

2. Next, you will need to click on the users button. The `Users` page appears. The second panel is the `Current Users` panel. For easy look up, simply click on the title links above each column to sort alphabetically.

3. Click the ✎ icon associated with the user you want to edit. The details

for that user are placed in the `Users` panel. *See Figure 6.13: Content Filter page – Edit Users on the next page.*

Figure 6.13: Content Filter Page – Edit Users



Users

Add a User: Jane | Exception | Remark: ● bad user

●This field may be blank | Enabled:: ☑ | Update

Current Users

Users	Remark	Status	Action
Jane	bad user	Exception	✓ ✎ ✗
Johnny	Not allowed to surf	Banned	✓ ✎ ✗

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) ✎ Edit ✗ Remove

4. Make the appropriate changes and then click the Update button. You can view the changes you made in the `Current Users` panel.

Removing Users

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.
2. Next, you will need to click on the users button. The `Users` page appears. The second panel is the `Current Users` panel. *See Figure 6.12: Content Filter page – Current Users panel, on page 107.*
3. Click the ✗ icon associated with the user you want to remove.

Disabling/Enabling Users

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.
2. Next, you will need to click on the users button. The `Users` page appears. The second panel is the `Current Users` panel. *See Figure*

6.12: Content Filter page – Current Users panel, on page 108.

3. Click the ✓icon associated with the user you want to disable. The✓ icon as been replaced with a 🚫. To enable the user, simply click on the 🚫 icon and the ✓icon is returned and the user will be enabled again.

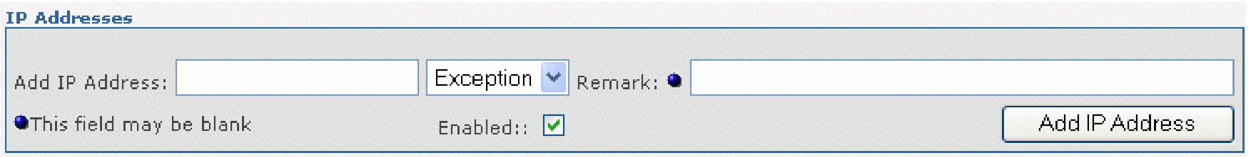
IP Addresses

This page allows you to alter access to the internet based on an IP address. You can also change whether a specific IP address is filtered or unfiltered. This allows you to setup certain computers to have completely unfiltered access to the internet.

Adding IP Addresses

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the `Content Filter Control` page appears*.*
2. Next, you will need to click on the ip addresses button. The `IP Addresses` panel appears. *See Figure 6.14: Content Filter – IP Addresses panel, below.*
3. In the `Add IP Addresses` field, key in the IP address you want to add to the Content Filter list.

Figure 6.14: Content Filter – IP Addresses Panel



IP Addresses

Add IP Address: [ ] Exception ▾ Remark: ● [ ]

●This field may be blank

Enabled:: ☑

4. Next, click on the drop down menu to the right of the `Add IP Address` field. You are given two options: `Banned` and `Exception`. See below for a description of each status option.

Banned Where web access is disallowed. **Note:** Only put IP addresses here, not host names.

Exception The IP address is not filtered, it passes requests straight through. Examples would be servers that need unfiltered access for updates. Also administrator workstations, which need to download programs and check out blocked sites, should be put here.

5. In the remark field you can add a brief description.

6. Lastly, check the enabled box. You are now ready to save the IP address to the list.

7. Click the Add IP Address button. The IP address you added is listed in the `Current IP Addresses panel.`

Viewing the Current List of IP Addresses

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the Content Filter Control page appears*.*

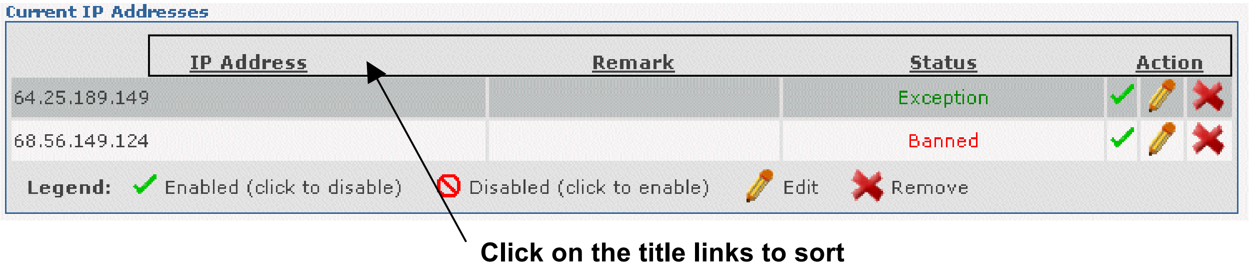
2. Next, you will need to click on the ip addresses button. The IP Addresses page appears. The second panel is the Current IP Addresses panel. *See Figure 6.14: Content Filter page – Current IP Addresses*

panel, below. This panel allows you to edit, disable and delete any of the IP addresses on the list.

NOTE

For easy look up, simply click on the title links above each column to sort alphabetically. For example: to sort the list by status, click on the Status link.

Figure 6.14: Content Filter Page – Current IP Addresses Panel



Current IP Addresses

IP Address	Remark	Status	Action
64.25.189.149		Exception	✓ ✎ ✗
68.56.149.124		Banned	✓ ✎ ✗

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) ✎ Edit ✗ Remove

Click on the title links to sort each column alphabetically

Editing IP Addresses

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the Content Filter Control page appears.
2. Next, you will need to click on the ip addresses button. The `IP Addresses` page appears. The second panel is the `Current IP Addresses` panel.

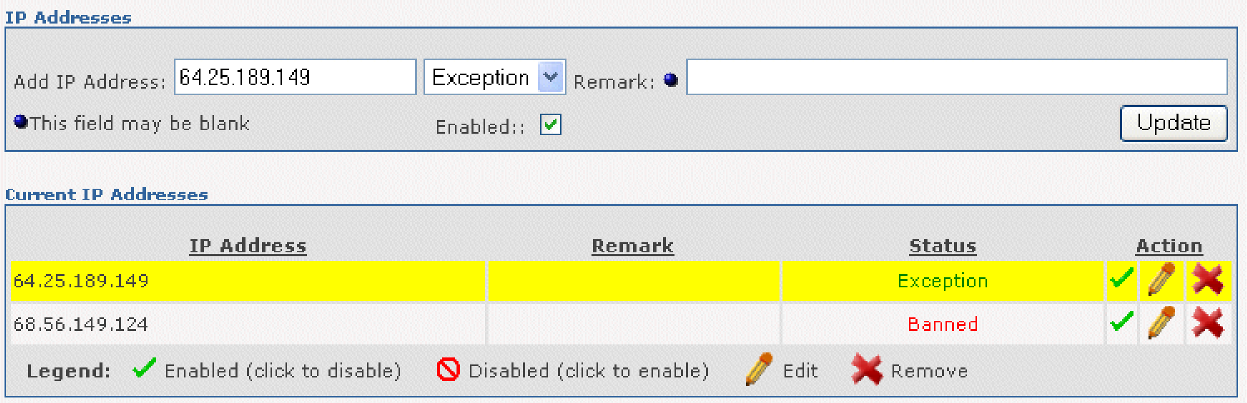
NOTE

For easy look up, simply click on the title links above each column to sort alphabetically.

3. Click the ✏ icon associated with the IP address you want to edit. The details for that IP address are placed in the `IP Addresses` panel. *See Figure 6.15: Content Filter page – Edit IP Addresses, on the next page.*

> **NOTE**
>
> The IP Address you are editing in highlighted yellow.

Figure 6.15: Content Filter Page – Edit IP Addresses



IP Addresses

Add IP Address: 64.25.189.149 | Exception | Remark: ●

●This field may be blank | Enabled:: ☑ | Update

Current IP Addresses

IP Address	Remark	Status	Action
64.25.189.149		Exception	✓ ✏ ✗
68.56.149.124		Banned	✓ ✏ ✗

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) ✏ Edit ✗ Remove

4. Make the appropriate changes and then click the Update button. You can view the changes you made in the `Current IP` Addresses panel.

Removing IP Addresses

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.

2. Next, you will need to click on the ip addresses button. The `IP Addresses` page appears. The second panel is the `Current IP Addresses` panel. *See Figure 6.14: Content Filter page – Current IP Addresses panel.* For easy look up, simply click on the title links above each column to sort alphabetically*.*

3. Click the ✗ icon associated with the IP Address you want to remove. Once you click the `delete` icon, the IP Address is removed

automatically.

Disabling/Enabling IP Addresses

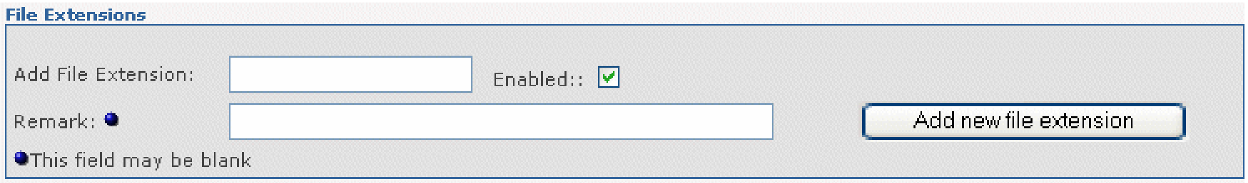
1. From the Administration Interface, click on the **Filters** button. New sets of buttons appear.
2. Next, you will need to click on the **ip addresses** button. The `IP Addresses` page appears. The second panel is the `Current IP Addresses` panel. *See Figure 6.14: Content Filter page – Current IP Addresses panel.*
3. Click the ✓ icon associated with the IP Address you want to disable. The ✓ icon as been replaced with a ⊘. To enable the IP Address, simply click on the ⊘ icon and the ✓ icon is returned and the IP Address will be enabled again.

Banning Files via Extensions

This page allows you to block certain file extensions such as .zip, .exe, etc.

1. From the Administration Interface, click on the **Filters** button. New sets of buttons appear. By default the `Content Filter Control` page appears.
2. Next, you will need to click on the **file extensions** button. The `File Extensions` Page appears. To add a new file extension you will be using the `File Extensions` panel. *See Figure 6.16: Content Filter – File Extensions panel.*
3. In the `Add File Extension` field, key in the file extension you want to add to the Content Filter list.

Figure 6.16: Content Filter – File Extensions Panel



File Extensions

Add File Extension: ______ Enabled:: ☑

Remark: ● ______

●This field may be blank

4. In the `Remark` field you can add a brief description. **Note:** This field is optional.
5. Lastly, check the `Enabled` box. You are now ready to save the file extension to the list.
6. Click the Add new file extension button. The content filter restarts automatically. The file extension you added is listed in the `Current File Extensions` panel.

Viewing the Current List of Banned File Extensions

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the `Content Filter Control` page appears.
2. Next, you will need to click on the file extensions button. The `File Extensions` page appears. The second panel is the `Current File Extensions` panel. *See Figure 6.17: Content Filter page – Current File Extensions panel.* This panel allows you to edit, disable and delete any of the IP addresses on the list.

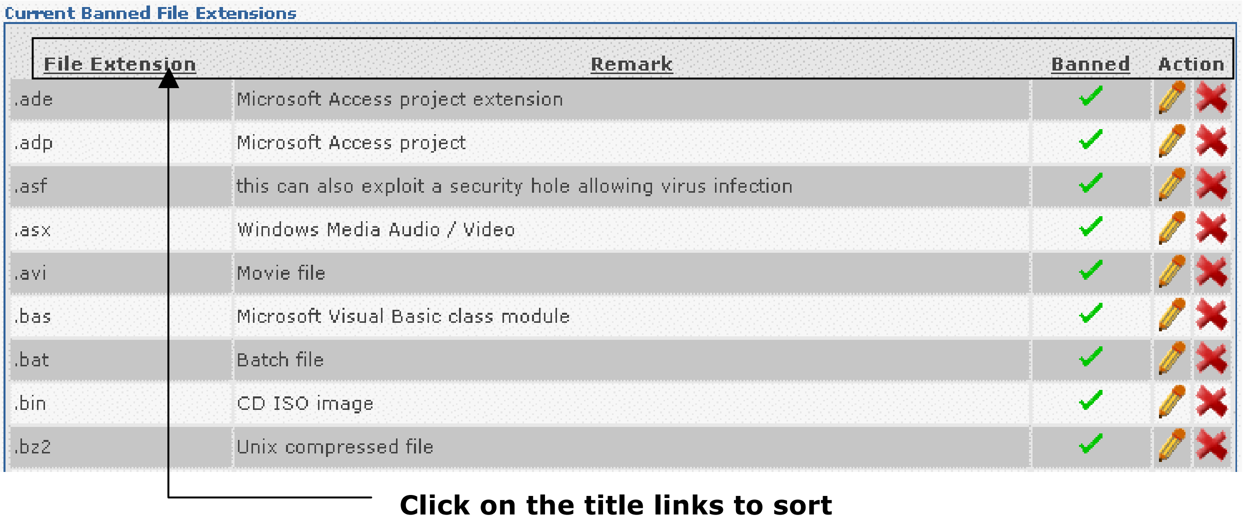
NOTE

For easy look up, simply click on the title links above each column to sort alphabetically. For example to sort the list by file extension click on the `File Extension` link.

NOTE

The Content Filter comes with some example file extensions to deny. This is a good way of blocking kids from downloading those lovely screen savers and hacking tools. Do not ban the file extension .html, or .jpg etc. If a URL ends in an extension that is in this list, The Content Filter will block it.

Figure 6.17: Content Filter Page – Current File Extensions Panel



Current Banned File Extensions

File Extension	Remark	Banned	Action
.ade	Microsoft Access project extension	✓	✎ ✗
.adp	Microsoft Access project	✓	✎ ✗
.asf	this can also exploit a security hole allowing virus infection	✓	✎ ✗
.asx	Windows Media Audio / Video	✓	✎ ✗
.avi	Movie file	✓	✎ ✗
.bas	Microsoft Visual Basic class module	✓	✎ ✗
.bat	Batch file	✓	✎ ✗
.bin	CD ISO image	✓	✎ ✗
.bz2	Unix compressed file	✓	✎ ✗

Click on the title links to sort each column alphabetically

Editing Banned File Extensions

1. From the Administration Interface, click on the **Filters** button. New sets of buttons appear. By default the `Content Filter Control` page appears.

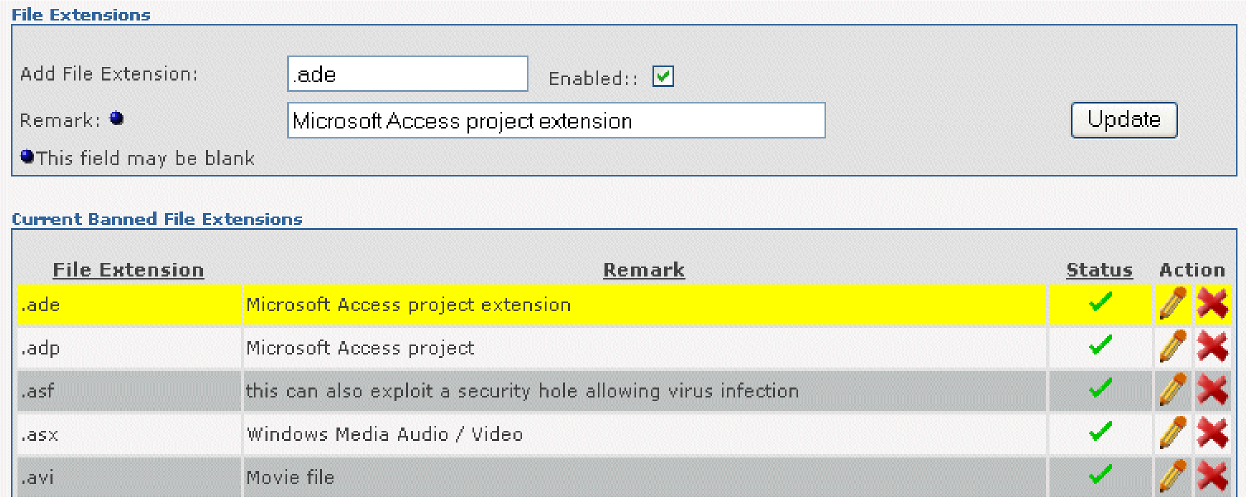
   Next, you will need to click on the **file extensions** button. The `File Extensions` page appears. The second panel is the `Current File Extensions` panel.

> **NOTE**
>
> For easy look up, simply click on the title links above each column to sort alphabetically.

3. Click the ✎ icon associated with the file extension you want to edit. The details for the extensions are placed in the `File Extension` panel. *See Figure 6.18: Content Filter page – Edit File Extensions.*

NOTE
The file extension you are editing is highlighted yellow

Figure 6.18: Content Filter Page – Edit File Extensions



File Extensions

Add File Extension: .ade Enabled:: ☑

Remark: ● Microsoft Access project extension Update

●This field may be blank

Current Banned File Extensions

File Extension	Remark	Status	Action
.ade	Microsoft Access project extension	✓	✎ ✗
.adp	Microsoft Access project	✓	✎ ✗
.asf	this can also exploit a security hole allowing virus infection	✓	✎ ✗
.asx	Windows Media Audio / Video	✓	✎ ✗
.avi	Movie file	✓	✎ ✗

4. Make the appropriate changes and then click the Update button. You can view the changes you made in the `Current File Extensions` panel.

Removing File Extensions

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.
2. Next, you will need to click on the file extensions button. The `File Extensions` page appears. The second panel is the `Current File Extensions` panel. *See Figure 6.17: Content Filter page – Current File Extensions panel, on the previous page.*

NOTE

For easy look up, simply click on the title links above each column to sort alphabetically.

3. Click the✗ icon associated with the file extension you want to remove.

NOTE

Once you click the delete icon, the file extension is removed automatically.

Disabling/Enabling File Extensions

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.
2. Next, you will need to click on the file extensions button. The `File Extensions` page appears. The second panel is the `Current File Extensions` panel. *See Figure 6.17: Content Filter page – Current File Extensions panel.*

NOTE

For easy look up, simply click on the title links above each column to sort alphabetically*.*

3. Click the ✓ icon associated with the file extension you want to disable. The ✓ icon has been replaced with a ⊘. To enable the file extension, simply click on the⊘ icon and the ✓ icon is returned and the file extension will be enabled again.

Banning MIME Types

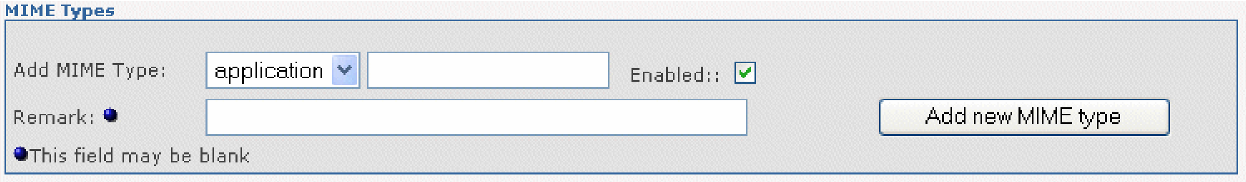
Mime Types are file types that are presented to your web browser. The Mime Type option allows you to specify which types of files (i.e. video files) you want to stop the web browser from opening.

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the `Content Filter Control` page appears.
2. Next, you will need to click on the file extensions button. The `MIME Types` Page appears. To add a new MIME type you will be using the `MIME Types` panel. *See Figure 6.19: Content Filter – MIME Types panel.*

3. Click on the drop down box next to the `Add MIME Types` field. There are three selections to choose from; application, audio, and video. Make your selection by clicking on it.

4. In the field next to the drop down, key in the name of the MIME Type.

Figure 6.19: Content Filter – MIME Types Panel



MIME Types

Add MIME Type: application

Enabled:: ☑

Remark: ●

●This field may be blank

5. In the Remark field you can add a brief description. This field is optional.

6. Lastly, check the enabled box. You are now ready to save the MIME Type to the list.

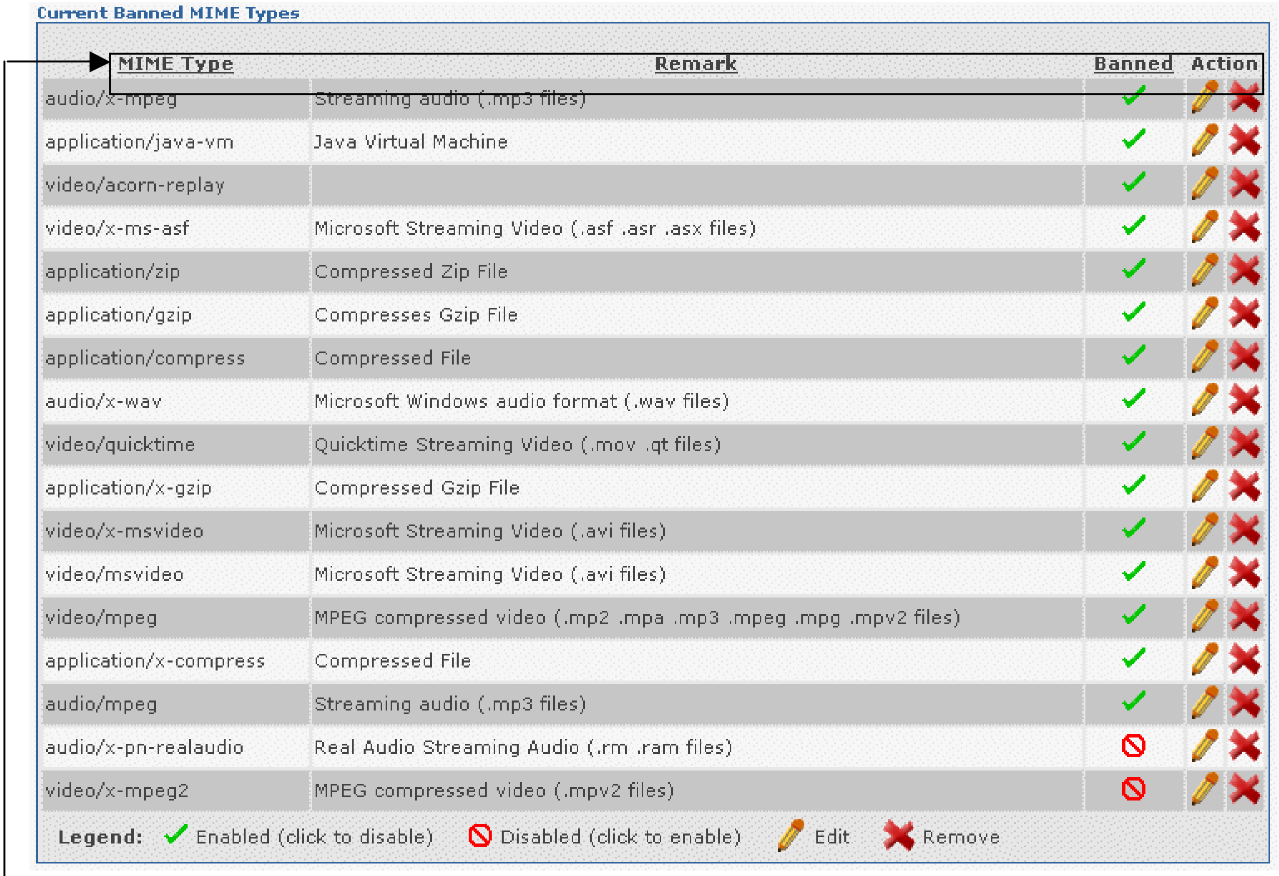
7. Click the Add new MIME type button. The content filter restarts automatically. The MIME Type you added is listed in the `Current MIME Types` panel.

Viewing the Current List of Banned MIME Types

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the Content Filter Control page appears*.*

2. Next, you will need to click on the mime types button. The `MIME Types` page appears. The second panel is the `Current MIME` Types panel. *See Figure 6.20: Content Filter page – Current MIME Types panel* on the next page. This panel allows you to edit, disable and delete any of the MIME Types on the list.

Figure 6.20: Content Filter Page – Current MIME Types Panel



Current Banned MIME Types

MIME Type	Remark	Banned	Action
audio/x-mpeg	Streaming audio (.mp3 files)	✓	✎ ✖
application/java-vm	Java Virtual Machine	✓	✎ ✖
video/acorn-replay		✓	✎ ✖
video/x-ms-asf	Microsoft Streaming Video (.asf .asr .asx files)	✓	✎ ✖
application/zip	Compressed Zip File	✓	✎ ✖
application/gzip	Compresses Gzip File	✓	✎ ✖
application/compress	Compressed File	✓	✎ ✖
audio/x-wav	Microsoft Windows audio format (.wav files)	✓	✎ ✖
video/quicktime	Quicktime Streaming Video (.mov .qt files)	✓	✎ ✖
application/x-gzip	Compressed Gzip File	✓	✎ ✖
video/x-msvideo	Microsoft Streaming Video (.avi files)	✓	✎ ✖
video/msvideo	Microsoft Streaming Video (.avi files)	✓	✎ ✖
video/mpeg	MPEG compressed video (.mp2 .mpa .mp3 .mpeg .mpg .mpv2 files)	✓	✎ ✖
application/x-compress	Compressed File	✓	✎ ✖
audio/mpeg	Streaming audio (.mp3 files)	✓	✎ ✖
audio/x-pn-realaudio	Real Audio Streaming Audio (.rm .ram files)	🛇	✎ ✖
video/x-mpeg2	MPEG compressed video (.mpv2 files)	🛇	✎ ✖

Legend: ✓ Enabled (click to disable) 🛇 Disabled (click to enable) ✎ Edit ✖ Remove

Click on the title links to sort each column alphabetically

Editing Banned MIME Types

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the `Content Filter Control` page appears.

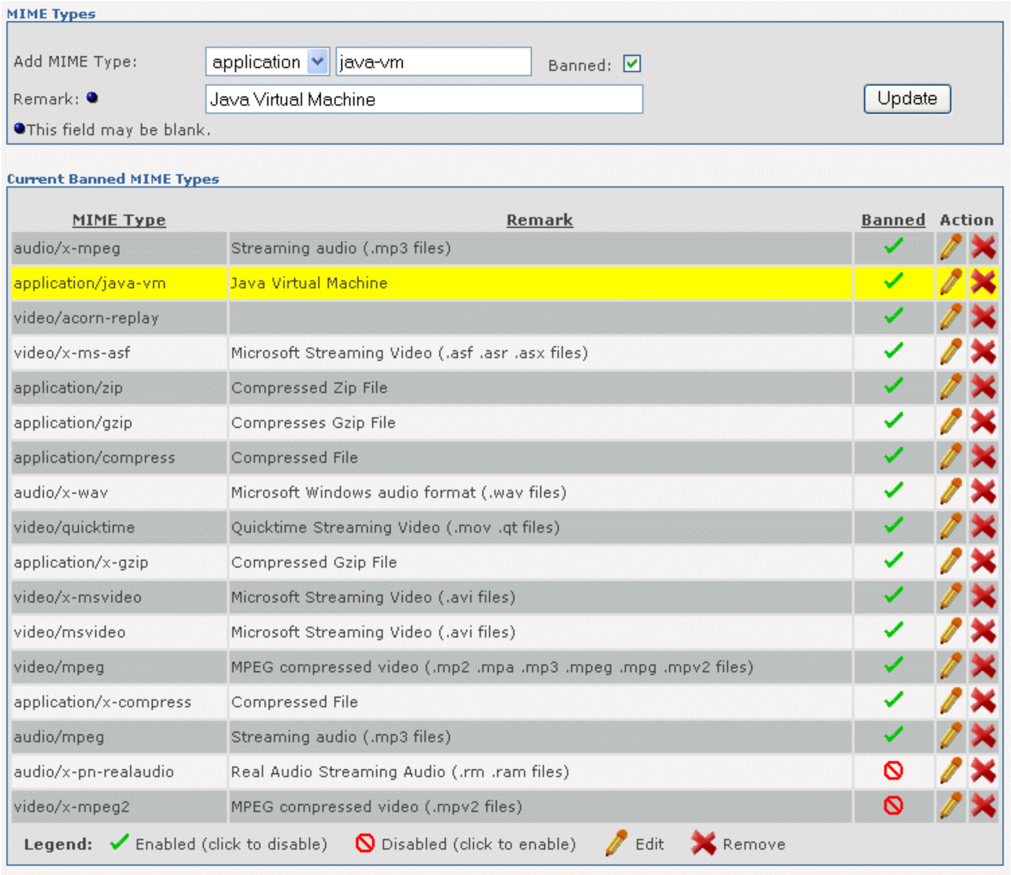
2. Next, you will need to click on the mime types button. The `MIME Types` page appears. The second panel is the `Current MIME Types` panel. **Note:** For easy look up, simply click on the title links above each column to sort alphabetically.

3. Click the ✎ icon associated with the MIME type you want to edit. The details for the MIME type are placed in the MIME Types panel. *See Figure 6.21: Content Filter page – Edit MIME Types* on the following page.

NOTE

The MIME type you are editing is highlighted yellow.

Figure 6.21: Content Filter page – Edit MIME Types



MIME Types

Add MIME Type: application ⌄ java-vm Banned: ☑

Remark: ● Java Virtual Machine

●This field may be blank.

Current Banned MIME Types

MIME Type	Remark	Banned	Action
audio/x-mpeg	Streaming audio (.mp3 files)	✓	✎ ✖
application/java-vm	Java Virtual Machine	✓	✎ ✖
video/acorn-replay		✓	✎ ✖
video/x-ms-asf	Microsoft Streaming Video (.asf .asr .asx files)	✓	✎ ✖
application/zip	Compressed Zip File	✓	✎ ✖
application/gzip	Compresses Gzip File	✓	✎ ✖
application/compress	Compressed File	✓	✎ ✖
audio/x-wav	Microsoft Windows audio format (.wav files)	✓	✎ ✖
video/quicktime	Quicktime Streaming Video (.mov .qt files)	✓	✎ ✖
application/x-gzip	Compressed Gzip File	✓	✎ ✖
video/x-msvideo	Microsoft Streaming Video (.avi files)	✓	✎ ✖
video/msvideo	Microsoft Streaming Video (.avi files)	✓	✎ ✖
video/mpeg	MPEG compressed video (.mp2 .mpa .mp3 .mpeg .mpg .mpv2 files)	✓	✎ ✖
application/x-compress	Compressed File	✓	✎ ✖
audio/mpeg	Streaming audio (.mp3 files)	✓	✎ ✖
audio/x-pn-realaudio	Real Audio Streaming Audio (.rm .ram files)	⦸	✎ ✖
video/x-mpeg2	MPEG compressed video (.mpv2 files)	⦸	✎ ✖

Legend: ✓ Enabled (click to disable) ⦸ Disabled (click to enable) ✎ Edit ✖ Remove

4. Make the appropriate changes and then click the Update button. You can view the changes you made in the `Current MIME Types` panel.

Removing MIME Types

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.
2. Next, you will need to click on the mime types button. The `MIME Types` page appears. The second panel is the `Current MIME Types` panel. *See Figure 6.20: Content Filter page – Current MIME Types panel.*

> **NOTE**
>
> For easy look up, simply click on the title links above each column to sort alphabetically*.*

3. Click the ✗ icon associated with the MIME type you want to remove.

> **NOTE**
>
> Once you click the delete icon, the MIME type is removed automatically.

Disabling/Enabling MIME Types

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.

2. Next, you will need to click on the mime types button. The `MIME Types` page appears. The second panel is the `Current MIME Types` panel. *See Figure 6.20: Content Filter page – Current MIME Types panel*.

> **NOTE**
>
> For easy look up, simply click on the title links above each column to sort alphabetically*.*

3. Click the ✓ icon associated with the MIME type you want to disable. The ✓ icon has been replaced with a ⊘. To enable the MIME type, simply click on the ⊘ icon and the ✓ icon is returned and the MIME type will be enabled again.

Working with Phrases

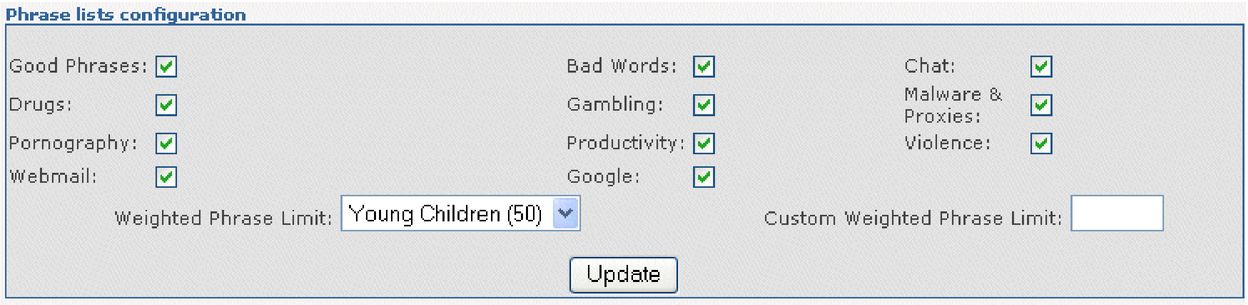
The phrases page allows you to block pages that contain certain phrases. Say you wanted to block a page about puppies. You could add the word puppies and set the count for that word, higher than the Weighted Phrase Limit you had set in the phrases section. Each time the NetSentron encountered a page with puppies in it, the page would be blocked.

1. From the Administration Interface, click on the **Filters** button. New sets of buttons appear. By default the `Content Filter Control` page appears.

2. Next, you will need to click on the **phrases** button. The Phrases page appears. The first panel is the Phrases lists configuration panel. *See Figure 6.22: Content Filter – Phrase list configuration panel,* below. This panel has a selection of pre-programmed phrases.

> **NOTE**
>
> By default ALL the phrase/word options have been enabled.

Figure 6.22: Content Filter – Phrase List Configuration Panel



Phrase lists configuration

Good Phrases:	☑	Bad Words:	☑	Chat:	☑
Drugs:	☑	Gambling:	☑	Malware & Proxies:	☑
Pornography:	☑	Productivity:	☑	Violence:	☑
Webmail:	☑	Google:	☑		

Weighted Phrase Limit: Young Children (50)

Custom Weighted Phrase Limit:

3. Next you can select how you want the phrase limited weighted. Click on the drop box next to `Weight Phrase Limit`. **NOTE**: This is the limit over which the page will be blocked. Each weighted phrase is given a value either positive or negative and the values added up. Phrases to

do with good subjects will have negative values, and bad subjects will have positive values. You have four choices: `Young Children (50)`, `Older Children (100)`, `Young Adults (160)` and `Custom`.

4. If `Custom` is selected you will need to key in a number in the `Custom Weighted Phrase Limit` field.

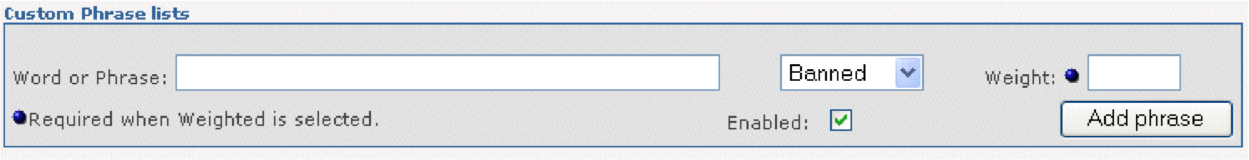
5. When you are satisfied with your selections, click on the Update button. The content filter restarts automatically. The changes you made have been recorded.

Working with Custom Phrases

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the `Content Filter Control` page appears.
2. Next, you will need to click on the phrases button. The `Phrases` page appears. When working with Custom Phrases you will be using the `Custom Phrase` List panel. *See Figure 6.23: Content Filter – Custom Phrase Lists panel.*
3. In the `Word` or `Phrase` field key in the name of the word or phrase you want to add.

> **NOTE**
>
> The phrases and words must be enclosed between < and >.

Figure 6.23: Content Filter – Custom Phrase Lists Panel



Custom Phrase lists

Word or Phrase:

Banned

Weight: ●

●Required when Weighted is selected.

Enabled: ☑

4. The next step is to select how you want the system to filter the word or phrase. Click on the drop down menu to the right of the `Word` or `Phrase` field. You have three choices: `Banned, Exception, Weighted`.

> **NOTE**
>
> If `Weighted` is selected you will need to key in a number in the `Weight` field.

5. Lastly, check the enabled box. You are now ready to save the Custom Word/Phrase to the list.

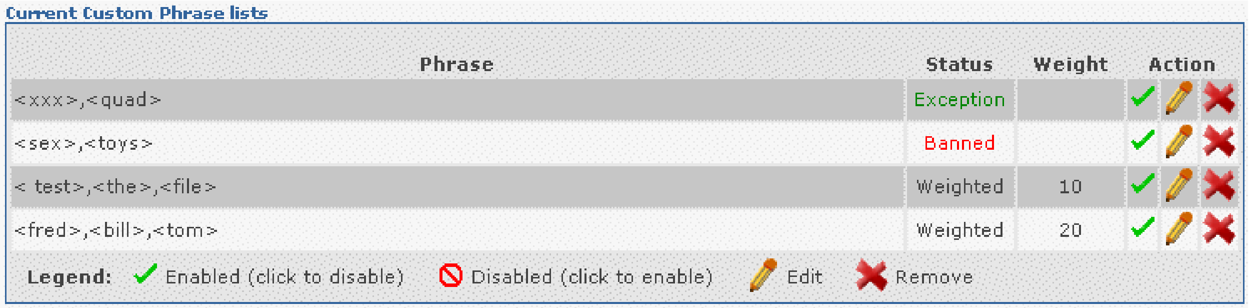
6. Click the Add phrase button. The content filter restarts automatically. The Custom Word/Phrase you added is listed in the `Current Custom Phrase` lists panel. *See Figure 6.24: Content Filter page – Current Custom Phrase lists panel.*

Viewing the Current Custom Phrase List

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the `Content Filter Control` page appears.

2. Next, you will need to click on the phrases button. The Phrases page appears. The third panel is the `Current Custom Phrase` lists panel. *See Figure 6.24: Content Filter page – Current Custom Phrase lists panel, below.* This panel allows you to edit, disable and delete any of the custom words or phrases on the list.

Figure 6.24: Content Filter Page – Current Custom Phrase Lists Panel



Current Custom Phrase lists

Phrase	Status	Weight	Action
<xxx>,<quad>	Exception		✓ ✎ ✖
<sex>,<toys>	Banned		✓ ✎ ✖
< test>,<the>,<file>	Weighted	10	✓ ✎ ✖
<fred>,<bill>,<tom>	Weighted	20	✓ ✎ ✖

Legend: ✓ Enabled (click to disable) ⃠ Disabled (click to enable) ✎ Edit ✖ Remove

Editing Custom Phrases/Words

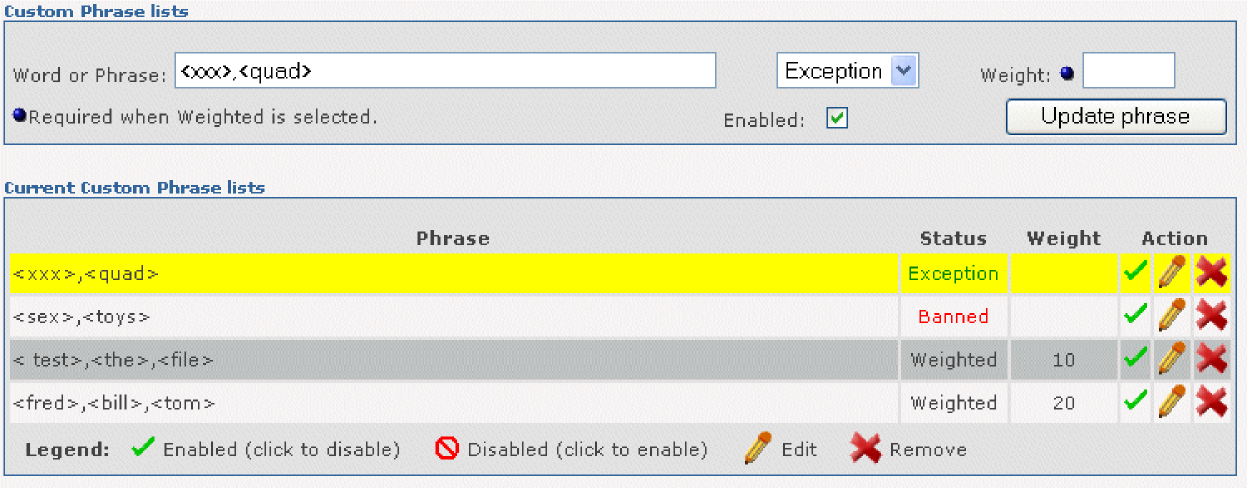
1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the `Content Filter Control` page appears.

2. Next, you will need to click on the phrases button. The Phrases page appears. The third panel is the `Current Custom Phrase` lists panel. *See Figure 6.24: Content Filter page – Current Custom Phrase list.* This panel allows you to edit, disable and delete any of the custom words or phrases on the list.

3. Click the ✎ icon associated with the phrase or word type you want to edit. The details for the phrase or word are placed in the `Custom Phrase lists` panel. *See Figure 6.25: Content Filter page – Edit Custom Phrases/Words below.*

> **NOTE**
>
> The Phrase/Word type you are editing is highlighted yellow.

Figure 6.25: Content Filter Page – Edit Custom Phrases/Words



Custom Phrase lists

Word or Phrase: <xxx>,<quad> Exception Weight: ●

●Required when Weighted is selected. Enabled: ☑ Update phrase

Current Custom Phrase lists

Phrase	Status	Weight	Action
<xxx>,<quad>	Exception		✓ ✎ ✖
<sex>,<toys>	Banned		✓ ✎ ✖
< test>,<the>,<file>	Weighted	10	✓ ✎ ✖
<fred>,<bill>,<tom>	Weighted	20	✓ ✎ ✖

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) ✎ Edit ✖ Remove

4. Make the appropriate changes and then click the Update button. You can view the changes you made in the `Current MIME Types` panel.

Removing Custom Phrases/Words

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.

2. Next, you will need to click on the phrases button. The `Phrases` page appears. The third panel is the `Current Custom Phrase lists` panel. *See Figure 6.24: Content Filter page – Current Custom Phrase lists panel on page 125.* This panel allows you to edit, disable and delete any of the custom words or phrases on the list.

3. Click the ✖ icon associated with the phrase/word you want to remove. **Not**e: Once you click the delete icon, the phrase/word is removed automatically.

Disabling/Enabling Custom Phrases/Words

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.

2. *2.* Next, you will need to click on the phrases button. The `Phrases` page appears. The third panel is the `Current Custom Phrase` lists panel. *See Figure 6.24: Content Filter page – Current Custom Phrase lists panel, on page 125.* This panel allows you to edit, disable and delete any of the custom words or phrases on the list*.*

3. Click the ✓ icon associated with the phrase/word you want to disable. The ✓ icon has been replaced with an ⊘ icon. To enable the phrase/word type, simply click on the ⊘ icon and the ✓ icon is returned and the phrase/word will be enabled again.

Blacklists

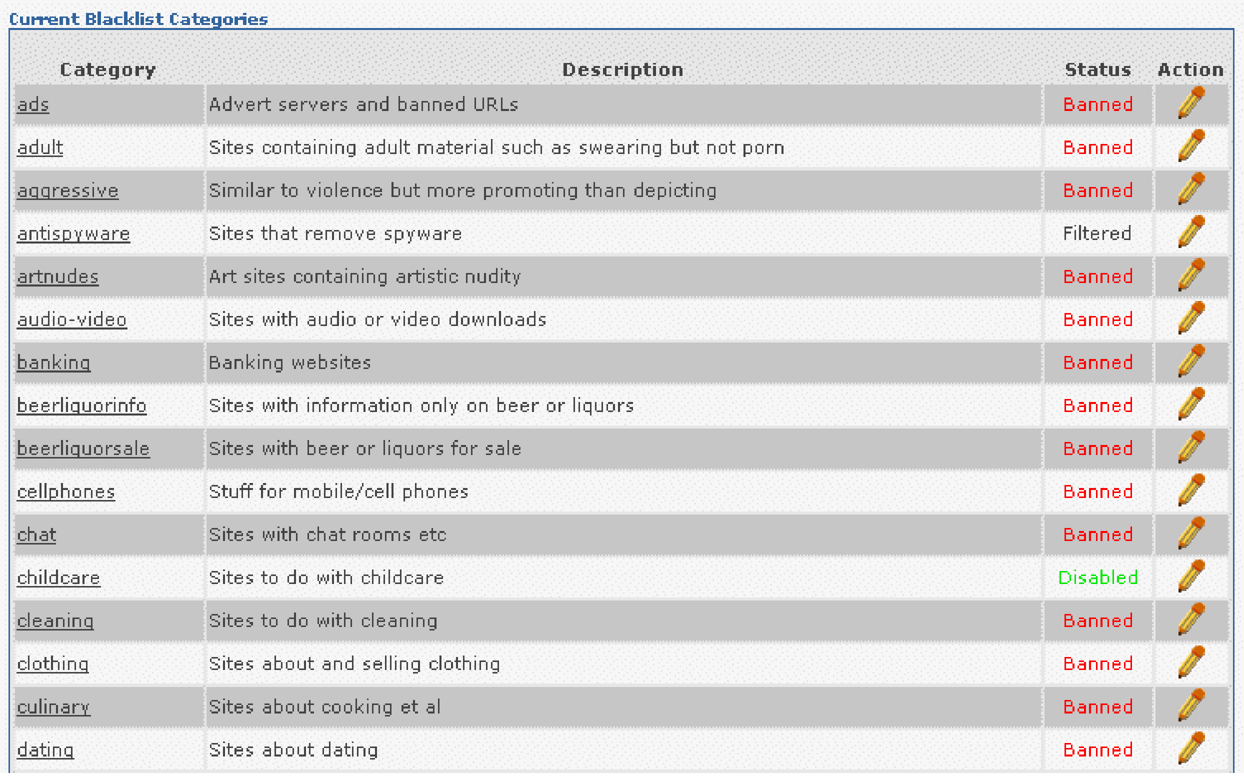
The NetSentron contains many blacklists that are broken down in to various categories. These categories can be enabled or disabled through the Blacklists page.

Viewing Current Blacklist Categories

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the `Content Filter Control` page appears*.*

2. Next, you will need to click on the blacklists button. The `Blacklist` page appears. The only panel on this page is the `Current Blacklists Categories` panel. *See Figure 6.26: Content Filter page – Current Blacklist Categories panel on the next page.* The only option available to you is the edit option.

Figure 6.26: Content Filter Page – Current Blacklist Categories Panel



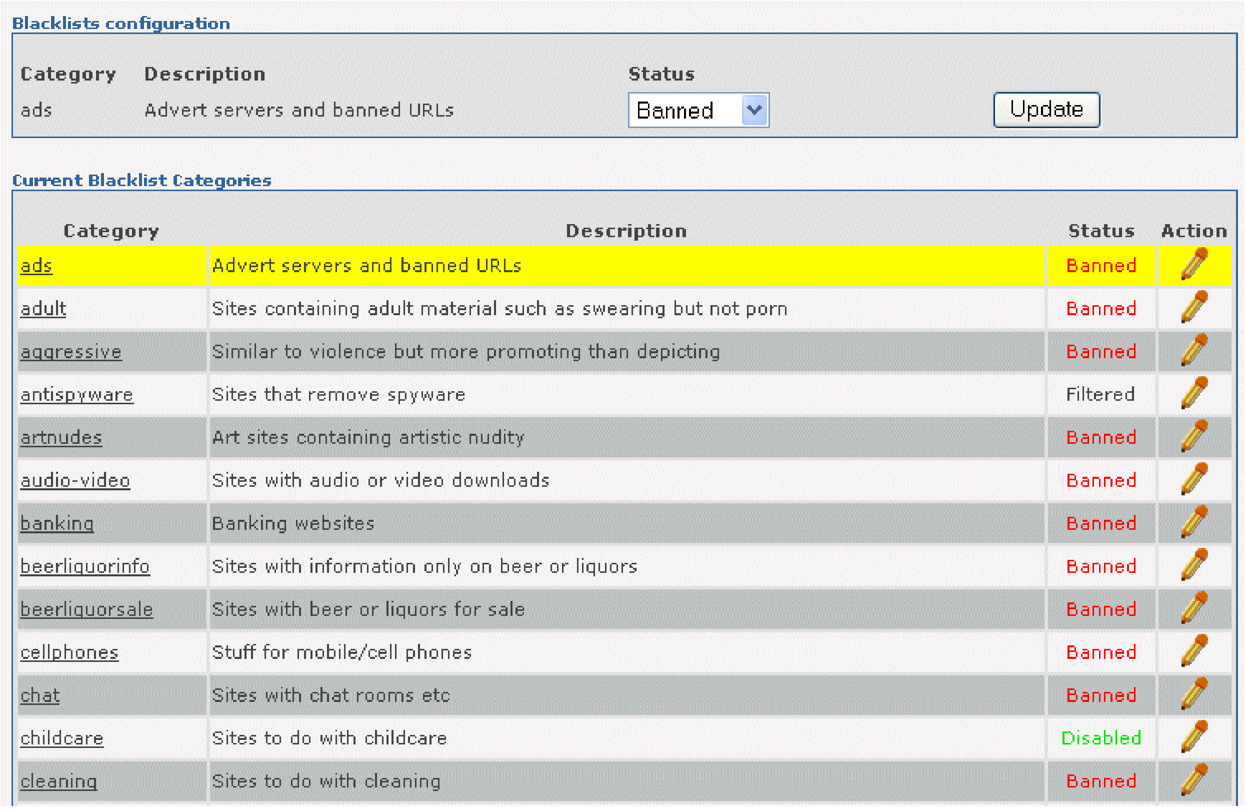
Current Blacklist Categories

Category	Description	Status	Action
ads	Advert servers and banned URLs	Banned	✎
adult	Sites containing adult material such as swearing but not porn	Banned	✎
aggressive	Similar to violence but more promoting than depicting	Banned	✎
antispyware	Sites that remove spyware	Filtered	✎
artnudes	Art sites containing artistic nudity	Banned	✎
audio-video	Sites with audio or video downloads	Banned	✎
banking	Banking websites	Banned	✎
beerliquorinfo	Sites with information only on beer or liquors	Banned	✎
beerliquorsale	Sites with beer or liquors for sale	Banned	✎
cellphones	Stuff for mobile/cell phones	Banned	✎
chat	Sites with chat rooms etc	Banned	✎
childcare	Sites to do with childcare	Disabled	✎
cleaning	Sites to do with cleaning	Banned	✎
clothing	Sites about and selling clothing	Banned	✎
culinary	Sites about cooking et al	Banned	✎
dating	Sites about dating	Banned	✎

Editing Blacklist Categories

1. From the Administration Interface, click on the Filters button. New sets of buttons appear. By default the `Content Filter Control` page appears.
2. Next, you will need to click on the blacklists button. The `Blacklist` page appears. The only panel on this page is the `Current Blacklists Categories` panel. *See Figure 6.26: Content Filter page – Current Blacklist Categories pane above.*
3. Click the ✎ icon associated with the category you want to edit. The details for the phrase or word are placed in the `Blacklists Configuration` panel. *See Figure 6.27: Content Filter page – Edit Blacklist Category.*

Figure 6.27: Content Filter Page – Edit Blacklist Category



Blacklists configuration

Category	Description	Status	
ads	Advert servers and banned URLs	Banned	Update

Current Blacklist Categories

Category	Description	Status	Action
ads	Advert servers and banned URLs	Banned	✎
adult	Sites containing adult material such as swearing but not porn	Banned	✎
aggressive	Similar to violence but more promoting than depicting	Banned	✎
antispyware	Sites that remove spyware	Filtered	✎
artnudes	Art sites containing artistic nudity	Banned	✎
audio-video	Sites with audio or video downloads	Banned	✎
banking	Banking websites	Banned	✎
beerliquorinfo	Sites with information only on beer or liquors	Banned	✎
beerliquorsale	Sites with beer or liquors for sale	Banned	✎
cellphones	Stuff for mobile/cell phones	Banned	✎
chat	Sites with chat rooms etc	Banned	✎
childcare	Sites to do with childcare	Disabled	✎
cleaning	Sites to do with cleaning	Banned	✎

4. You are only allowed to make changes to the status. Click on the drop down menu and select the new status.

5. Click the Update button when you are down with your changes. You can view the changes you made in the `Current Blacklists Categories` panel.

Blanket Block

The blanket block check box at the top of the page allows you to block out ALL websites other than those specifically allowed in the whitelist, or lists set to exception. This is useful in a setting where you want machines to only be able to access a very small subset of websites.

Blanket IP Block

This check box stops clients from entering the IP address of a website to get around the filtering. This should be enabled to keep people from accessing things they should not.

Automatic Blacklist Updating

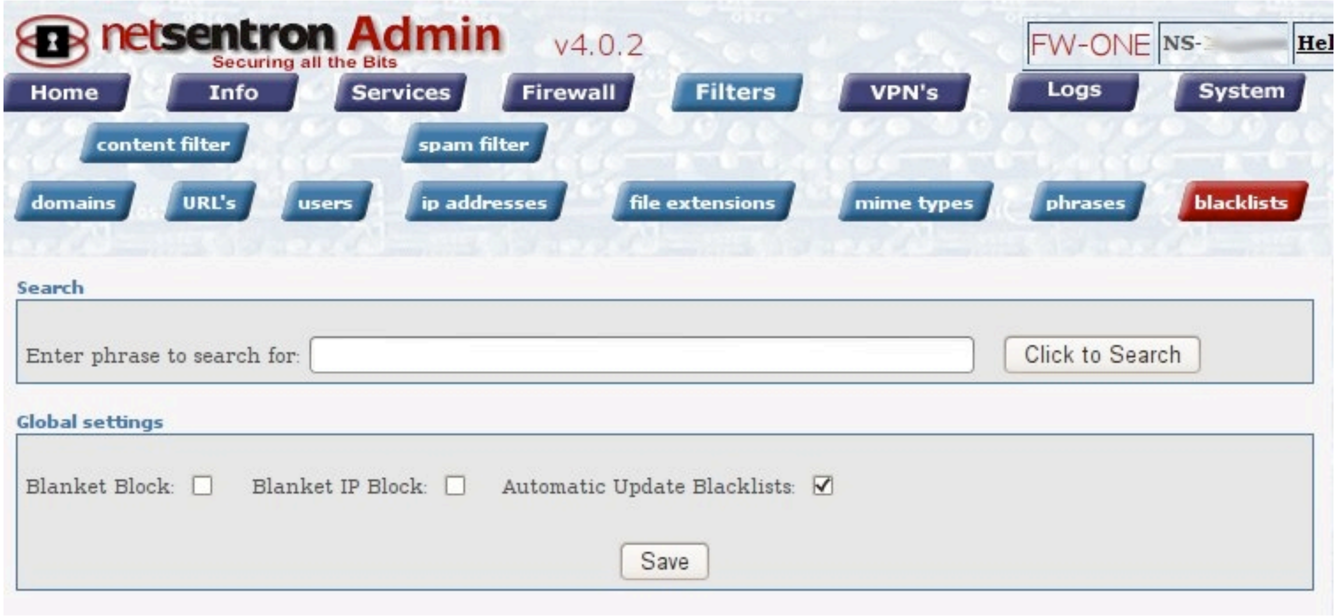
As of version 4.0.2, we have added the ability for the NetSentron to update the blacklists on a daily basis. Blacklists on the NetSentron are used as a first line of defense to block unwanted or inappropriate sites. If a site is not in a blacklist, we still scan the page for inappropriate content.

If you wish to be emailed daily notices of the blacklist updates, insure that you configure your NetSentron to connect to an SMTP server, instructions for that are located in Chaper 11 – Mail Configuration.

To enable automatic blacklist updating go to Filters->Blacklists.

There you will see a box labeled Global settings which has three check boxes in it. The third check box labeled Automatic Update Blacklists is the one you are looking for. Check the check box next to it and click Save. That is it, your NetSentron will now do nightly updates to your blacklists. We also do an update to blacklists every three months using the updates page, if you do not wish to use this feature.

Figure 6.28: Automatic Blacklist Update Panel



Search

Enter phrase to search for:

Global settings

Blanket Block: ☐ Blanket IP Block: ☐ Automatic Update Blacklists: ☑

Spam Filtering

The Spam Filter is a filter which attempts to mark unwanted or unsolicited email with a tag in the subject line of the email. The administrator can then set up a filter on the mail client that groups spam together (usually for the purpose of deleting).

Spam Filtering Control

The Spam Filtering Control panel is where you would configure the main settings for the Spam Filter.

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.

2. Click the spam filter button. The Spam Filter page appears. *See Figure 6.29: Spam Filter on page 133.*

3. The Spam Filter page has been divided into four separate panels. The top panel, Spam filtering control, is where you would configure the main settings. The following is a description of the options provided in the Spam filtering control panel.

Enabled Selecting this option enables the spam setting.

Required Hits This option sets the number of required hits n.nn required before a mail is considered spam. n.nn can be an integer or a real number. 5.0 is the default setting, and is quite aggressive. 10.0 is the far end of the spectrum and will allow a lot of spam to pass by the filter.

Subject Line Tag

Key in words or characters that will be added to the subject line of an email that has been tagged as spam. This allows you to add a filter to you mail client that will catch these spam tagged emails and deal with them using the filtering rules of your mail client.

Show Hits In Subject Line

This will add the (#.## / #.##) to the subject line of the tagged emails. The first #.## represents the count (or hits) that was totaled for this piece of mail. And the second #.## represents the setting that you have selected in the `Required hits` field.

4. Once you have selected your settings click on the Save button.

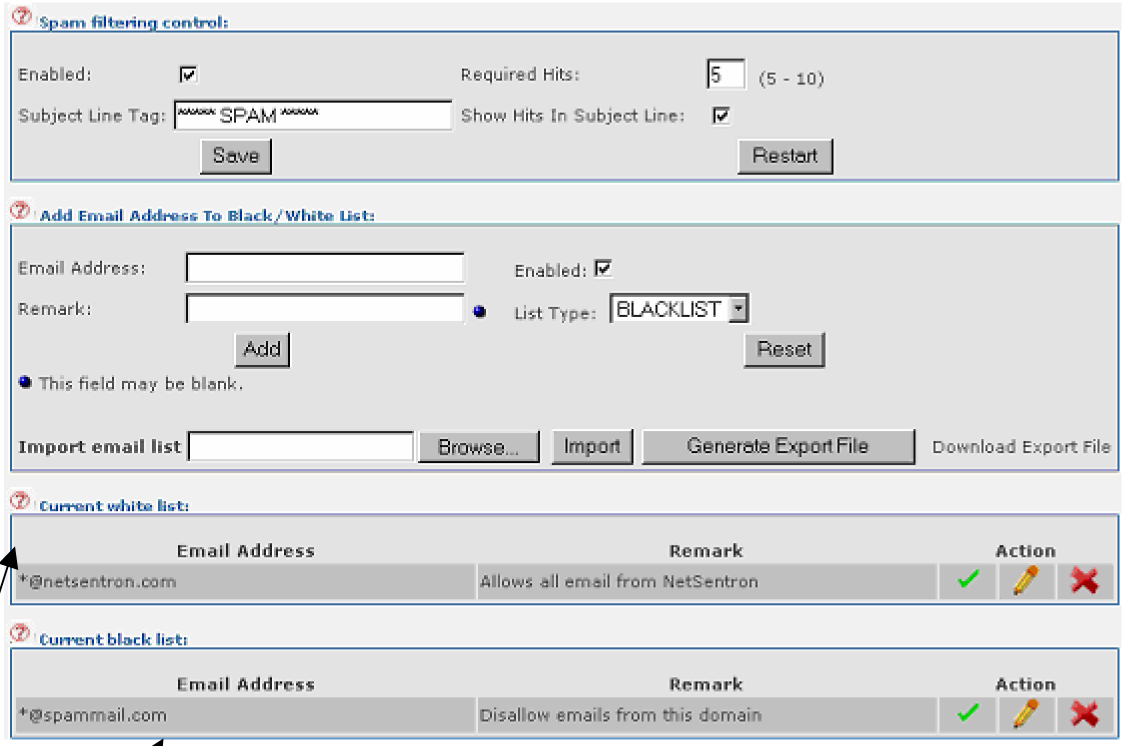
NOTE

For the Spam filter to work, make sure you have selected **Enabled**. Click on the Save button. You should see warning message stating that you need to restart the Spam Filter before changes take effect.

⚠ It is highly recommended to check all email clients are closed before restarting the Spam Filter.

5. Click on the Restart button.

Figure 6.29: Spam Filter



Spam filtering control:

Enabled: ☑ Required Hits: 5 (5 - 10)

Subject Line Tag: ***** SPAM ***** Show Hits In Subject Line: ☑

Add Email Address To Black/White List:

Email Address: Enabled: ☑

Remark: ● List Type: BLACKLIST

● This field may be blank.

Import email list

Current white list:

Email Address	Remark	Action
*@netsentron.com	Allows all email from NetSentron	✓ ✎ ✗

Current black list:

Email Address	Remark	Action
*@spammail.com	Disallow emails from this domain	✓ ✎ ✗

Current White
and Black List

Working with Email Lists

Adding an Email Address to a Black or White List

This option allows you to add an email address to the black or white list. The white list is the list of allowed email addresses and the black list is the list of denied email addresses, or addresses that will always be tagged as Spam.

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.

2. Click the spam filter button. The `Spam Filter` page appears. *See Figure 6.29: Spam Filter.*

3. The `Spam Filter` page has been divided into four separate panels. The second panel down is where you would add email addresses to the black and white lists.

4. In the `Email Address` field key in the email address you want to have listed. Place an asterisk in front of the domain name to disallow all email.

> **NOTE**
>
> Whitelist and blacklist addresses are file-glob-style patterns, so friend@somewhere.com, *@isp.com, or *.domain.net will all work. Specifically, * and ? are allowed, but all other metacharacters are not. Regular expressions are not used for security reasons.

5. In the Remark field key in a description of the new rule you are adding.

6. To enable, make sure the enabled button has been checked.

7. In the `List Type` field, use the drop down menu to select the list you want to add the address to and the click on the Add button. The email address you added will be listed below in the selected white/black list panel. *See Figure 6.28: Spam Filter.*
You should see warning message stating that you need to restart the Spam Filter before changes take effect.

> ⚠ It is highly recommended that make sure all email clients are closed before restarting the Spam Filter.

8. Click on the Restart button. The changes have taken effect.

Exporting Email Lists from the NetSentron

Exporting email lists from the NetSentron gives the administrator the ability to take existing email lists from one NetSentron to use on another NetSentron; therein saving time from having to re-enter all the lists again. Exporting email lists is used in conjunction with the import feature also found on the Spam Filter page. For instruction on importing email lists go to *Importing Email Lists to the NetSentron* on page___.

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.

2. Click the spam filter button. The `Spam Filter` page appears. *See Figure 6.29: Spam Filter on page 133.*

3. The first step is to generate an export file of the email list. Click on the Generate Export File button. The file has been generated.

4. Next, right click on the `Download Export File` link. An Option panel will appear. Click on the `Save As` option. The Save As dialogue box will open.

> **NOTE**
>
> The file will appear in the `File name`: field.

5. Using the `Save in:` drop down box, select where you want to save the file, and then click on the Save button. The file has been saved.

> **NOTE**
>
> Depending on which windows operating systems you are using the file will be saved as a .tar or .tgz.

6. To import this file into another NetSentron follow the instruction on *Importing Email Lists to the NetSentron*.

Creating Email Lists using a .txt file

The NetSentron allows for the administrator to create and save email lists all in one step outside of the NetSentron. Once a list has been created it can be uploaded to the Spam Filter page. For instruction on importing email lists go to *Importing Email Lists to the NetSentron.*

1. Open up a text editor (*for example Notepad*).

2. To create an email list using a text editor you must first enter each email address individually. Each line you enter represents one email address in the list. (i.e. *1,WHITELIST,*@netsentron.com, Allows all email from NetSentron,on*).

3. On one line key in the following criteria in order as listed, separated by commas with no spaces.

Criteria	**Description**
Sequence Number	For example if this is the first email address on your list the number would be 1. The second email would be number 2 and so on.
WHITELIST or BLACKLIST	Only key in the list you want the email address located in. For example you want to allow the email address then you would only key in

NOTE

The number must be of numeric *(1 not one)* value.

WHITELIST.

NOTE

Always use CAPS when entering the list name.

E-mail Address	Key in the email address you want to have listed. Place an asterisk in front of the domain name to disallow all email.

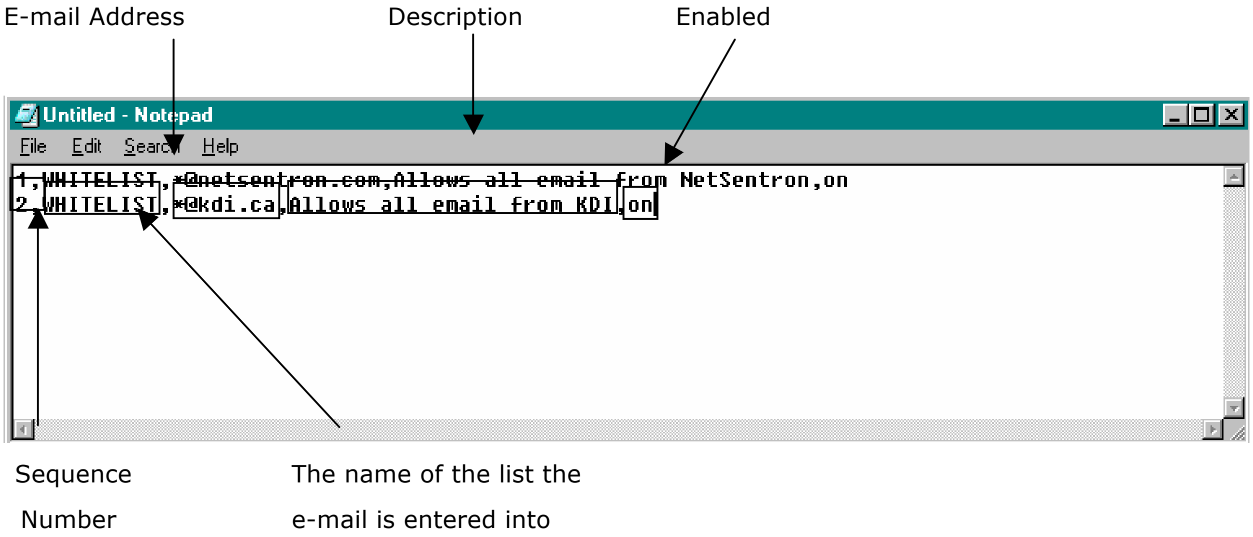
NOTE

whitelist and blacklist addresses are file-glob-style patterns, so friend@somewhere.com, *@isp.com, or *.domain.net will all work. Specifically, * and ? are allowed, but all other metacharacters are not. Regular expressions are not used for security reasons.

Description	Key in a description of the new rule you are adding.
on or off	To have the address you are adding to the list enabled you would key in ***on***. If you want the address you are adding disabled you would key in *off*.

4. Once you have entered all the criteria, save your file. For an example see *Figure 6.30: Example Email list* below*.* Now that your email list has been created, follow the instruction *Importing Email Lists to the NetSentron,* below, to import your email list to the NetSentron.

Figure 6.30: Example Email List



```
1,WHITELIST,*@netsentron.com,Allows all email from NetSentron,on
2,WHITELIST,*@kdi.ca,Allows all email from KDI,on
```

Importing Email Lists to the NetSentron

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.
2. Click the spam filter button. The `Spam Filter` page appears. *See Figure 6.29: Spam Filter on page 133.*
3. Click on the Browse... button. The `Choose File` dialog box will appear.
4. Locate the email list you want to import and double click on it. The `Choose File` dialog box disappears. The file you selected has been automatically inserted in the `Import email` list field.

5. Now that you have selected the email list you want to import, click on the Import button. The NetSentron has automatically inserted the email list into the `Current white and/or black list` panels.

NOTE

Before the changes can take effect you will need to restart the Spam Filter.

⚠ It is highly recommended to check all email clients are closed before restarting the `Spam Filter`.

6. Click the Restart button

Disabling/Enabling Spam Email Rules

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.
2. Click the spam filter button. The `Spam Filter` page appears.
3. Select the email address you want to disable, and then click on the ✓ icon. You should now see a small ⊘ icon. If you want to enable the email rule, click on the small ⊘ icon and the ✓ icon will be showing.

NOTE

You should see warning message stating that you need to restart the Spam Filter before changes take effect. It is highly recommended that make sure all email clients are closed before restarting the Spam Filter.

⚠ It is highly recommended to check all email clients are closed before restarting the Spam Filter.

4. Click the Restart button.

Editing an Email Address on a Black or White List

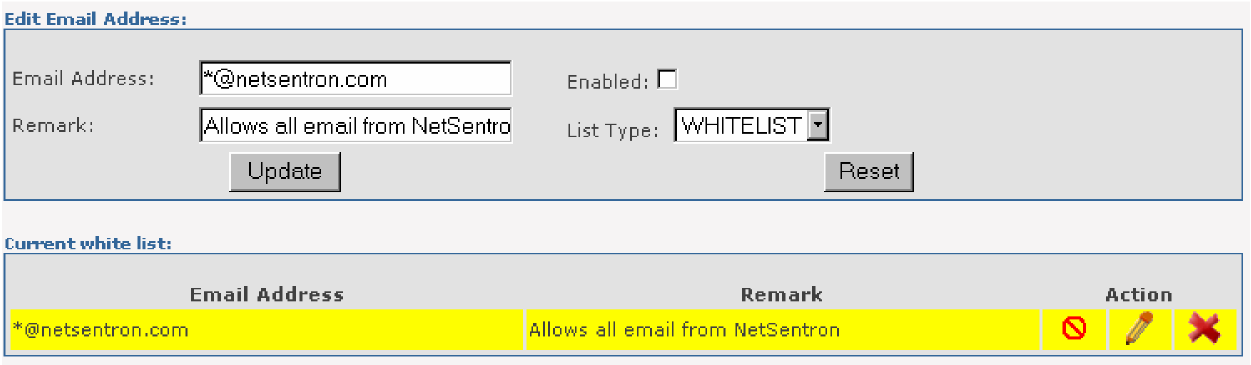
1. From the Administration Interface, click on the Filters button. New sets of buttons appear.
2. *Click* the spam filter button. The `Spam Filter` page appears. *See Figure 6.29: Spam Filter on page 133.*

3. Locate the email address you want to make the changes to and then click on the ✎ icon. The details for that email are placed in the `Edit Email Address` panel. *See Figure 6.31:Spam-Edit Email Addresses.*

NOTE

The address you are editing is highlighted yellow.

Figure 6.31: Spam – Edit Email Address



Edit Email Address:

Email Address: *@netsentron.com

Enabled: ☐

Remark: Allows all email from NetSentro

List Type: WHITELIST ▾

Current white list:

Email Address	Remark	Action		
*@netsentron.com	Allows all email from NetSentron	⦸	✎	✖

4. Make the appropriate changes and then click the Update button.

NOTE
You should see warning message stating that you need to restart the Spam Filter before changes take effect. It is highly recommended that make sure all email clients are closed before restarting the Spam Filter.

5. Click on the Restart button.

Deleting an Email Address from a Black or White List

1. From the Administration Interface, click on the Filters button. New sets of buttons appear.

2. Click the spam filter button. The Spam Filter page appears. *See Figure 6.29: Spam Filter on page 133.*

3. Locate the email address you want to delete and the click on the corresponding ✗ icon. The details for that email are placed in the `Edit Email Address` panel. Once you click the delete icon, the address is automatically removed from the list.

NOTE
You should see warning message stating that you need to restart the Spam Filter before changes take effect. It is highly recommended that make sure all email clients are closed before restarting the Spam Filter.

⚠ It is highly recommended to check all email clients are closed before restarting the Spam Filter.

4. Click on the Restart button.

Chapter 7 Firewall

The purpose of the Firewall is to protect all your computers sitting on your network from any hacking attempts made against you. This Firewall section of the manual allows the administrator to add all sorts of firewall rules. These types of rules would include Port Forwarding, and External Service Access rules. Other features would include: allowing the administrator to edit hosts as well as block certain IP addresses. Also, from this section the administrator can make certain changes to some of the advanced network settings.

Port Forwarding

The NetSentron allows you to forward incoming connection requests to a specific port to any system on your Internal Network or DMZ network. The Port Forwarding Administration page has been divided into two separate panels. The Add a New Rule Panel gives the administrator the ability to add new rules. The Current Rules panel lists the port forwarding rules added.

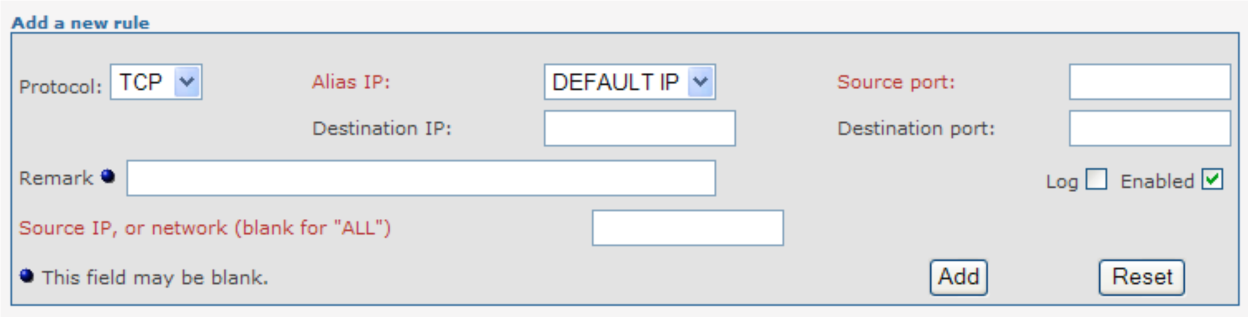
Adding Port Forwarding Rules

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click the port forwarding button. The Port Forwarding administration page appears. *See Figure 7.0: Port Forwarding- Add a new Rule* on the next page. You will need to fill in the following fields:

Protocol	The TCP/UDP drop down list allows you to choose which protocol this rule will follow. Most regular servers use TCP. Some game servers and chat servers use UDP. If the protocol is not specified in the server documentation, then it is usually TCP. Click on the drop box to choose either TCP, UDP or GRE
Alias IP	IP address of the External (RED) interface card.
Source Port	Determines the port that the requests will connect to your network on.
Destination IP	Determines which IP address the incoming requests are forwarded to. This is the address on the green or orange network.
Destination Port	Determines the port that the incoming requests will be forwarded to on the Destination IP.
Remark	Key in any remarks pertaining to the rule.
Log	Checking the log box will enable logging of the port forwarding rule. These logs will show up on the Firewall Logs page
Enabled	Check the box to enable the new rules before adding.
Source IP, or network (blank for "ALL")	Key in an individual IP address of the External (RED) interface card. Or leave it blank to allow all.

Figure 7.0: Port Forwarding – Add A New Rule



Add a new rule

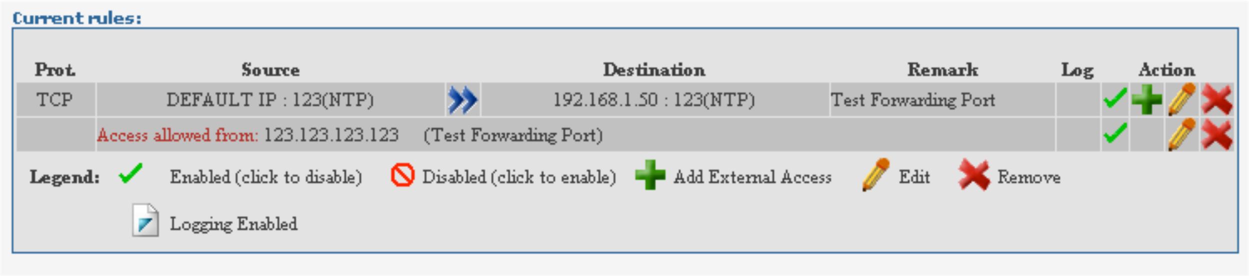
Protocol:	TCP	Alias IP:	DEFAULT IP	Source port:	
		Destination IP:		Destination port:	
Remark ●				Log □	Enabled ☑
Source IP, or network (blank for "ALL")					

● This field may be blank.

Add Reset

3. Once you have entered the information pertaining to the new rule, click the Add button. The new rule will be listed in the Current rules panel. *See Figure 7.1: Port Forwarding – Current Rules* below.

Figure 7.1: Port Forwarding - Current Rules



Current rules:

Prot.	Source		Destination	Remark	Log	Action
TCP	DEFAULT IP : 123(NTP)	»	192.168.1.50 : 123(NTP)	Test Forwarding Port		✓ + ✎ ✖
	Access allowed from: 123.123.123.123 (Test Forwarding Port)					✓ ✎ ✖

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) + Add External Access ✎ Edit ✖ Remove
✎ Logging Enabled

Restricting Access to Port Forwarding Rules

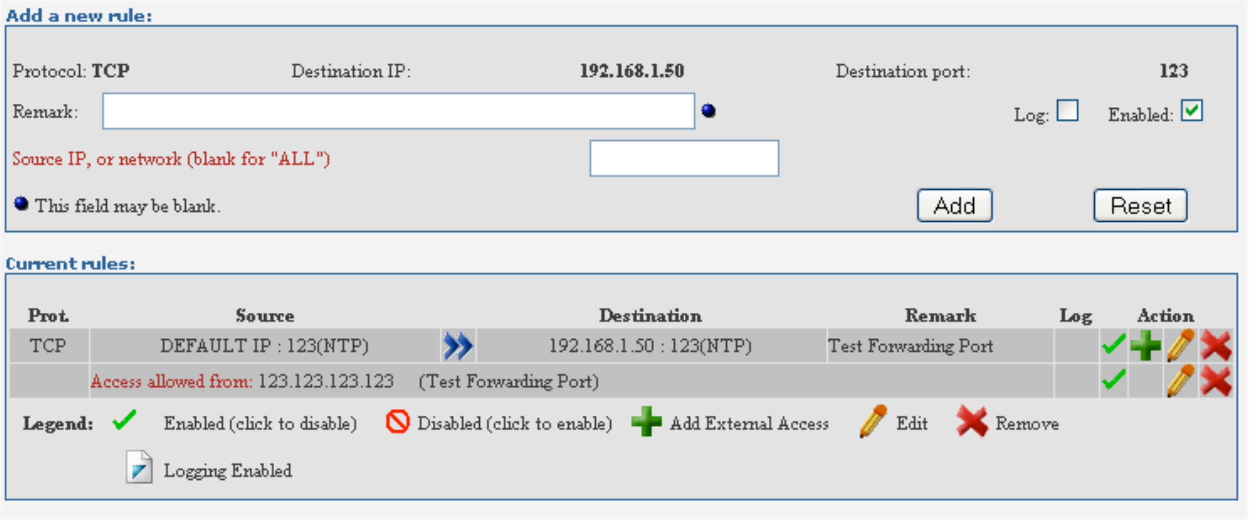
When you add a Port Forwarding rule you are leaving the access open to everyone. The following are instructions on how to allow only specific IP addresses access.

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.
2. Click the port forwarding button. The Port Forwarding administration page appears. *See Figure 7.2:Adding Restrictions,*on the next page.
3. Click the + icon on the same line of the rule you want to add restrictions too. The Add a new rule panel has been altered.

NOTE

You only have access to the Remark and Source IP fields.

Figure 7.2: Adding Restrictions To Port Forwarding Rule



Add a new rule:

Protocol: TCP Destination IP: 192.168.1.50 Destination port: 123

Remark: ● Log: □ Enabled: ☑

Source IP, or network (blank for "ALL")

● This field may be blank.

Add Reset

Current rules:

Prot.	Source		Destination	Remark	Log	Action
TCP	DEFAULT IP : 123(NTP)	»	192.168.1.50 : 123(NTP)	Test Forwarding Port		✓ ✚ ✎ ✖
	Access allowed from: 123.123.123.123 (Test Forwarding Port)					✓ ✎ ✖

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) ✚ Add External Access ✎ Edit ✖ Remove

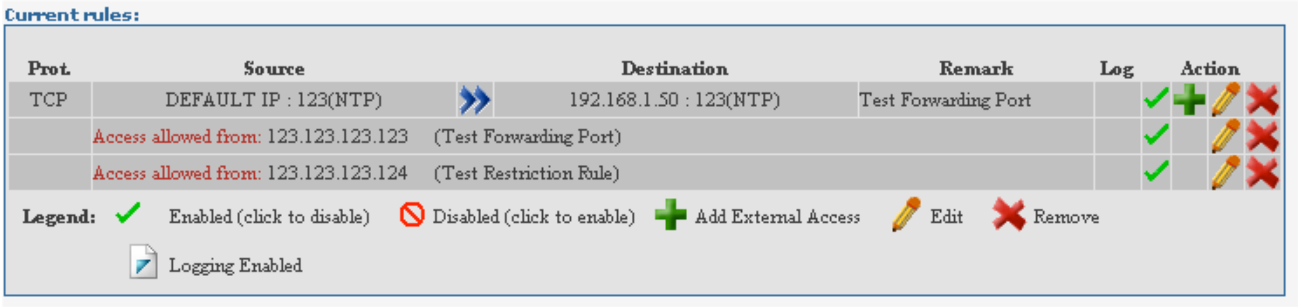
Logging Enabled

4. Key in a remark in the Remark field (any remarks pertaining to the restriction you are placing on the rule)

5. Key in address of the IP that you are allowing, and then click the Add button. The IP that you are allowing access from is listed under the Port Forward rule in the Current rules panel. *See Figure 7.3:Port Forwarding Rule with Restrictions* below.

6. To edit a restriction placed on a Port Forwarding rule click on the corresponding ✎ icon. To remove a restriction placed on a Port Forwarding rule click on the corresponding ✖ icon.

Figure 7.3: Port Forwarding Rule With Restrictions



Current rules:

Prot.	Source		Destination	Remark	Log	Action
TCP	DEFAULT IP : 123(NTP)	»	192.168.1.50 : 123(NTP)	Test Forwarding Port		✓ ✚ ✎ ✖
	Access allowed from: 123.123.123.123 (Test Forwarding Port)					✓ ✎ ✖
	Access allowed from: 123.123.123.124 (Test Restriction Rule)					✓ ✎ ✖

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) ✚ Add External Access ✎ Edit ✖ Remove

Logging Enabled

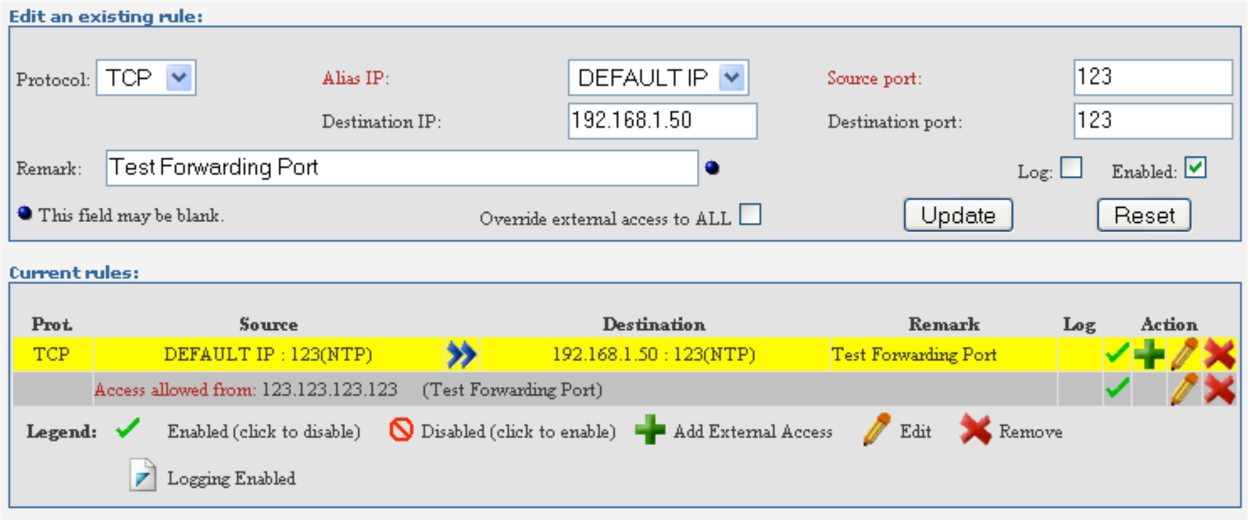
Disabling/Enabling a Port Forwarding Rules

1. From the Administration Interface, click on the **Firewall** button. New sets of buttons appear.
2. Click the **port forwarding** button. The Port Forwarding administration page appears. *See Figure 7.1: Current Rules*.
3. Click the ✓ icon on the same line of the rule you want to disable. The ✓ icon changes to the ⊘ (disabled) icon. To re-enable the rule click on the ⊘ icon and the ✓ re-appears.

Editing Port Forwarding Rules

1. From the Administration Interface, click on the **Firewall** button. New sets of buttons appear.
2. Click the **port forwarding** button. The Port Forwarding administration page appears.
3. Click the ✎ icon on the same line of the rule you want to edit. The details for that rule are placed in the Edit an existing rule panel. *See Figure 7.4: Edit Existing Port Forward* Rule, below*.*

Figure 7.4: Edit Existing Port Forward Rule



Edit an existing rule:

Protocol: TCP	Alias IP:	DEFAULT IP	Source port:	123	
	Destination IP:	192.168.1.50	Destination port:	123	
Remark: Test Forwarding Port ●				Log: □	Enabled: ☑
● This field may be blank.	Override external access to ALL □		Update	Reset	

Current rules:

Prot.	Source		Destination	Remark	Log	Action
TCP	DEFAULT IP : 123(NTP)	»	192.168.1.50 : 123(NTP)	Test Forwarding Port		✓ ✚ ✎ ✖
	Access allowed from: 123.123.123.123 (Test Forwarding Port)					✓ ✎ ✖

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) ✚ Add External Access ✎ Edit ✖ Remove

📝 Logging Enabled

4. Make the appropriate changes and then click the Update button. The Add a new rule panel re-appears. The changes made have been recorded and can be viewed in the Current Rules panel.

Deleting Port Forwarding Rules

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click the port forwarding button. The Port Forwarding administration page appears. *See Figure 7.1: Current Rules.*

3. Click the ✖ icon on the same line of the rule you want to remove. Note: Once you click the delete icon, the rule is removed automatically.

External Access

The External Access page allows you to open up ports to administer the NetSentron remotely.

NOTE

Use with extreme caution as you are opening up your firewall to the Internet. The External Access page has been divided into two panels. The Add a new rule panel allows the administrator the ability to add, edit and delete rules. The `Current Rules` panel lists all the current `External Access` rules.

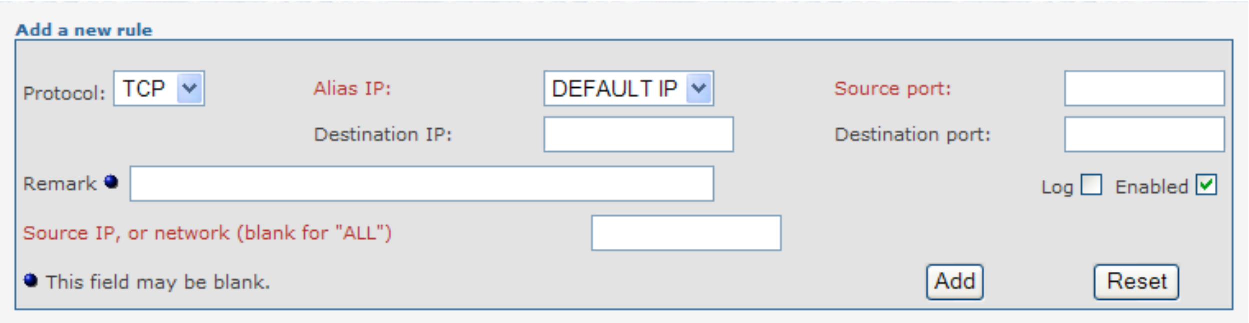
Adding External Access Rules

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click on the external access button. `The External Access` page appears. *See Figure 7.5: External Access Page* on the next page. You will need to fill in the following fields:

Source IP, or network (blank for "ALL")	Allows access from the specified IP address. If left blank it is open up to anyone.
Destination IP	IP address of the External (RED) interface card.
Destination Port	Determines the port that the incoming requests will be allowed in on.
Protocol	The TCP/UDP drop down list allows you to choose which protocol this rule will follow. Most regular servers use TCP. Some game servers and chat servers use UDP. If the protocol is not specified in the server documentation, then it is usually TCP
Log	Checking the log box will enable logging of the external access rule. These logs will show up on the Firewall Logs page
Remarks	Key in any notes pertaining to the rule.
Enabled	Check the box to enable the new rules before adding.

Figure 7.5: External Access Page – Add A New Rule



Add a new rule

Protocol: TCP Alias IP: DEFAULT IP Source port:

Destination IP: Destination port:

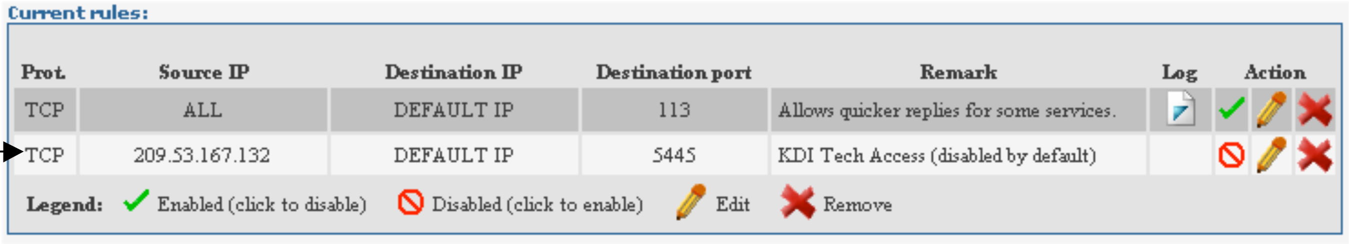
Remark ● Log □ Enabled ☑

Source IP, or network (blank for "ALL")

● This field may be blank.

3. Once you have entered the information pertaining to the new rule, click the Add button. The new rule will be listed in the Current rules panel. *See Figure 7.6: External Access Page* below.

Figure 7.6: External Access Page – Current Rules



Current rules:

Prot.	Source IP	Destination IP	Destination port	Remark	Log	Action
TCP	ALL	DEFAULT IP	113	Allows quicker replies for some services.	📄	✓ ✎ ✖
TCP	209.53.167.132	DEFAULT IP	5445	KDI Tech Access (disabled by default)		⊘ ✎ ✖

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) ✎ Edit ✖ Remove

Shows a list of the current rules

Editing External Access Rules

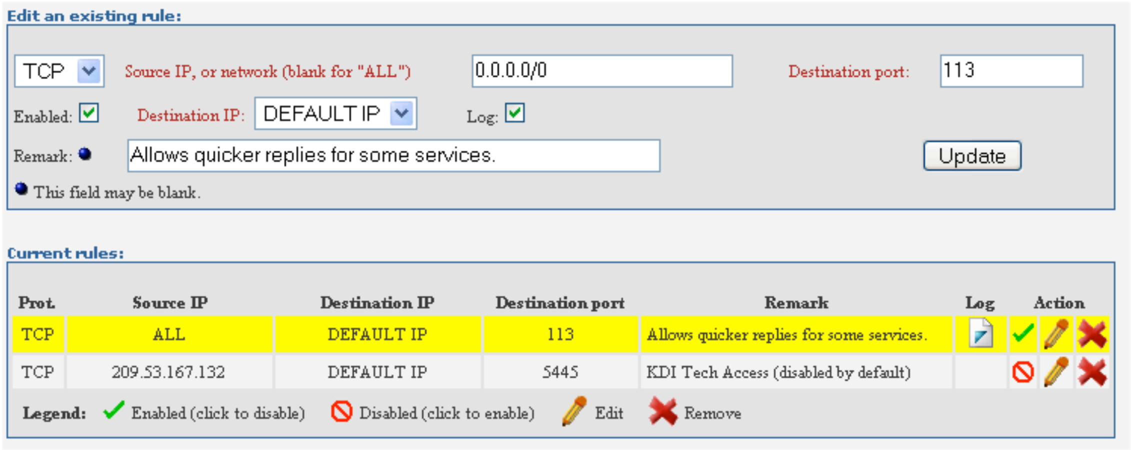
1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click on the external access button. The External Access page appears. To make changes to any External Access Rule you will need to use the `Current Rules` panel. *See Figure 7.6: External Access Page* above.

3. Click the ✎ icon associated with the rule you want to edit. The details for that rule are placed in the `Edit an Existing Rule` panel.

Figure 7.7: External Access Page – Editing an Existing Rule below.

Figure 7.7: External Access Page – Editing an Existing Rule



Edit an existing rule:

TCP ▾ Source IP, or network (blank for "ALL") 0.0.0.0/0 Destination port: 113

Enabled: ☑ Destination IP: DEFAULT IP ▾ Log: ☑

Remark: ● Allows quicker replies for some services. Update

● This field may be blank.

Current rules:

Prot.	Source IP	Destination IP	Destination port	Remark	Log	Action
TCP	ALL	DEFAULT IP	113	Allows quicker replies for some services.	📝	✓ ✎ ✖
TCP	209.53.167.132	DEFAULT IP	5445	KDI Tech Access (disabled by default)		⦸ ✎ ✖

Legend: ✓ Enabled (click to disable) ⦸ Disabled (click to enable) ✎ Edit ✖ Remove

4. Make the appropriate changes and then click on the Update button. The external access rule been updated.

Deleting External Access Rules

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click on the external access button. The External Access page appears. *See*

3. *Figure 7.6: External* Access Page*,* on the previous page.

4. Click the ✖ icon associated with the rule you want to remove.

NOTE

Once you click the delete icon, the rule is removed automatically.

Disabling/Enabling External Access Rules

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.
2. Click on the external access button. The External Access page appears. *See*
3. *Figure 7.6: External Access* Page on the previous page.

4. Click the ✓ icon on the same line of the rule you want to disable. The ✓ icon is changes to the ⊘ (disabled) icon. To re-enable the rule click on the ⊘ icon and the ✓ re-appears.

DMZ Pinholes

A DMZ or Demilitarized Zone (Orange zone) is used to allow a machine on the BLUE LAN to access resources on the GREEN LAN by poking holes in the protective firewall that isolates the BLUE LAN.

Adding a new DMZ Pinhole Rule

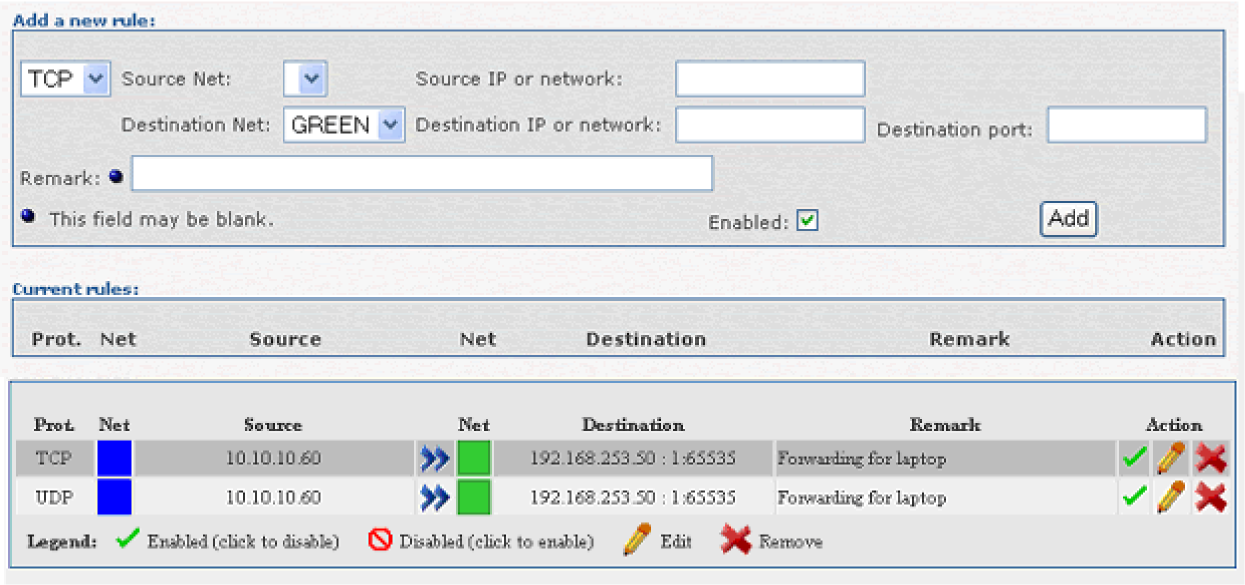
The following is an example of how to allow a machine on BLUE to access a web server on the GREEN LAN. A normal web server usually runs on port 80 TCP, so this is the hole we would need to open up to allow the machine on BLUE access.

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click on the button. The `DMZ Pinhole` page appears. *See Figure 7.8 DMZ Pinholes Page on the next page.*

3. To add a new rule you will use the `Add a New Rule` panel. You will need to fill in the following fields;

Figure 7.8: DMZ Pinholes Page



Add a new rule:

TCP	Source Net:		Source IP or network:		
	Destination Net:	GREEN	Destination IP or network:		Destination port:
Remark: ●					
● This field may be blank.			Enabled: ☑		Add

Current rules:

Prot.	Net	Source	Net	Destination	Remark	Action

Prot.	Net	Source		Net	Destination	Remark	Action
TCP	🟦	10.10.10.60	»	🟩	192.168.253.50 : 1:65535	Forwarding for laptop	✓ ✎ ✗
UDP	🟦	10.10.10.60	»	🟩	192.168.253.50 : 1:65535	Forwarding for laptop	✓ ✎ ✗

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) ✎ Edit ✗ Remove

4. Start by selecting *TCP* from the drop down list.

5. In the `Source Net` field select BLUE. This only makes sense as the source machine is on the BLUE LAN.

6. Next, key in the `Source IP` or `Network` field. This will be the IP or network address of the machine on BLUE. This field will accept entire networks in the format of *192.168.1.0/24* or *92.168.1.0/255.255.255.0* if you wish to configure entire networks.

7. In the Destination Net field, select GREEN as that is where the web server is located.

8. In the `Destination IP` or network field, key in the IP or network address of the web server. Again, an entire network can be specified here instead of a single IP Address

9. In the `Destination Port` field key in ***80*** (Port ranges can be entered here) which is the port that HTTP runs on.

10. In the `Remark` field, key in some form of description of why you have opened this hole up in the security.

11. Once you have keyed in all your settings and you have checked `Enabled`, click on the Add button. You can view the newly created rule in the Current rules panel. The machine on the BLUE LAN will now be able to access the web server on the GREEN LAN.

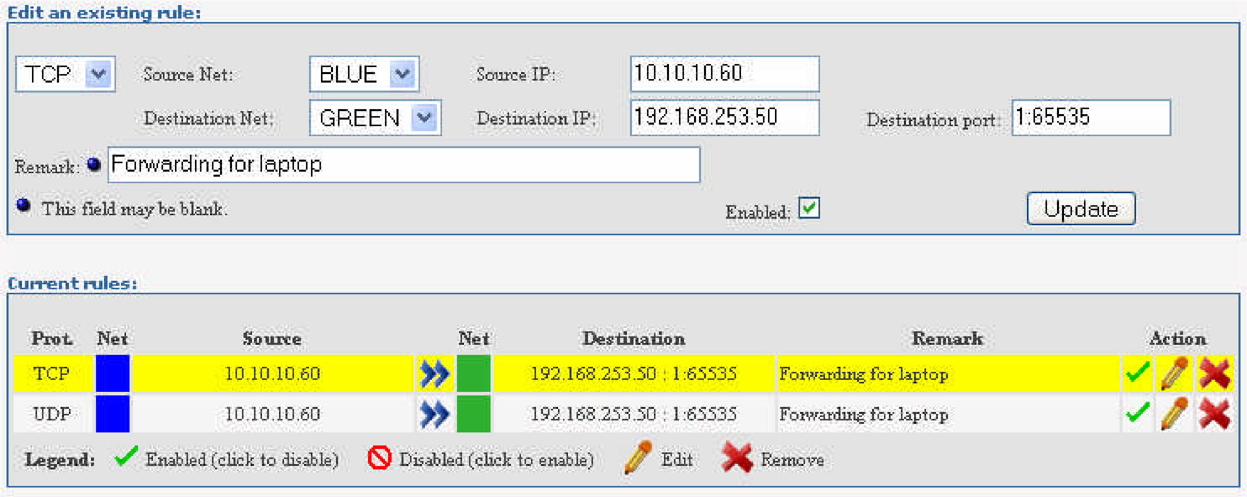
Editing DMZ Pinhole Rules

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click on the dmz pinholes button. The `DMZ Pinholes` page appears.

3. Click the ✎ icon associated with the rule you want to edit. The details for that rule are placed in the `Edit an Existing Rule` panel.(The rule you are editing is highlighted yellow.) *See Figure 7.9, below.*

Figure 7.9: DMZ Pinholes Page - Editing An Existing Rule



Edit an existing rule:

TCP	Source Net:	BLUE	Source IP:	10.10.10.60		
	Destination Net:	GREEN	Destination IP:	192.168.253.50	Destination port:	1:65535

Remark: ● Forwarding for laptop

● This field may be blank.

Enabled: ☑

Update

Current rules:

Prot.	Net	Source		Net	Destination	Remark	Action		
TCP	🟦	10.10.10.60	»	🟩	192.168.253.50 : 1:65535	Forwarding for laptop	✓	✎	✗
UDP	🟦	10.10.10.60	»	🟩	192.168.253.50 : 1:65535	Forwarding for laptop	✓	✎	✗

Legend: ✓ Enabled (click to disable) ⃠ Disabled (click to enable) ✎ Edit ✗ Remove

4. Make the appropriate changes and then click on the Update button. The DMZ Pinhole rule been updated.

Deleting DMZ Pinhole Rules

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click on the dmz pinholes button. The DMZ Pinholes page appears.

3. Click the ✗ icon associated with the rule you want to remove.

   Once you click the delete icon, the rule is removed automatically.

Hosts

The Hosts page allows the administrator to edit the hosts file. This is useful for windows networks that have Linux boxes on them. If a Linux box is entered on this page, you should see them show up in the windows network neighborhood, etc.

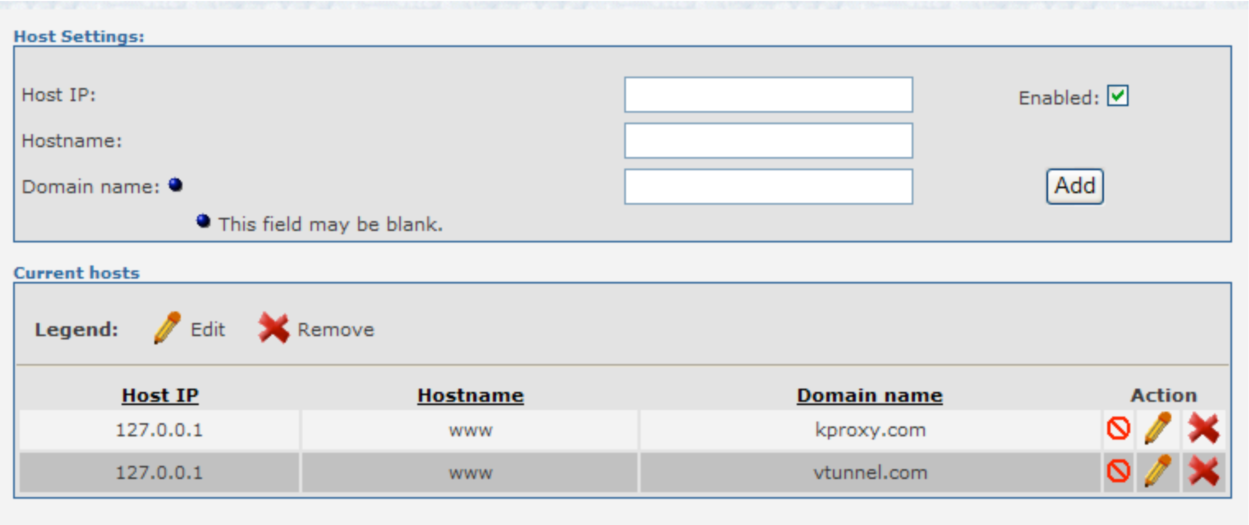
Adding a Host

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click the hosts button. The Hosts page appears. *See* **Error! Reference source not found.**, on the next page.

3. Fill in the fields in the Setting panel and then click the Add button. The settings you added will be displayed in the `Current Hosts` panel.

Figure 7.10: Hosts Administration Page



Host Settings:

Host IP:		Enabled: ☑
Hostname:		
Domain name: ●		Add

● This field may be blank.

Current hosts

Legend: ✎ Edit ✖ Remove

Host IP	Hostname	Domain name	Action
127.0.0.1	www	kproxy.com	⊘ ✎ ✖
127.0.0.1	www	vtunnel.com	⊘ ✎ ✖

Editing a Current Host

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click the hosts button. The `Hosts` page appears. *See* **Error! Reference source not found.**, **Error! Reference source not found.**.

3. Click the ✎ icon associated with the host you want to edit. The details for that host are placed in the Settings panel. Make the appropriate changes and then click the Add button. The host settings have been re-entered in the `Current Hosts` panel.

Removing a Current Host

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click the hosts button. The Hosts page appears. *See* **Error! Reference source not found.**, above

3. Click the ✖ icon associated with the host you want to remove.

NOTE

Once you click the delete icon, the host is removed automatically.

IP Block

The IP Block page allows the administrator to block incoming or outgoing access to an IP Address. It also allows logging of the blocking restrictions. You can also block IP addresses from the Firewall Logs page. For instructions on blocking IP addresses from the Firewall Logs see the section on *Blocking IP Addresses from Firewall Logs Page,* on the next page.

Blocking an IP

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.
2. Click the ip block button. The IP Block page appears. Once you have keyed in your settings, check the enabled box and then click the Add button. The rule you have added in is displayed in `the` Current Rules panel as Figure 7.11 shows below.
3. Figure the next page.
4. In the `Add a New Rule` panel, fill in the fields. The following is a list of all the settings available:

Protocol

The TCP/UDP drop down list allows you to choose which protocol this rule will follow. Most regular servers use TCP. Some game servers and chat servers use UDP. If the protocol is not specified in the server documentation, then it is usually TCP

Source IP or network

Key in the IP address or network you want to block.

Port

Key in the Port range. Leaving the * will include all ports available. If you are keying in port range enter ***a:*** between the range*. i.e. 220:225*

Drop packets

Select this option to give no response if someone is trying to connect to the NetSentron. It would be as if the machine is turned off.

Reject packets

Select this option to give a response if someone is trying to connect to the NetSentron. This basically lets the person know that a machine is present but they cannot access it.

Log

Checking the log box will enable logging of the blocking rule. These logs will show up on the Firewall Logs page.

Enabled

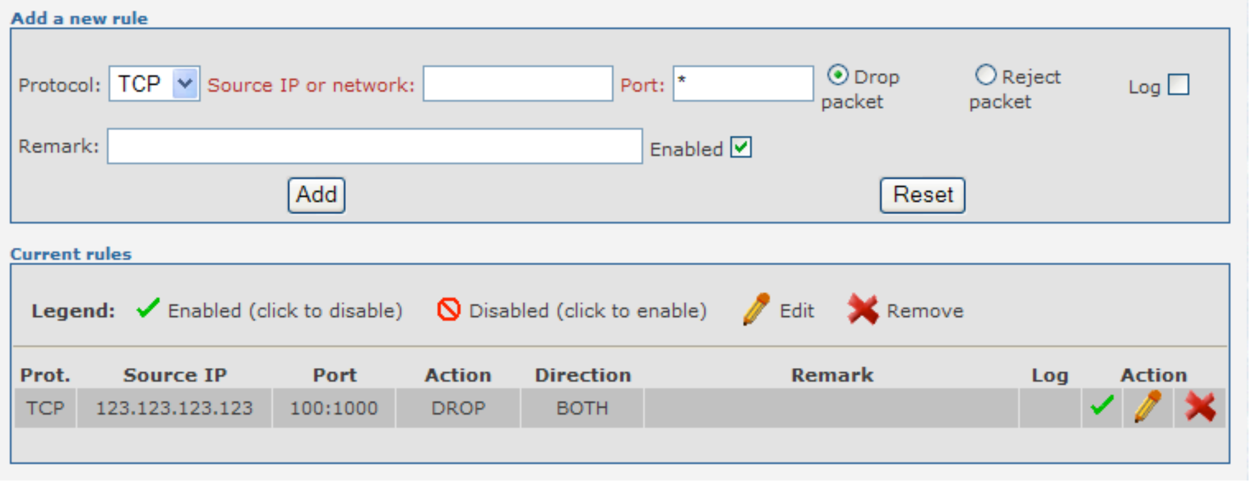
Check the box to enable the new rules before adding.

Remark

Add a brief description of the IP Blocking rule you are adding.

5. Once you have keyed in your settings, check the enabled box and then click the Add button. The rule you have added in is displayed in the `Current Rules` panel as *Figure 7.11* shows below.

Figure 7.11: IP Block Page



Add a new rule

Protocol: TCP Source IP or network: Port: * ● Drop packet ○ Reject packet Log □

Remark: Enabled ☑

Add Reset

Current rules

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) ✎ Edit ✗ Remove

Prot.	Source IP	Port	Action	Direction	Remark	Log	Action
TCP	123.123.123.123	100:1000	DROP	BOTH			✓ ✎ ✗

Editing a Blocked IP

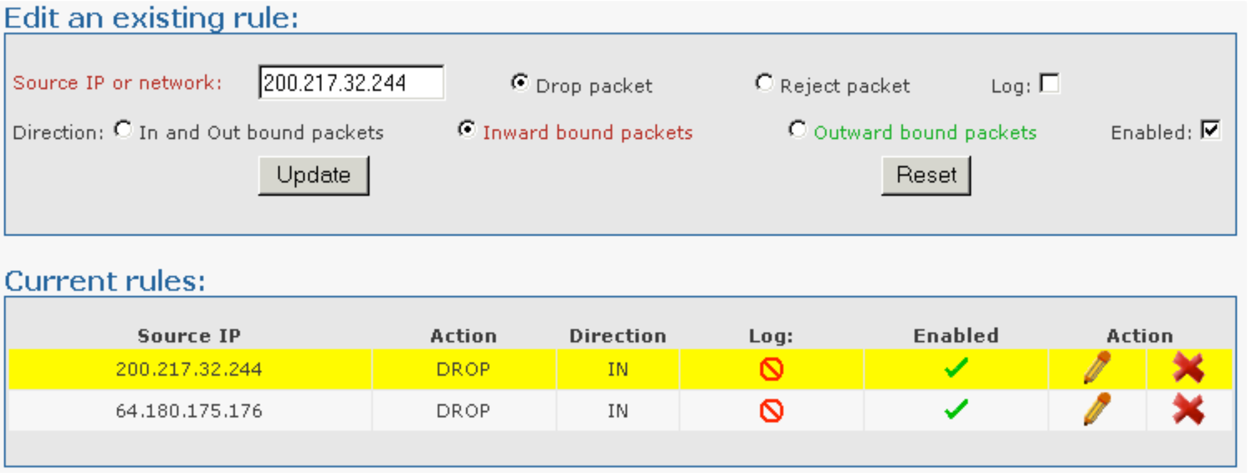
1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click the ip block button. The IP Block page appears. Once you have keyed in your settings, check the enabled box and then click the Add button. The rule you have added in is displayed in the `Current` Rules panel as Figure *7.11 shows below*.

Figure

3. Click the ✏ icon associated with the blocked IP you want edit. The details for that rule are placed in the Edit an existing rule panel. *See Figure 7.4: Edit Existing* Port Forward Rule *Blocked IP* below.

Figure 7.12: Edit Existing Blocked IP



Edit an existing rule:

Source IP or network: 200.217.32.244 ● Drop packet ○ Reject packet Log: □

Direction: ○ In and Out bound packets ● Inward bound packets ○ Outward bound packets Enabled: ☑

Current rules:

Source IP	Action	Direction	Log:	Enabled	Action	
200.217.32.244	DROP	IN	⊘	✓	✏	✖
64.180.175.176	DROP	IN	⊘	✓	✏	✖

4. Make the appropriate changes and then click the Update button. The `Add a New Rule` panel appears. The changes made have been recorded.

Removing a Blocked IP

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click the ip block button. The IP Block page appears. Once you have keyed in your settings, check the enabled box and then click the Add button. The rule you have added in is displayed in the `Current Rules` panel as Figure 7.11 shows below.

3. Figure Click the ✖ icon associated with the blocked IP you want to remove.

> **NOTE**
>
> Once you click the delete icon, the blocked IP is removed automatically.

Enabling/Disabling a Blocked IP

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click the ip block button. The IP Block page appears. Once you have keyed in your settings, check the enabled box and then click the Add button. The rule you have added in is displayed in the `Current Rules` panel as Figure 7.11 shows below.

3. Figure

4. Click the ✓ icon associated with the blocked IP you want to disable. The ✓ icon as been replaced with a ⊘. To enable the Blocked IP Rule simply click on the ⊘ icon and the ✓ icon is returned and your IP Blocking rule is re-enabled.

Advanced Networking

The Advanced Networking page allows you to set the ping to be disabled so no one can ping you. `Advanced Network Settings` enables SYN Cookies and can block multicast traffic as well as ignore IGMP packets.

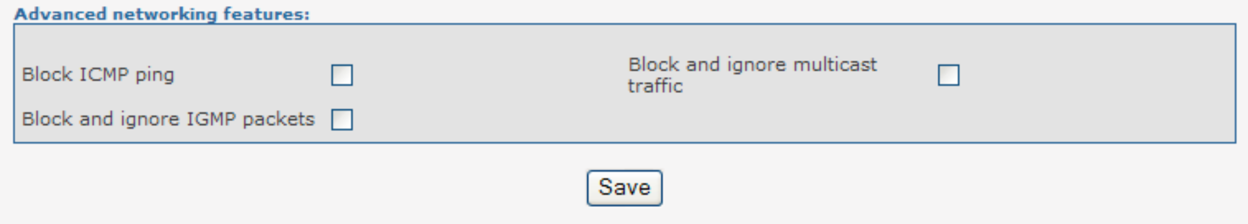
> **NOTE**
>
> Only use these settings if you are having problems.

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.
2. Click on the advanced networking button. The Advanced Networking page appears. *See Figure 7.13: Advanced Networking Page*, on the next page.
3. Click on the setting you want to enable. See the following list for a description of the settings on this page:

Block ICMP Ping	Selecting this option allows the administrator to stop anyone from using the ping utility to identify your machine.
Block and ignore IGMP packets	Many windows exploits make use of fragmented packets sent through this protocol.
Block and ignore multicast traffic	Similar to broadcast traffic. It is like selective broadcast; only those that request the traffic get it. Allows a one to many communication rather than one to one

4. Click the Save button to enable the settings.

Figure 7.13: Advanced Networking Page



Advanced networking features:

Block ICMP ping □

Block and ignore multicast traffic □

Block and ignore IGMP packets □

Save

ByPass Proxy

The Bypass Proxy page gives the administrator the ability to allow certain IP address to be by passed through the Content Filter System. This is sometimes required by some scholastic systems that are running on Java or Oracle based systems. If you are having trouble with an remote application working, try adding the remote IP address to bypass proxy and choosing the specific port the app runs on, or all ports.

> ⚠ It is advised to use this feature with caution.

Adding a New Bypass Proxy Rule

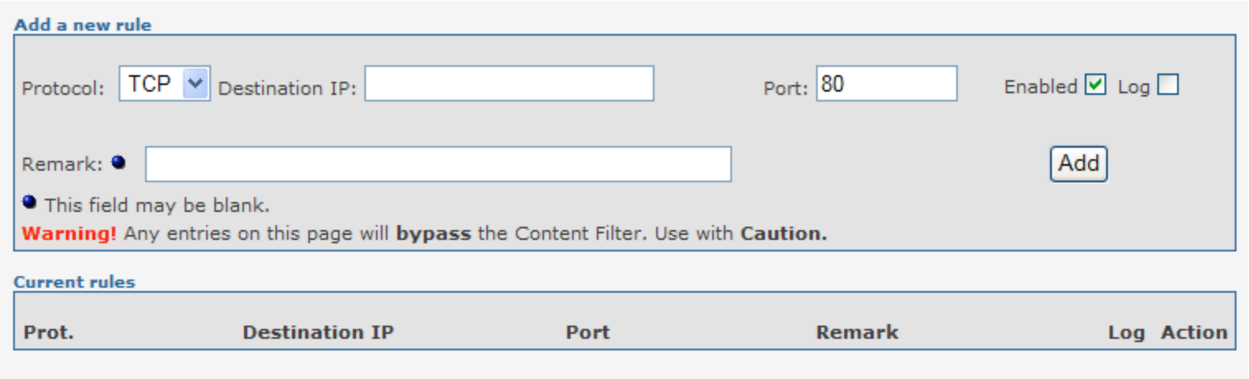
1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.
2. Click on the bypass proxy button. The `Bypass Proxy` page appears. *See Figure 7.14: Bypass Proxy Pgae,* on the next page.

3. In the `Add a New Rule` panel, fill in the fields. The following is a list of all the settings available in the `Add a New Rule` panel.

Protocol	The TCP/UDP drop down list allows you to choose which protocol this rule will follow. Most regular servers use TCP. Some game servers and chat servers use UDP. If the protocol is not specified in the server documentation, then it is usually TCP.
Destination IP	Determines which IP addresses will be bypassed by the Content Filter.
Port	Key in the Port range. Leaving the ***** will include all ports available. If you are keying in port range enter ***a:*** between the range*.* *i.e. 220:225*
Enabled	Check the box to enable the new rules before adding.
Log	Checking the log box will enable logging of the bypass proxy rule. These logs will show up on the Firewall Logs page.
Remark	Add a brief description of the ByPass Proxy rule you are adding.

4. Once you have entered your settings, check enabled and then click the Add button. The new rule is displayed in the `Current Rules` panel.

Figure 7.14: Bypass Proxy Page



Add a new rule

Protocol: TCP Destination IP: Port: 80 Enabled ☑ Log □

Remark: ● Add

● This field may be blank.

Warning! Any entries on this page will **bypass** the Content Filter. Use with **Caution.**

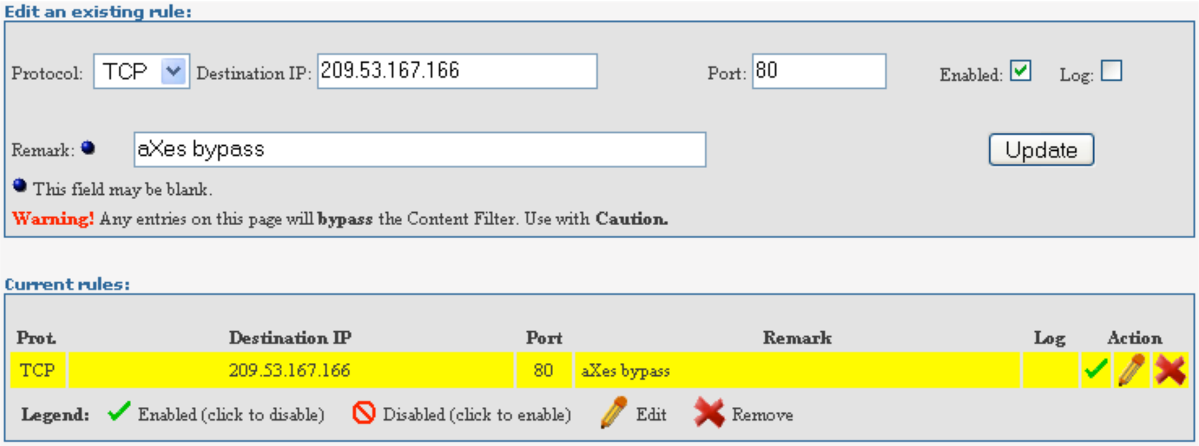
Current rules

Prot.	Destination IP	Port	Remark	Log	Action

Editing Bypass Proxy Rules

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.
2. Click on the bypass proxy button. The `Bypass Proxy` page appears.
3. Click the ✎ icon associated with the Bypass Proxy rule you want to edit. The details for that rule are placed in the Edit an existing rule panel. *See Figure 7.15: Bypass Proxy Page- Editing a Rule* below.

Figure 7.15: Bypass Proxy Page – Editing a Rule



Edit an existing rule:

Protocol: TCP Destination IP: 209.53.167.166 Port: 80 Enabled: ☑ Log: □

Remark: ● aXes bypass Update

● This field may be blank.

Warning! Any entries on this page will **bypass** the Content Filter. Use with **Caution.**

Current rules:

Prot.	Destination IP	Port	Remark	Log	Action
TCP	209.53.167.166	80	aXes bypass		✓ ✎ ✗

Legend: ✓ Enabled (click to disable) ⃠ Disabled (click to enable) ✎ Edit ✗ Remove

4. Make the appropriate changes and then click the Update button. You can view the changes you made in the Current rules panel.

Removing Bypass Proxy Rules

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click on the bypass proxy button. The `Bypass Proxy` page appears.

3. Click the ✖ icon associated with the Bypass Proxy rule you want to remove.

NOTE
Once you click the delete icon, the Bypass Proxy rule is removed automatically.

Disabling/Enabling Bypass Proxy Rules

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear

2. Click on the bypass proxy button. The `Bypass Proxy` page appears

3. Click the ✓ icon associated with the Bypass Proxy rule you want to disable. The ✓ icon as been replaced with an 🛇 icon. To enable the Bypass Proxy Rule simply click on the 🛇 icon and the ✓ icon is returned and your Bypass Proxy rule is re-enabled.

Static Routing

Static routing is used to redirect packets to another network segment from the current network segment. *See Figure* below for an example of where static routing would be used.

Figure 7.16: Example Of Where Static Routing Would Be Used

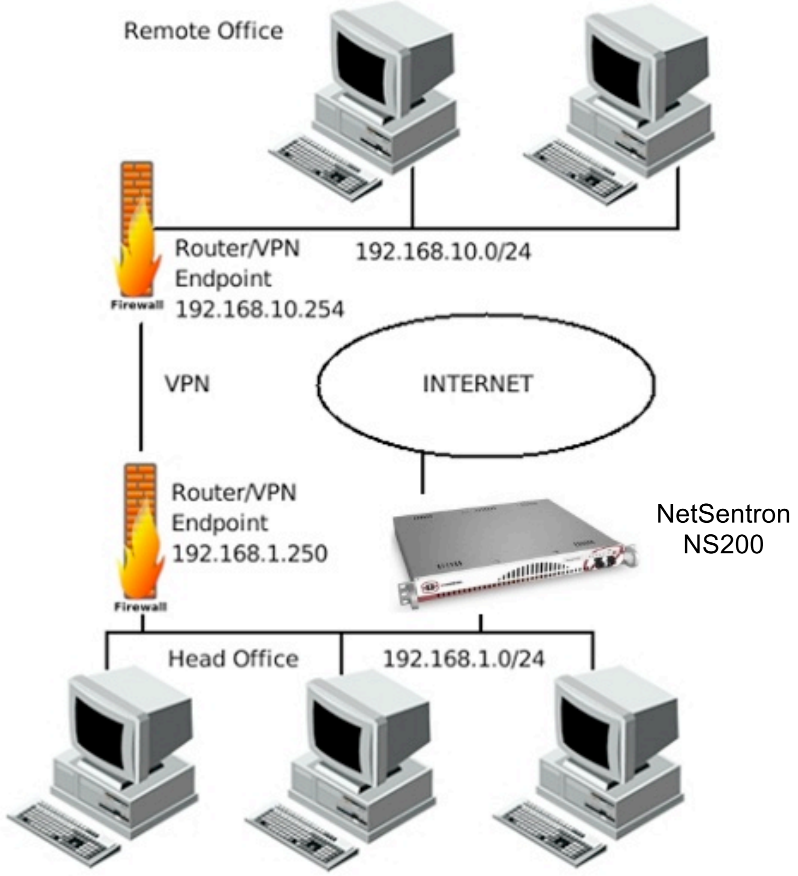


Figure 7.16 shows two offices connected with a VPN. One is the head office and the other is a remote office. At the Head Office, the NetSentron is the Internet Gateway, which means all traffic goes through the NetSentron. Because all traffic goes through the NetSentron, we can configure the NetSentron to redirect any packets bound for the 192.168.10.0/24 network through the VPN Endpoint (192.168.1.250).

NOTE

There are other uses for static routing as well, but this is the most common.

Adding Static Routes

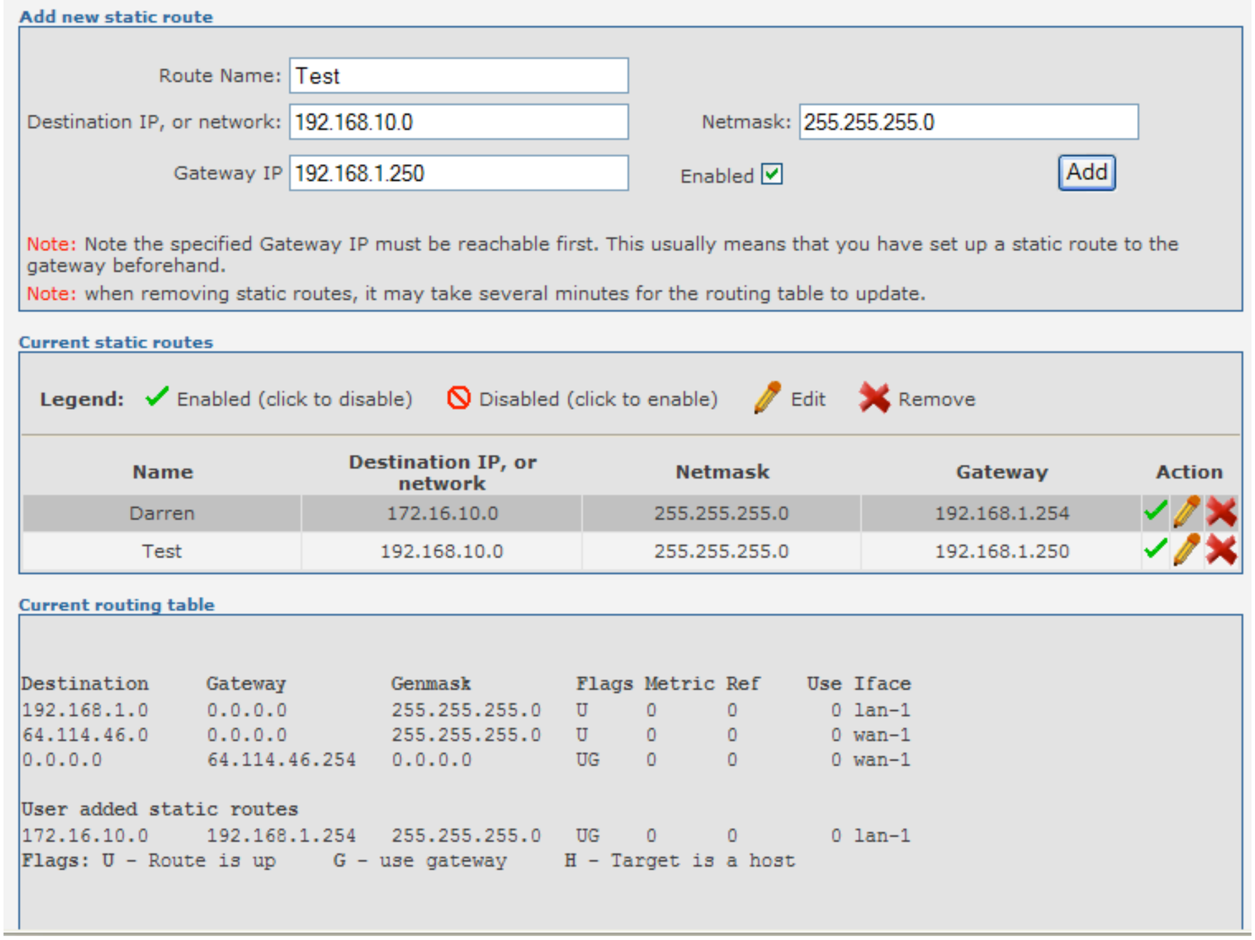
1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click the static routing button. The Static Routing page appears. *See Figure 7.17,* on the next page. The Static Routing Page is divided into three sections. The first section is for adding a new Static Route, the second section shows what Static Routes have been defined by the administrator and the third section shows the actual routing table of the NetSentron. The Static Routes entered by the administrator if properly configured, will show up in the third section.

NOTE

The Gateway IP must always be reachable from the NetSentron GREEN LAN, if it is not, the Static Route will not work.

Figure 7.17: Static Routing Page



Add new static route

Route Name:	Test		
Destination IP, or network:	192.168.10.0	Netmask:	255.255.255.0
Gateway IP	192.168.1.250	Enabled ☑	Add

Note: Note the specified Gateway IP must be reachable first. This usually means that you have set up a static route to the gateway beforehand.

Note: when removing static routes, it may take several minutes for the routing table to update.

Current static routes

Legend: ✓ Enabled (click to disable) ⊘ Disabled (click to enable) ✎ Edit ✗ Remove

Name	Destination IP, or network	Netmask	Gateway	Action
Darren	172.16.10.0	255.255.255.0	192.168.1.254	✓ ✎ ✗
Test	192.168.10.0	255.255.255.0	192.168.1.250	✓ ✎ ✗

Current routing table

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     0.0.0.0         255.255.255.0   U     0      0        0 lan-1
64.114.46.0     0.0.0.0         255.255.255.0   U     0      0        0 wan-1
0.0.0.0         64.114.46.254   0.0.0.0         UG    0      0        0 wan-1

User added static routes
172.16.10.0     192.168.1.254   255.255.255.0   UG    0      0        0 lan-1
Flags: U - Route is up     G - use gateway     H - Target is a host
```

3. When adding a new static route you will first want to give it a name. Anything can be used here and it is simply a reminder so you know what and why you created the Static Route.

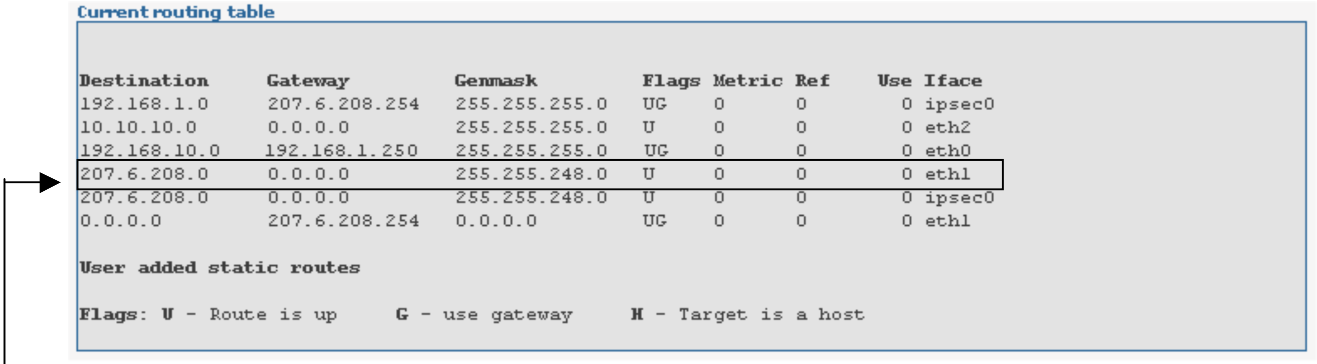
4. Next, you will need to describe the remote network that is the Destination. In this case, the remote network is 192.168.10.0/24 as per the example used in Figure 7.17.

NOTE

Figure 7.17 had a remote network (192.168.10.0/24) that was connected to our LAN through a second firewall on the LAN. In order for packets to be properly routed through the second firewall, we need to tell the NetSentron about the network on the other side of the VPN as well as the gateway that should be used to reach the other network.

5. Enter a netmask as well, since we entered .0 as the last octet of the Destination, the remote network is a /24 network comprising of 256 addresses. <u>We enter the netmask in its full notation 255.255.255.0</u>
6. Tell the NetSentron what gateway to use to access the network 192.168.10.0/24. In this case it is the Router/VPN Endpoint in the picture, which is addressed as 192.168.1.250.
7. Ensure that the `Enabled` has been checked and the press the Add button*. See Figure 7.18,* below to see what the current routing table should display if everything was entered correctly.

Figure 7.18: Static Routing Page – Current Routing Table



Current routing table

```
Destination     Gateway         Genmask         Flags Metric Ref    Use Iface
192.168.1.0     207.6.208.254   255.255.255.0   UG    0      0        0 ipsec0
10.10.10.0      0.0.0.0         255.255.255.0   U     0      0        0 eth2
192.168.10.0    192.168.1.250   255.255.255.0   UG    0      0        0 eth0
207.6.208.0     0.0.0.0         255.255.248.0   U     0      0        0 eth1
207.6.208.0     0.0.0.0         255.255.248.0   U     0      0        0 ipsec0
0.0.0.0         207.6.208.254   0.0.0.0         UG    0      0        0 eth1

User added static routes

Flags: U - Route is up     G - use gateway     H - Target is a host
```

NOTE

If you **do not** see the above line, then you have configured something wrong, recheck you settings and adjust as necessary.

If you do see the above line, then packets will now be routed to your second gateway if destined for the 192.168.10.0/24 network.

*Wireless

Setting Up Wireless with the NetSentron

The NetSentron is capable of supporting a wireless network almost as a DMZ, and as an administrator you can allow machines on the wireless network access to local area network resources. Currently the NetSentron does not support wireless network cards, so you will need to connect a wireless access point directly to the BLUE card installed in the NetSentron.

Adding another Network Card

The wireless network that is connected to the NetSentron is called the BLUE (Wireless) LAN. To configure this, you will need to add another network adapter to your NetSentron. Some NetSentrons come with an on board Network Interface Card (NIC) that is not enabled. You can enable this in the BIOS. Once enabled you are ready to go.

NOTE

If you have run out of PCI slots in your NetSentron, you can add a USB Network adapter.

Configuring the new Network Card

1. From the Administration Interface, click the System **button**. New sets of buttons appear.
2. Next, click the ssh button. Before you can make any changes you will have to activate the SSH session. To do this, check each box on the display.

It is highly recommended that you disable the SSH access once you are done with your changes. To do this, uncheck all the boxes on the Remote access display and then click the Save button.

3. Once you have selected each box, click on the Save button. The SSH session has now been activated. The `SSH Session` appears.

NOTE

If you want to login as root, use the backspace button on your keyboard remove the name `setup` and key in `root`.

4. Next, press the **Enter** button on your keyboard. A login prompt will appear with the name `setup`.

5. Key in your setup password. If you are logging in as `root`, key in the root password. If logging in as `setup`, key in the setup password.

NOTE

If you are accessing SSH for the first time, key in the default password, ***setup***. Press the **Enter** button on your keyboard. The Section Menu appears.

NOTE

You are unable to use your mouse in this display. Use the **left** and **right** arrows to move between selections. Use the **Tab** button on your keyboard to move between OK and Quit. Use the **Space** or **Enter** buttons on your keyboard to make a selection.

6. Using the arrow keys, select `Networking` and then click the **Enter** button on your keyboard. The `Networking Configuration` menu appears.
7. Use the arrow keys to tab down to `Network Configuration Type` and then click the **Enter** button on your keyboard. The `Network Configuration Type` menu appears.
8. Use the arrow keys to tab down to `GREEN + BLUE + RED` and then click the **Enter** button on your keyboard. The `Networking Configuration` menu appears.
9. Next, use the arrow keys to select `Drivers and Card Assignments`. Press the **Enter** button on your keyboard. The `Drivers and Card Assignments` menu appears.
10. You will need to probe for the new card and assign it to BLUE. Make the change and press **Enter**. You are returned to the `Networking Configuration` menu.
11. Finally you will need to assign an IP Address to the new network card. Select a segment that is different from your GREEN (LAN) segment. Use the arrow keys to select `Address Settings`. Press the **Enter** button on your keyboard. The `Address Settings` menu appears.
12. Use the arrow keys to make your selection and the **Enter** button on your keyboard.
13. Key in the ***IP Address*** you are assigning to the new network card and then arrow down to `DONE`. Press **Enter** on your keyboard.
14. Use the arrow keys to tab over to `Done` and press **Enter** on your keyboard. Use the arrow keys and `Done` until you are returned to the main menu.

> ⚠ Please ensure that you have disabled the SSH access once you are done with your changes. To do this, uncheck all the boxes on the Remote access display and then click the button.

Confirming Wireless Configuration

Once you have completed the configuration through setup, bring up the NetSentron Administration Interface, and verify that your BLUE (Wireless) is configured.

1. From the Administration Interface, click on the Information button. New sets of buttons appear.
2. Click on the network status button. The `Network Status` page is displayed. You should now see an entry for BLUE (Wireless). You can also view an entry for the BLUE (Wireless), by going to System and then setup net.

> **NOTE**
>
> Almost any access point will do. However, if you purchase an access point that is a full fledged wireless router, you will need to put it into Access Point mode instead of router mode. You may also need to add some static routing to the wireless access point to let machines on the BLUE LAN know how to get to the GREEN LAN. Configuration of the wireless access point/router is beyond the scope of this guide. Please refer to the instruction manual that came with your wireless access point/router for more information on how to adjust the settings to match what is needed.

Wireless Rules

You can use the Wireless page to set up rules to allow Wireless Access Points on the Blue network to connect to your NetSentron. Without the wireless access point, MAC adapter and IP Address on this page you will not be able the Wireless Access Point. We will assume from this point that you have your wireless access point installed and configured.

Connecting on BLUE or GREEN LAN

There are two methods you can use to allow machines on BLUE to access the Internet and machines on the GREEN LAN. The first method is the less secure method, which involves specifying the machine MAC Adapter Address and IP Address to allow access to the Internet and the resources on the GREEN LAN. The second method is through the use of a VPN and is the preferred method of connecting to the Internet and the resources on the GREEN LAN. In this section we will cover the first method. The VPN method of connecting is covered in the VPN section of the manual. Make sure you setup up your Wireless network access point with WEP or WPA enabled.

DO NOT run your wireless network without some sort of Wireless Encryption on it.

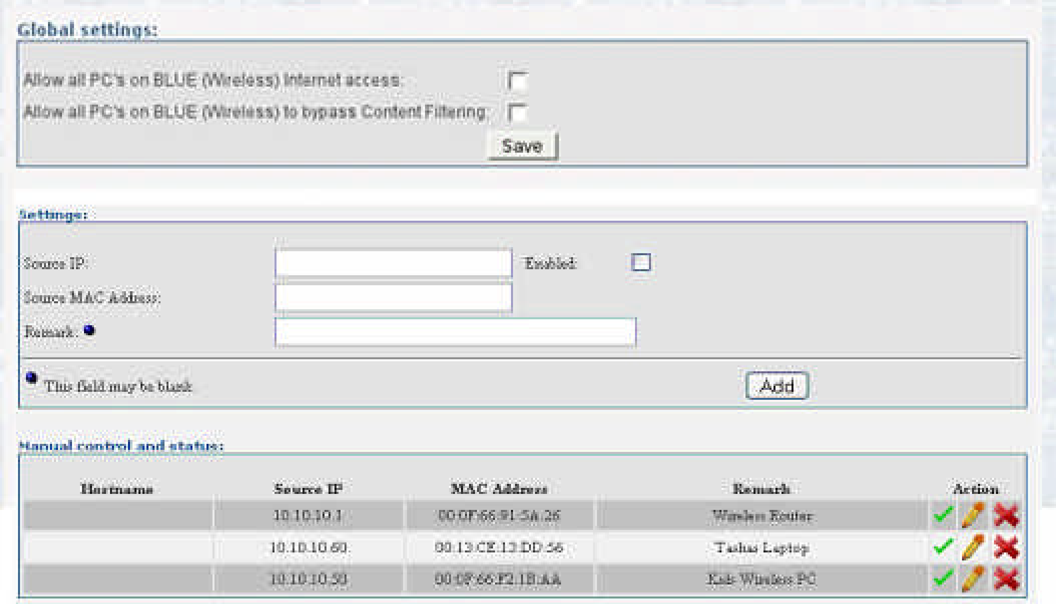
> **NOTE**
>
> The PCs that are on the BLUE LAN must have fixed addresses or fixed leases. Both the NetSentron and the wireless access point are capable of assigning the same IP address to a machine on the BLUE LAN. Alternatively you can assign static IP Address to each machine. The preferred method is to use a fixed lease as it allows more flexibility when moving the machine to another network. See the DHCP section of the manual for more information.
>
> To allow a machine on the BLUE network to access the Internet, follow the *Adding Wireless Rules*, below.

Adding Wireless Rules: Allowing PCs on the BLUE LAN to access resources using the Wireless Page & DMZ PinHoles

1. From the `GUI` Interface, click on the Firewall button. New sets of buttons appear.

2. Click on the **wireless** button. The `Wireless` page appears. *See Figure 7.19:Wireless Page* on the next page.

Figure 7.19: Wireless Page



Global settings:

Allow all PC's on BLUE (Wireless) Internet access: □
Allow all PC's on BLUE (Wireless) to bypass Content Filtering: □

Settings:

Source IP: Enabled: □
Source MAC Address:
Remark: ●

● This field may be blank

Manual control and status:

Hostname	Source IP	MAC Address	Remark	Action
	10.10.10.1	00:0F:66:91:5A:26	Wireless Router	✓ ✎ ✗
	10.10.10.60	00:13:CE:13:DD:56	Tashas Laptop	✓ ✎ ✗
	10.10.10.50	00:0F:66:F2:1B:AA	Kids Wireless PC	✓ ✎ ✗

Note

If you want to allow all the PCs on the Blue network (wireless) access to the Internet and or to bypass the Content Filter, simply check the appropriate box in the Global settings panel as seen above. If want to setup up each PC on the wireless separately, go to the next step.

3. In the `Source IP` field, key the IP Address of the wireless Access Point, or a machine, on the Blue network.

4. In the `Source MAC Address` field key the Mac Address of the wireless Access Point, or a machine, on the Blue network.

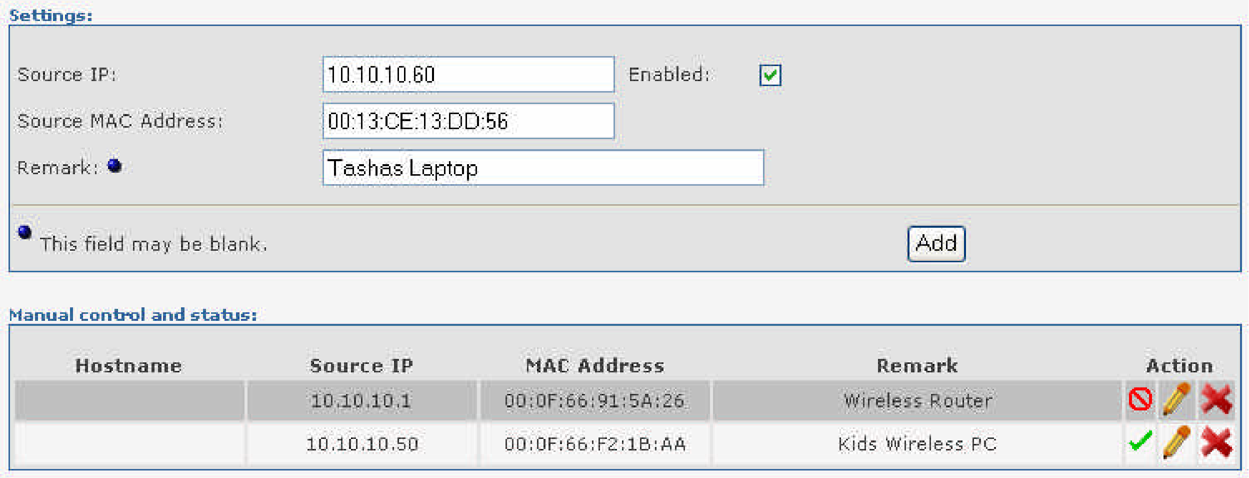
5. In the `Remark` field, key a brief description of the wireless rule you are adding. The Wireless page acts as an ACL list, and without a machine being in that list it will have no Internet access or be able to access any resources on the GREEN LAN.

6. Once you have entered your wireless settings, check the Enabled box and then click the Add button. You can view your wireless settings in the `Manual Control and Status` panel. To allow a machine on the BLUE LAN to access resources on the GREEN LAN, we need to poke holes in the protective firewall that isolates the BLUE LAN. You can do this on the DMZ Pinholes page.

Editing Wireless Rules

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.
2. Click the wireless button. The `Wireless` page appears.
3. Click the ✎ icon associated with the wireless rule you want edit. The details for that rule are placed in the Settings panel. *See Figure 7.20, below.*
4. Make your changes and then click on the Add button.
5. You can view the changes you made in the Manual Control and Status panel.

Figure 7.20: Wireless Page – Editing A Rule



Settings:

Source IP:	10.10.10.60	Enabled:	☑
Source MAC Address:	00:13:CE:13:DD:56		
Remark: ●	Tashas Laptop		

● This field may be blank.

Manual control and status:

Hostname	Source IP	MAC Address	Remark	Action
	10.10.10.1	00:0F:66:91:5A:26	Wireless Router	⊘ ✎ ✖
	10.10.10.50	00:0F:66:F2:1B:AA	Kids Wireless PC	✓ ✎ ✖

Removing a Wireless Rule

1. From the Administration Interface, click on the Firewall button. New sets of buttons appear.

2. Click the wireless button. The `Wireless` page appears. *See Figure 7.19 Wireless Page,* on the previous page. Click on the ✗ icon associated with the wireless rule you want to remove. (Once you click the delete icon, the wireless rule is removed automatically.)

BLUE LAN Tips

Because the BLUE LAN is a different segment than the GREEN LAN, Windows Networking will not behave as expected.

You need to setup a WINS server on the GREEN LAN, and insure that this WINS Server is entered into your DHCP server, whether that is the NetSentron, your Wireless Access Point, or manual configuration.

Without a WINS server, the Windows Network Neighborhood will not work. You will have to access machines by IP Address.

Some Common Ports that you will probably want to open up:

- TCP 137-139 & UDP 137 – Allows File & Printer Sharing to work
- TCP 80 & 443 – HTTP & HTTPS
- TCP 21 – FTP
- TCP 3389 – Microsoft Remote Desktop

More information on common ports can be found here:

http://www.governmentsecurity.org/articles/CommonPorts.php

BLUE LAN Troubleshooting

If you find you are unable to reach a machine on GREEN or a service on a machine on GREEN, go to the LOGS->Firewall page of the NetSentron GUI.

Search for the IP Address of the machine on BLUE. Most likely you will see an entry listing the Port and Protocol for the service that is being blocked.

Advanced Firewall

The NetSentron has an advanced firewall that is not enabled by default. The purpose of the advanced firewall is to give you greater control over the packets that come into and leave your network. By default the NetSentron blocks incoming packets, except those specifically allowed and needed. The Advanced Firewall, allows you to control the outgoing packets, allowing only specified packets to leave the firewall.

Warning:

The Advanced Firewall is a feature that requires explicit knowledge of ports, protocols and services. It is intended for an experienced administrator who understands firewalls.
Improper configuration of this feature can block your access entirely to the NetSentron, or the Internet. Also improper configuration of this feature could lead to opening up your firewall, and exposing your network to outside networks. Use with extreme caution.

Advanced Firewall Introduction

The Advanced Firewall is found under the Firewall tab. There are three submenu items associated with it; advanced firewall setup, advanced firewall rules, and advanced firewall services. The advanced firewall section of this manual is written with the experienced firewall administrator in mind.

The advanced firewall setup page allows you to set up basic settings of the Advanced Firewall, such as MAC adapter of the administrator's PC, logging, default actions for denying packets, and how the firewall are displayed. It is also the page that allows you to Enable or Disable the Advanced Firewall. Backing up, restoring and resetting to factory defaults is also on this page.

The advanced firewall rules page contains the list of configured rules for the Advanced Firewall. We have created the minimum set of rules necessary for a NetSentron configured with a Red and Green interface to surf the internet and function normally. This page also allows the adding, editing and deleting of rules.

The advanced firewall services page contains the services that you use in the advanced firewall rules page. Services consist of ports and protocols. Services can be grouped together to form Service Groups.

Also on this page you can create networks, groups of networks and groups of IP Addresses.

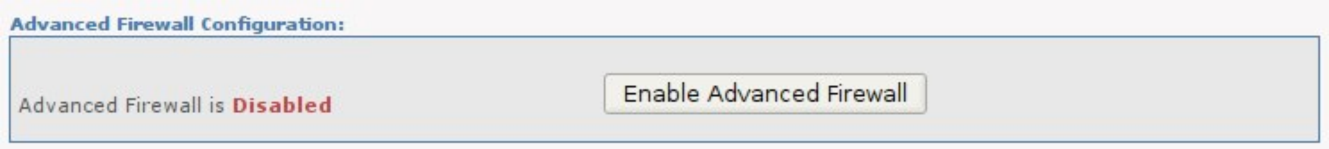
Each of these pages will be reviewed in greater detail on the following pages.

NOTE
If the Advanced Firewall has not been previously configured, you will not be able to enable it or edit the firewall rules.

Advanced Firewall Configuration

The Advanced Firewall Configuration is used to enable and disable the Advanced Firewall.

Figure 7.21 - Advanced Firewall Configuration



Advanced Firewall Configuration:

Advanced Firewall is **Disabled**

Clicking the button will enable the firewall, clicking it a second time will disable it. *See Figure 7.21:Advanced Firewall Configuration* above.

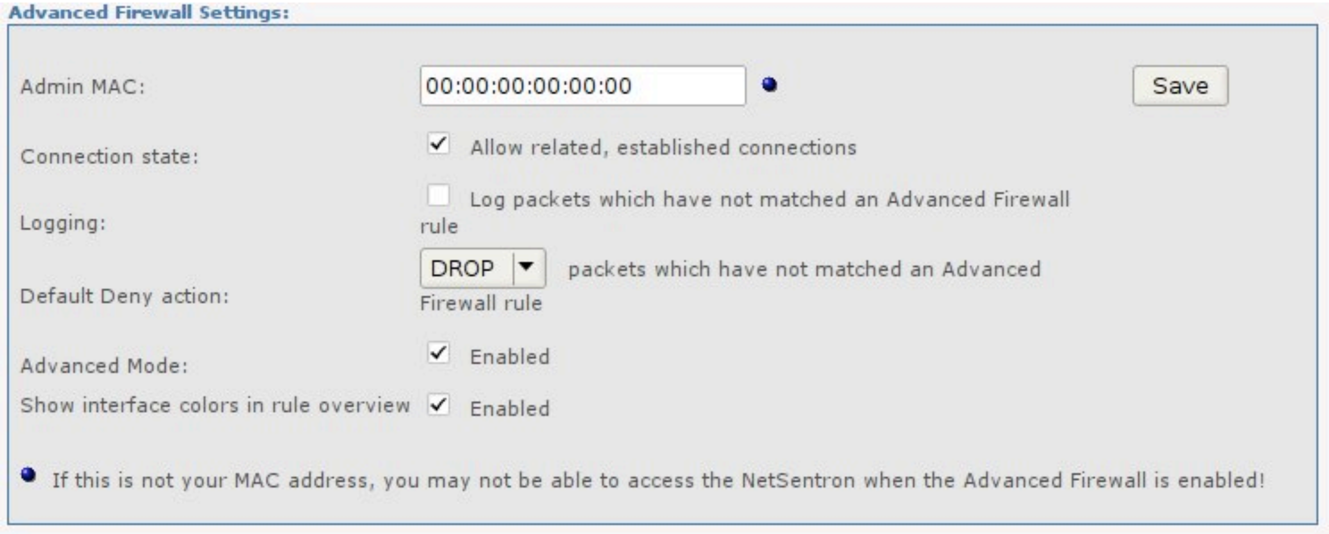
NOTE

If the Advanced Firewall is not yet configured, this button will not show up.

Advanced Firewall Settings

Advanced Firewall Settings is used to set some default settings for the Advanced Firewall. *See Figure 7.22:Advanced Firewall Settings* below.

Figure 7.22: Advanced Firewall Settings



Advanced Firewall Settings:

Admin MAC: 00:00:00:00:00:00 ●

Connection state: ☑ Allow related, established connections

Logging: □ Log packets which have not matched an Advanced Firewall rule

Default Deny action: DROP ▾ packets which have not matched an Advanced Firewall rule

Advanced Mode: ☑ Enabled

Show interface colors in rule overview ☑ Enabled

● If this is not your MAC address, you may not be able to access the NetSentron when the Advanced Firewall is enabled!

Below is a list of the settings found under Advanced Firewall Settings:

Admin MAC: This is the MAC adapter address of a computer on your LAN that will always have access to the NetSentron. It is a failsafe to keep you from being locked out of the NetSentron in the event of a misconfiguration. Usually you would enter the MAC adapter address of the Administrators computer.

Connection State: This should be enabled if you are using Port Forwarding to any machines on your LAN. If you are not using Port Forwarding, then this can be ignored. It allows packets that have come from a Port Forwarding rule to return back out to the internet.

Logging: If you wish to log packets that have not matched an Advanced Firewall Rule, then enable this option.

Default Deny Action: This is the action taken by the firewall for a denied packet. It can be dropped or rejected. The difference is that a dropped packet is literally dropped with no response to the source computer, whereas the rejected option will send a reply to the denied computer telling it that the packet has been denied. The default option is DROP.

Advanced Mode: This feature is disabled by default, but when enabled, adds some more advanced features to the firewall rules page.

- It allows rules to restrict by source port for sources of packets and allows inversion of rules.
- It allows specifying interfaces on the destination for packets and allows inversion of rules.
- Adds additional logging options if logging is enabled.

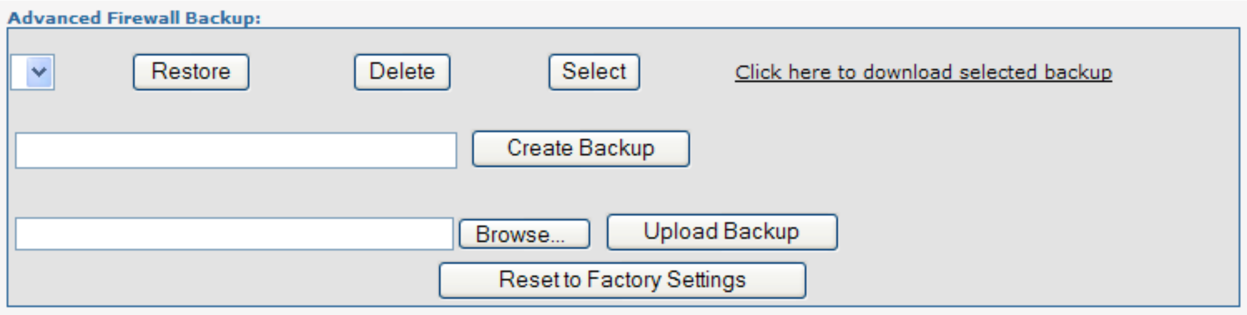
It is up to you whether or not you use these advanced features.

Show interface colors in rule overview: This makes the rules page easier to read by color coding the network interfaces.

Advanced Firewall Backup

This section allows you to create a back up of the advanced firewall, download it, or restore it. It also allows you to reset the Advanced Firewall to the factory settings. *Figure 7.23: Advanced Firewall Backup* shows you, below, the screen with the associated buttons to select your options.

Figure 7.23: Advanced Firewall Backup


Advanced Firewall Backup:
Restore
Delete
Select
Click here to download selected backup
Create Backup
Browse...
Upload Backup
Reset to Factory Settings

To create a backup, enter a name in the white input area to the left of the **Create Backup** button. Then click on the **Create Backup** button. You will see your new backup appear in the drop down list. Select it and then click on the **Select** button. You can now click on the link **Click here to download selected backup** to download the backed up firewall rules. These rules can be restored to another NetSentron if you wish.

To restore a back up, click on the **Browse** button to find the back-up file on your computer and then click the **Upload Backup** button. Next, select the correct back up from the drop down list, click on **Select**, and then click on the **Restore** button. Your back up will now have been restored.

If you wish to restore a back up stored on the NetSentron, select the back up from the drop down list, click on **Select**, and then click on the **Restore** button. Your back up will now have been restored.

If you wish to delete a back up, select it from the list and click on the **Delete** button.

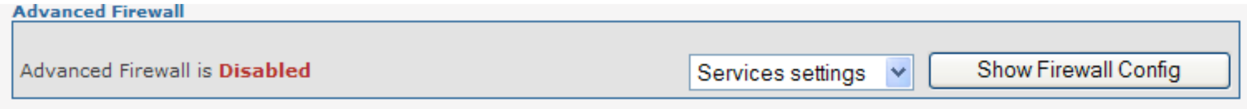
To reset to factory defaults, click on the Reset to Factory Settings button and click **OK** when the Confirm prompt comes up. This will restore your Advanced Firewall settings to how they were when the NetSentron was shipped from the factory. You will then need to go back to the Advanced Firewall Setup and re-enter your MAC adapter address and choose your appropriate options again.

Advanced Firewall Services Page

The advanced firewall services page is broken up into several sections depending upon the configuration choice you make. The first section titled

Advanced Firewall allows you to select from several different configurations; Services Settings, Services Grouping, Address Settings and Address Grouping. Select one and then press **Show Firewall Config**: this will change the layout of the page specific to the selection. This section is shown before the rules section as it is necessary to create the proper services first, before you can create rules.

Figure 7.24 – Advanced Firewall



Advanced Firewall

Advanced Firewall is **Disabled**

Services Settings, Services Grouping, Address Settings and Address Grouping configurations will now be explained in detail.

Services Settings Configuration

This configuration has three main areas. The first, `Add Service`, *Figure 7.26*, is for adding a new service. The second area is the Custom services area that shows the custom services that have been added. The third area shows all the default services that one would normally expect to see in a firewall.

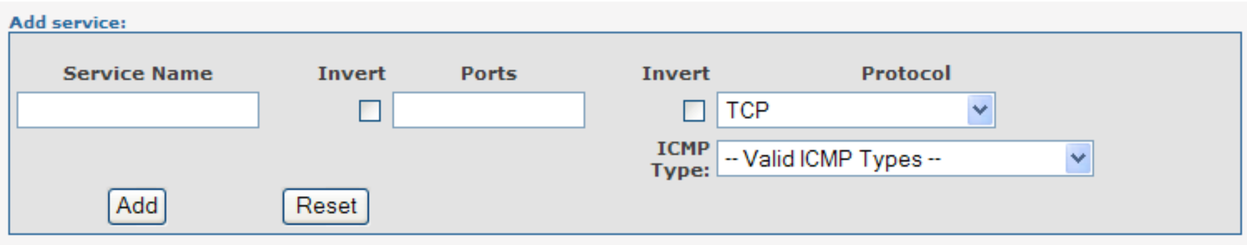
A service is comprised of a name, a port if necessary, a protocol and if necessary an ICMP type.

We have already added several Custom Services for you such as NetSentron GUI Access, Content Filter, Denied and various messengers. Each one has a name, a protocol, a port if the protocol supports it, and an ICMP type if the protocol supports it. The Custom services area also shows how many times the service is being used.

NOTE
You cannot delete a custom service if it is being used. You cannot change the name of a custom service if it is being used, either.

To add a new service, simply give the service a unique name, enter the port or ports necessary, choose the protocol from the drop down list and select an ICMP type if necessary. You can also make it an inverted service by checked the Invert checkbox. This would make the rule act in reverse to what you would expect. Click on the **Add** button to add the new service. You should see it appear below in the custom services section.

Figure 7.25: Add Service



Add service:

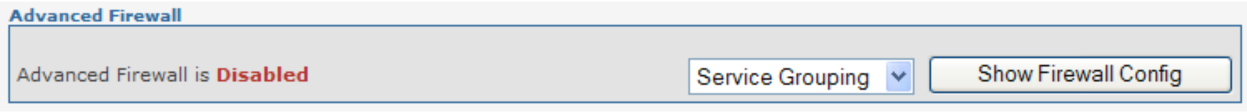
Service Name	Invert	Ports	Invert	Protocol
	□		□	TCP
			ICMP Type:	-- Valid ICMP Types --

In the next section, we will look at the `Services Grouping` section. That will allow you to group services together to make more complex rules.

Services Grouping Configuration

The Services Grouping Configuration allows you to group together services into a single rule. *See Figure 7.26; Service Grouping* below. As an example: to administer a NetSentron, you need access to TCP port 222 and TCP port 5445. If we did not have groups, we would have to create two rules to allow us to administer a NetSentron: one for port 222 and one for port 5445. Instead, if we group them together so that we only have to create one rule to allow access to a NetSentron.

Figure 7.26: Service Grouping Configuration



Advanced Firewall

Advanced Firewall is **Disabled**

Service Grouping

In Service Groups, we have created a group called Admin NetSentron – Administer NetSentron. Notice it contains two services that are both custom (NetSentronGUI Access and NetSentronSSH Access). If you go back to the Services Configuration, you will see that NetSentronGUI Access is TCP port 5445 and that NetSentronSSH Access is TCP port 222.

We have created several default groups for you. An example is the Base Services, which allows access to DHCP, NTP, BOOTPC, AUTH and BOOTPS. These are required for your client PCs to get an address and update their clock.

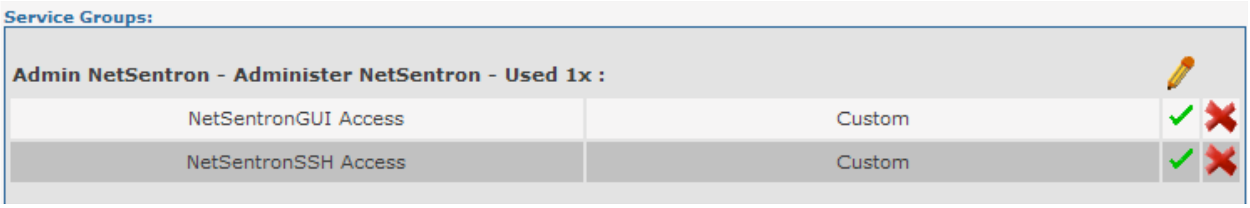
We have created a group called Email Services, which contains the necessary email services so that a client PC may send and receive email.

There are several more groups available. Some of them, like Windows Networking and LDAP, you will notice are not used at all. These are here for your convenience.

If you look at the Service Groups section, *see Figure 7.27 below,* you will notice the edit pencil next to the group names. A group name can only be changed if the group is not being used.

Notice that the services within the group have the green checkmark and the red X. The green checkmark can be clicked on to disable that service for the group. The red X deletes the rule from the group. Services can be enabled/disabled and deleted even if a group is being used and the Advanced Firewall is enabled – the firewall rules will be updated on the fly.

Figure 7.27: Service Groups Display



Service Groups:

Admin NetSentron - Administer NetSentron - Used 1x :

NetSentronGUI Access	Custom	✓	✗
NetSentronSSH Access	Custom	✓	✗

Adding a Service Group

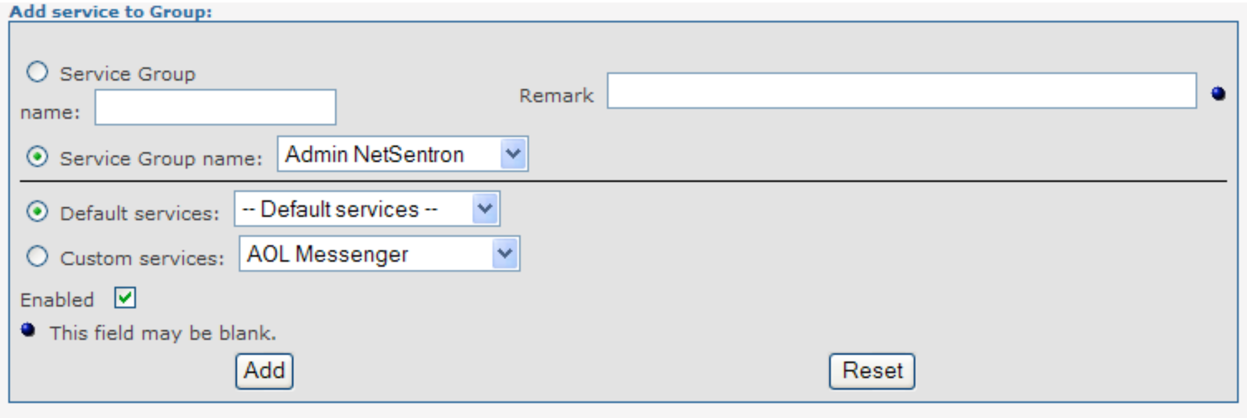
1. Enter a unique name into the Service Group name field.

2. Enter a Remark about the Service Group that describes it for you in a meaningful way so that you can remember it.

3. Choose a service, either one from the Default services drop down list or the Custom services drop down list.

4. Make sure the Enabled box is checked and then click Add. *See Figure 7.28* on the next page. Your new group should show up now in the Service Groups section.

Figure 7.28: Add Service to Group Display



Add service to Group:

○ Service Group name: ____ Remark ____ ●

◉ Service Group name: Admin NetSentron

◉ Default services: -- Default services --

○ Custom services: AOL Messenger

Enabled ☑

● This field may be blank.

5. To add more services to the new group, this time select your group from the Service Group name drop down list and then select a service and click the Add button.

Address Settings Configuration

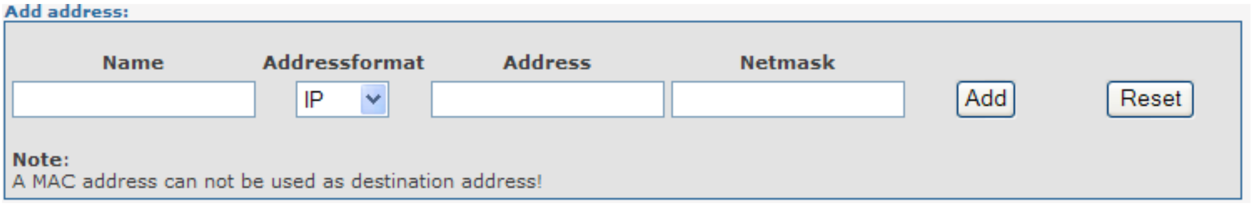
The `Address Settings Configuration` is for dealing with IP Addresses. Several addresses and networks have been created for you by default. The `Green Address, Green Network, Red Address, local host, local net,` and `Any` will show up for all configurations. If you have a Blue or Orange network setup, then `Address and Network` entries will be created for those network cards as well.

Addresses are useful for restricting rules to specific IP addresses or Networks. As an example, in the last section we created a Service group called NetSentron Administration. It makes sense that we would only want to allow access to admin the NetSentron from the Green Network.

If you have computers or servers that need to have their own rules, then you can create the address settings for them here; *see Figure 7.30 below*. If your network is using DHCP, then you can use a MAC adapter instead of an actual IP address. This allows specific rules for machines without specifying an IP address—very handy for a laptop on your network that comes and goes.

To add a new address, simply enter the Name of the address (or computer), select IP or MAC for Address format, then enter the address or MAC adapter of the machine. Click Add to create the new address. Do this for as many addresses as you need.

Figure7.29: Add Address Panel


Add address:

Name	Addressformat	Address	Netmask		
	IP			Add	Reset

Note:
A MAC address can not be used as destination address!

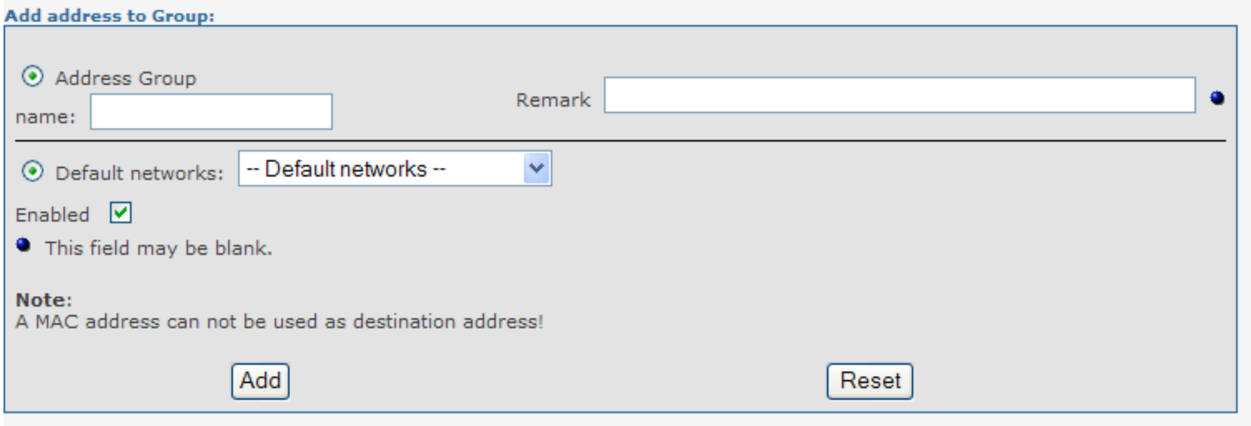
Address Grouping Configuration

Now that you have created some Addresses in the previous section, you might want to group them together. As an example, maybe you created several addresses for a couple of laptops: you can now group those together under a group called Laptops.

To create a new group, give the group a name, and enter a remark that will help you remember the purpose of the group. Choose a `Default Network` or a `Custom Address` and click **Add.** Your new group will show up under `Address Groups`.

To add more to this group, this time select your group from the Address Group Name drop down list and then add another network or custom address. Repeat as necessary.

Figure7.30: Add Address to Group Configuration



Add address to Group:

○ Address Group name:

Remark ●

○ Default networks: -- Default networks --

Enabled ☑

● This field may be blank.

Note:
A MAC address can not be used as destination address!

Advanced Firewall Rules Page

The Advanced firewall rules page is the page that contains all of the rules for the advanced firewall. It is broken up into three sections, Advanced Firewall, Add a new Rule and Current Rules. The first section merely shows the status of the advanced firewall (if it is enabled or disabled).

The second section is for adding a new firewall rule, you select an action (ACCEPT, DROP, REJECT, or Log Only) and then click on New Rule. This will open a new page where you can add the rule, we will cover this in greater details later on.

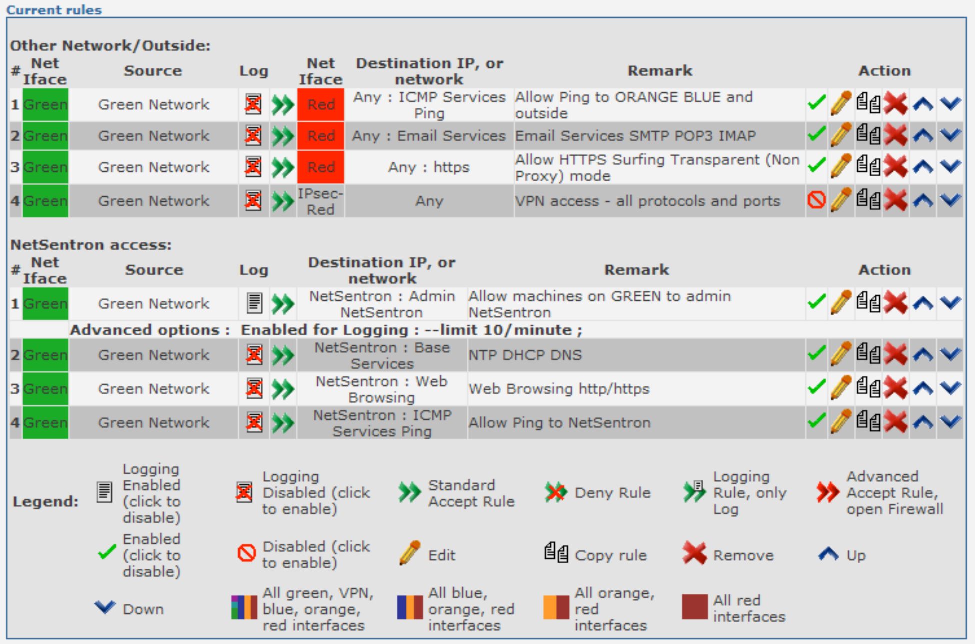
The third section is the current rules. By default, we have already created a set of rules for you so that the Advanced Firewall will work when enabled.

Current Rules

The `Current Rules` section shows the `Interface, Source, Destination, Logging` and `Remarks`. If `Advanced Mode` is enabled, then you will also see the destination interface as well as any advanced logging options.

The current rules page, *see Figure 7.31 below,* is an overview of all the rules that are setup for the advanced firewall. The current rules section is actually broken up into two parts. The first part shows rules that go to Other Networks or Outside (Wireless, VPN, DMZ or the outside world). The second part shows rules that allow access to the NetSentron itself.

Figure7.31: Current Rules Display



Current rules

Other Network/Outside:

#	Net Iface	Source	Log		Net Iface	Destination IP, or network	Remark	Action
1	Green	Green Network	☒	»	Red	Any : ICMP Services Ping	Allow Ping to ORANGE BLUE and outside	✓ ✎ ⧉ ✗ ▲ ▼
2	Green	Green Network	☒	»	Red	Any : Email Services	Email Services SMTP POP3 IMAP	✓ ✎ ⧉ ✗ ▲ ▼
3	Green	Green Network	☒	»	Red	Any : https	Allow HTTPS Surfing Transparent (Non Proxy) mode	✓ ✎ ⧉ ✗ ▲ ▼
4	Green	Green Network	☒	»	IPsec-Red	Any	VPN access - all protocols and ports	⦸ ✎ ⧉ ✗ ▲ ▼

NetSentron access:

#	Net Iface	Source	Log		Destination IP, or network	Remark	Action
1	Green	Green Network	▤	»	NetSentron : Admin NetSentron	Allow machines on GREEN to admin NetSentron	✓ ✎ ⧉ ✗ ▲ ▼
	Advanced options :	Enabled for Logging : --limit 10/minute ;					
2	Green	Green Network	☒	»	NetSentron : Base Services	NTP DHCP DNS	✓ ✎ ⧉ ✗ ▲ ▼
3	Green	Green Network	☒	»	NetSentron : Web Browsing	Web Browsing http/https	✓ ✎ ⧉ ✗ ▲ ▼
4	Green	Green Network	☒	»	NetSentron : ICMP Services Ping	Allow Ping to NetSentron	✓ ✎ ⧉ ✗ ▲ ▼

Legend:

- ▤ Logging Enabled (click to disable)
- ☒ Logging Disabled (click to enable)
- » Standard Accept Rule
- ✗ Deny Rule
- » Logging Rule, only Log
- » Advanced Accept Rule, open Firewall
- ✓ Enabled (click to disable)
- ⦸ Disabled (click to enable)
- ✎ Edit
- ⧉ Copy rule
- ✗ Remove
- ▲ Up
- ▼ Down
- ▮ All green, VPN, blue, orange, red interfaces
- ▮ All blue, orange, red interfaces
- ▮ All orange, red interfaces
- ▮ All red interfaces

At the end of each line is a set of icons for taking action on the rule. The first icon is a Green Check or Red circle with a line through it. This indicates whether or not the rule is enabled (green check) or disabled (red circle). You can click on the check or circle to toggle the state of the rule (enabled or disabled).

The next icon is the yellow pencil. This is for editing the rule and will bring up another page. We will cover that in more detail later.

The third icon is two documents beside each other. This is the `copy rule` button and allows you to copy an existing rule. This is useful for duplicating rules set up on Green for the Blue Network.

The fourth icon is a red X. This is used for deleting the rule.

The remaining two icons are up and down arrows. These arrows are used to move the rule up or down in the list of existing rules.

There are two more icons for each rule that are not under the Action heading.

The first is under the Log heading. It is to show whether logging is enabled or disabled. If logging is enabled for the rule, you will see a white document. If it is disabled, the white document will have a red X through it. You can click on the icon to enable or disable logging for the chosen rule.

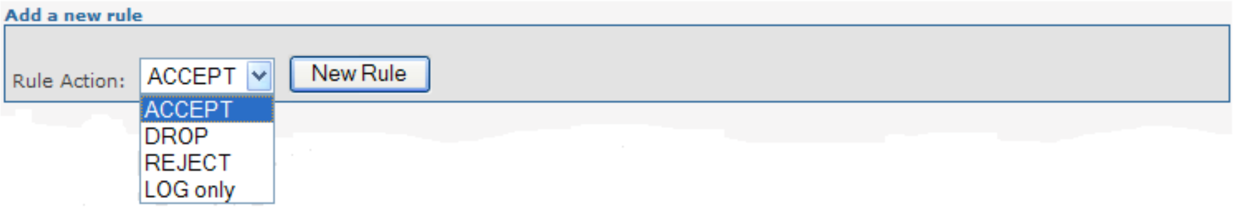
The second icon is next to the log column: it is the two green greater than signs together '>>' and indicates a standard accept rule. This icon changes depending upon choices when creating or editing the rule. The icon will have a red X through it if the rule is a deny rule. Or if the rule is a logging only rule, it will contain a small white document in it similar to the Log icon. Finally, if the rule you create is an advanced rule that opens up the firewall, the icon will turn RED.

Adding a New Rule

To add a new rule, you first need to decide what kind of a rule it is: ACCEPT, DROP, REJECT or LOG Only.

- ACCEPT allows the packets to flow through from the source to the destination outlined in the rule.
- DROP will drop the packet without any report or reply to the client machine.
- REJECT will reject the packet, but will report back to the client machine that the packet has been rejected.
- LOG Only is strictly a logging rule. It will log any and all packets that match the rule.

Figure 7.32: Adding a New Rule Display



Once you select the type of rule you want to create, click on the New Rule button. A new page will come up: the Add a New Rule Page, see Figure 7.31

above.

Add a New Rule Page

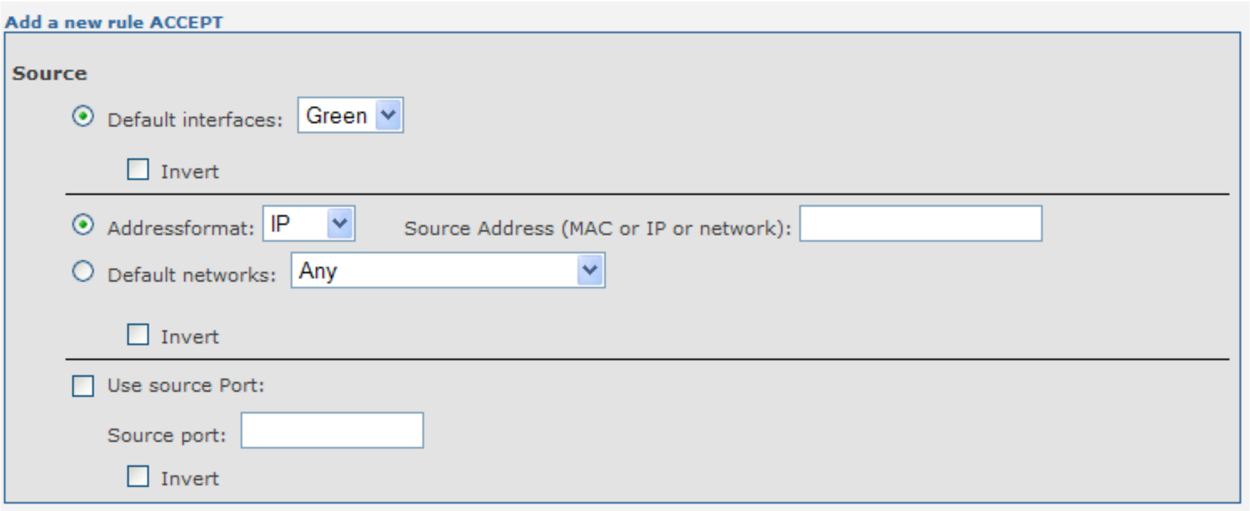
The `Add a New Rule` Page allows you to add a new rule. It is comprised of four sections, Source, Destination, Additional and Timeframe.

Source Section

The source section is where you define the source of the packets. This section is further broken down in to three sub-sections, Interfaces, Addresses and Ports. *See Figure 7.32 on the next page.*

You must select an interface as the source of the packets: Any, Green, Red, Blue, or Orange. If you are running a VPN, you will see IPSEC-Blue and IPSEC-Red as well. That means that the packets we want to apply the rule to would be coming from the interface selected. Note that if you have the advanced mode enabled there will be an `Invert` check box. This makes the rule have the opposite effect (eg. if you chose Green and then checked the Invert check box, the rule would apply to packets coming from anywhere but the Green interface).

Figure 7.33: Add a New Rule Display-Source Selection



Add a new rule ACCEPT

Source

● Default interfaces: Green

□ Invert

● Addressformat: IP   Source Address (MAC or IP or network):

○ Default networks: Any

□ Invert

□ Use source Port:

Source port:

□ Invert

The next subsection to configure is the Network or IP Address. You can select a specific IP address or MAC adapter address. That means the rule will only apply to that specific IP or MAC adapter.

You can restrict the rule to a specific network such as Green, Blue, Orange, etc.

You can restrict the rule to a custom address you have created.

Or you can restrict the rule to an Address Group, which will contain several addresses or networks.

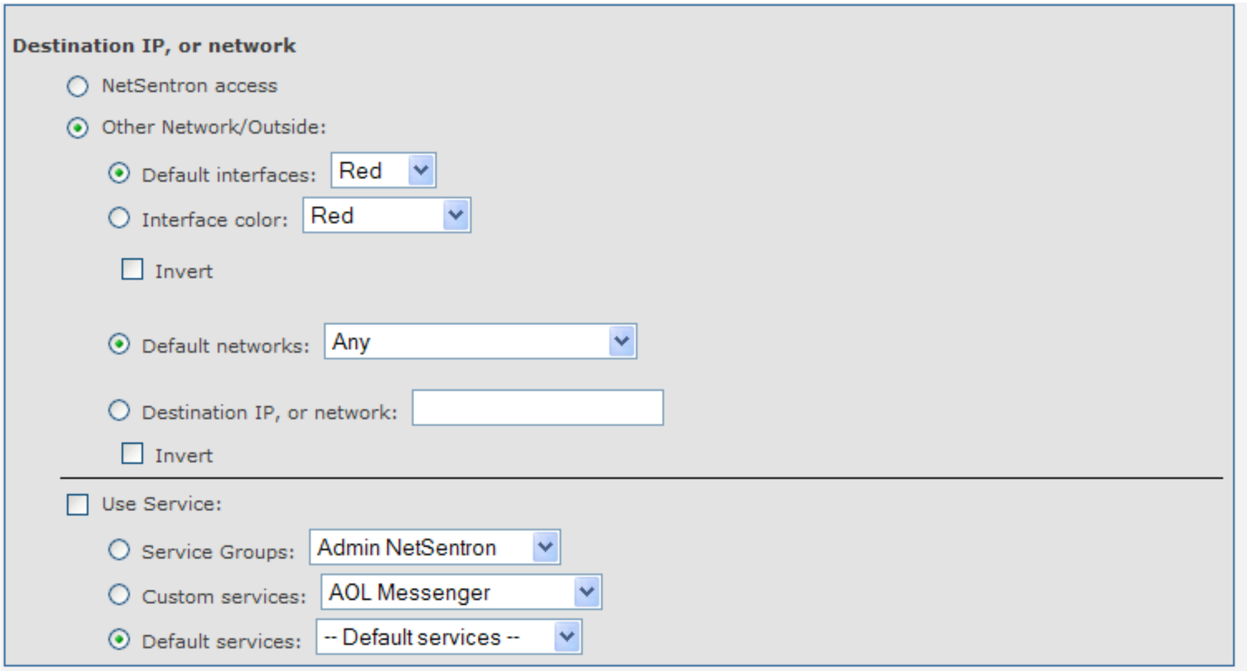
NOTE
The Invert button in this subsection will make the rule apply to all addresses or networks other than the selected one.

The final subsection of the source section is the `Source Port` subsection. This allows you to specify a port (or range of ports) that the rule will apply to. Again there is an invert button so that you can reverse the rule. This subsection is optional, and can be toggled by checking the `Use Source Port` check box.

Destination Section

The Destination Section is further broken down in to two subsections, IP/Network and Service. The IP/Network subsection is required to be filled in and the Service subsection is optional.

Figure 7.34: Destination IP, or Network Display



Destination IP, or network

○ NetSentron access

● Other Network/Outside:

● Default interfaces: Red

○ Interface color: Red

□ Invert

● Default networks: Any

○ Destination IP, or network:

□ Invert

□ Use Service:

○ Service Groups: Admin NetSentron

○ Custom services: AOL Messenger

● Default services: -- Default services --

You first need to decide if the packets are going to the NetSentron or going elsewhere (including other networks behind the NetSentron such as Orange, Blue or VPN).

If the packets are bound directly for the NetSentron to access a service of the NetSentron such as DHCP, Proxy, Filtering, or Administration of the NetSentron, then choose the first option NetSentron access.

If, however, the packets are bound elsewhere such as Mail servers outside the NetSentron, VPNs or pinging, then choose the second option Other Network/Outside.

If you chose Other Network/Outside, then you need to further define the rule. You will need to select an interface for the destination. As with other settings, there is an Invert check box to reverse the rule.

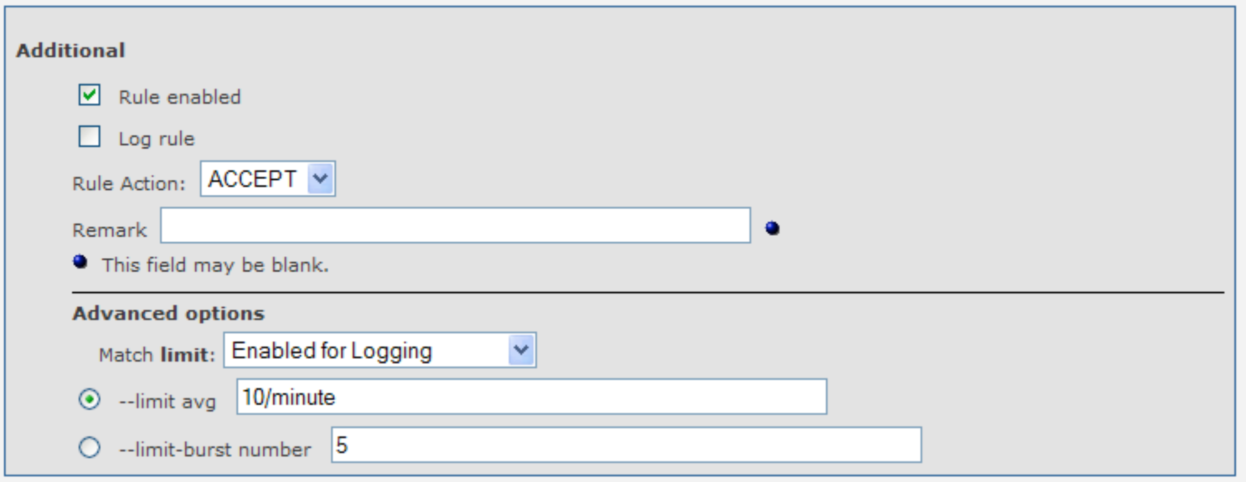
After selecting an interface, you now need to select a Network, an address, an address group or a specific destination IP address or network. Again, the `Invert` check box is present to reverse the rule.

The destination section is the Service subsection is optional. If you wish to restrict your rule further by choosing an actual service, you would do so here. Click on the `Use Service` check box and then select a Service Group, Custom Service or a Default Service.

Additional Section

The Additional Section contains some extra options and depending upon whether or not you have enabled the advanced option, it may also contain an `Advanced Options` subsection as seen in *Figure 7.35* below.

Figure 7.35: Additional Section- Advanced Options Display



Additional

☑ Rule enabled

□ Log rule

Rule Action: ACCEPT

Remark

● This field may be blank.

Advanced options

Match **limit:** Enabled for Logging

● --limit avg 10/minute

○ --limit-burst number 5

The first check box is for enabling or disabling the rule.

The second check box enables or disables logging for the rule.

The Rule Action is the same option you took before clicking on create new rule and allows for ACCEPT, DROP, REJECT, and LOG Only.

The Remark field is for putting in a description of the rule. It is recommended that you use this field; it will show up in the list of rules.

Advanced Options Subsection

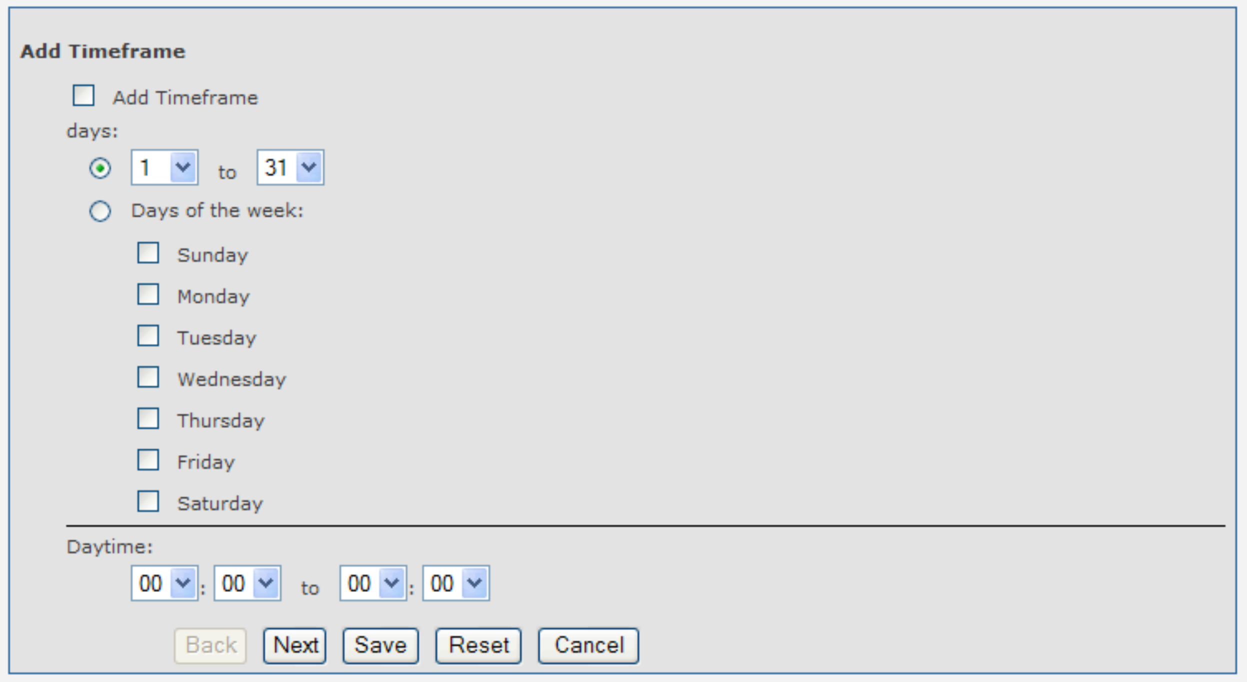
This section allows you to set some advanced parameters for logging. An understanding of IPTables is required to understand this section fully. Basically it allows you to set limits on the logging of packets, which is sometimes required so that the log files are not flooded. If you are unfamiliar with IPTables, then leaving these settings in their default options is recommend. *See Figure 7.35 above.*

Add TimeFrame Section

The `Add Timeframe` section allows you to specify times when the rule will be in effect.

To apply a time frame to the rule, check the box `Add Timeframe`. Then choose either days or days of the week. If choosing days, then adjust your start and finish days. If you selected days of the week, then check off the days of the week that you wish the rule to be in effect.

Figure 7.36: Add Timeframe Display



Add Timeframe

☐ Add Timeframe

days:

● 1 to 31

○ Days of the week:

☐ Sunday
☐ Monday
☐ Tuesday
☐ Wednesday
☐ Thursday
☐ Friday
☐ Saturday

Daytime:

00 : 00 to 00 : 00

When you have everything looking as you want, then click either **Next** or **Save. Save** will save the rule and return you to the list of rules. **Next**, will save the rule and then return you to the same page so you can create another rule.

Edit Rule Page

The edit rule page is almost identical to the `Add rule` page, except all of the information is already there. Refer to the `Add Rule` page for specific details about a section or subsection.

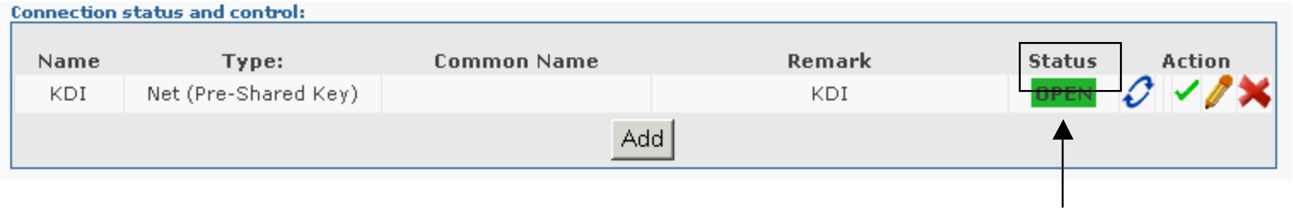
Chapter 8 IPSEC VPN

A VPN allows for two or more remote computers or networks to share information through a secure tunnel over a medium such as the Internet. This tunnel provides Authentication and encryption of the information that is passed through it. The easiest way to set up a VPN tunnel is by having a NetSentron at both ends of the tunnel.

VPN Connection and Status Control

The `VPN Connection and Status Control` panel allows the administrator the ability to edit, restart, disable, and remove a VPN Connection. From this display you can also view the status of the VPN connection. If at any time an established VPN connection is no longer working, you can check here to see if the connection is opened or closed. To open the VPN Connection Status and Control panel, simply click the VPN's button. The VPN page appears. The Connection and Status Control panel is the second panel from the top. *See Figure 8.1: VPN Display-Connection and Status Control, below.*

Figure 8.1: VPN Display – Connection And Status Control



Connection status and control:

Name	Type:	Common Name	Remark	Status	Action
KDI	Net (Pre-Shared Key)		KDI	OPEN	↻ ✓ ✎ ✗

Add

The status for this VPN connection shows Open

Checking the Status of a VPN Connection

You can check the status of any VPN connection from the `Connections and Status Control` panel located on the VPN Page. All open VPN connections are displayed in green and all closed VPN connections will be displayed in red.

Restarting a VPN Connection

1. From the Administration Interface, click on the VPN's button. The VPN page appears.

2. From the Connections Status and Control panel click on the ⟳ icon for the VPN connection you want to restart. The status of the VPN Connection should be showing OPEN.

Disabling/Enabling a VPN Connection

1. From the Administration Interface, click on the VPN's button. The VPN page appears.
2. From the Connections Status and Control panel click on the ✓ icon to disable the VPN connection. You should now see a small ⊘ icon. If you want to enable the VPN Connection, click on the small ⊘ icon and the ✓ icon will be showing.

Editing a VPN Connection

There are times when you might need to make changes to current VPN connections. The following are instructions on how to edit a VPN connection.

1. From the Administration Interface, click on the VPN's button. The VPN page appears.

2. From the `Connections Status and Control` panel click on the ✎ icon for the VPN connection you want to edit. The `Connections` panel appears.

3. Make the appropriate changes and then click on the Save button. You are returned to the VPN page. The changes you made have been confirmed.

⚠

Be advised that when you are adding or editing a connection, **DO NOT** leave the page before clicking on the Save button. If you leave the page before using the Save button you will lose all entered data.

Removing a VPN Connection

If a VPN connection is no longer required the administrator has the ability to remove it. The following are instructions on how to remove current VPN connections.

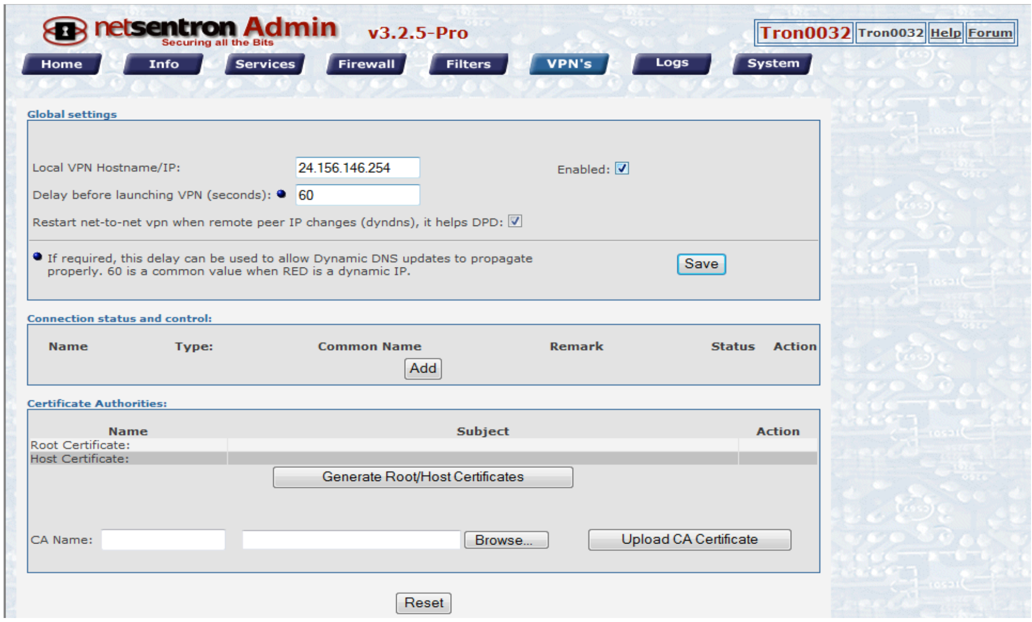
1. From the Administration Interface, click on the VPN's button. The VPN page appears.
2. From the `Connections Status and Control` panel click on the ✖ icon for the VPN connection you want to remove. Be advised that once you click the button, the connection is automatically removed and your page is refreshed.

Net-to-Net VPN - Using Pre-Shared Secrets

The Net-to-Net VPN connection allows for a secured VPN connection between two or more NetSentron Servers.

1. From the Administration Interface, click on the VPN's button. The VPN page appears. *See Figure 8.2: VPN Page, below.*

Figure 8.2: VPN Page



Global settings

Local VPN Hostname/IP: 24.156.146.254

Enabled: ☑

Delay before launching VPN (seconds): ● 60

Restart net-to-net vpn when remote peer IP changes (dyndns), it helps DPD: ☑

● If required, this delay can be used to allow Dynamic DNS updates to propagate properly. 60 is a common value when RED is a dynamic IP.

Connection status and control:

Name	Type:	Common Name	Remark	Status	Action

Certificate Authorities:

Name	Subject	Action
Root Certificate:		
Host Certificate:		

CA Name:

2. First you will need to change the Local VPN Hostname/IP. If your Red (WAN) adapter has a static IP address, then enter that address in the Local VPN Hostname/IP. If your Red (WAN) adapter has a dynamic address, then you will need to setup a Dynamic DNS configuration. For instructions on how to set up a Dynamic DNS refer to *Setting up a Dynamic DNS*, on page 70.

Determining *if your Internet Service Provider* (ISP) *uses Dynamic or Static IP addresses or PPPoE*

To allow the NetSentron to communicate with your ISP, you will need to determine whether or not you have been assigned a static or dynamic address or PPPoE. You can accomplish this by calling your ISP.

NOTE

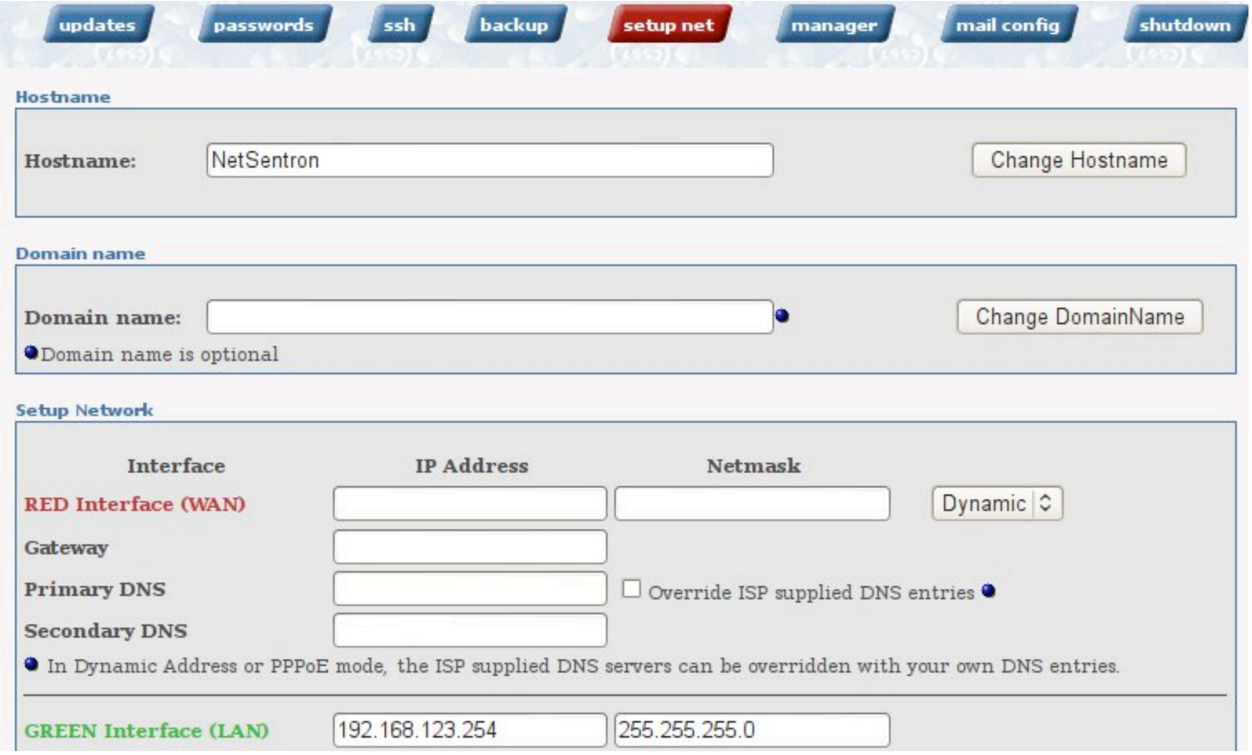
If you have a Static IP, confirm with your ISP that you are indeed receiving a true Static IP and not one that is being served through DHCP.

The next sections assume that you have logged into the NetSentron Administration GUI.

Configuring the External Network

Inside the administration guide, click on the System button. Next, click the setup net tab. You will find yourself on a screen that looks like this:

Figure2.1: Setup Net page



Hostname

Hostname: NetSentron [Change Hostname]

Domain name

Domain name: ● [Change DomainName]

●Domain name is optional

Setup Network

Interface	IP Address	Netmask	
RED Interface (WAN)			Dynamic
Gateway			
Primary DNS		□ Override ISP supplied DNS entries ●	
Secondary DNS			

● In Dynamic Address or PPPoE mode, the ISP supplied DNS servers can be overridden with your own DNS entries.

GREEN Interface (LAN)	192.168.123.254	255.255.255.0

Configuring the External Network when using **a** Dynamic IP

On the setup net page, choose Dynamic from the drop down list. Leave the RED Interface **(WAN) blank, as** well as the netmask.

If you wish to override the ISP supplied DNS servers, you can check the `Override ISP supplied DNS entries` and then enter a `Primary & Secondary DNS` entry.

Finally click Update to save the changes. The NetSentron will reset the network settings. This may take a moment or two.

Configuring the External Network when using a Static IP

On the setup net page, choose Static from the drop down list. Then enter your static IP address for the RED Interface (WAN) and the netmask. Then enter your gateway in the Gateway input field. Enter your primary and secondary DNS servers into the Primary & Secondary DNS input fields.

Finally click Update to save the changes. The NetSentron will reset the network settings. This may take a moment or two.

Configuring the External Network when using PPPoE (Point-to-Point Protocol over Ethernet)

On the ***setup*** net page, choose PPPoE from the drop down list. Next click ***Update to save*** the changes. The NetSentron will reset the network settings, this may take a moment or two. After the page is refreshed, there should now be a button that says **Setup PPPoE**. Click on that button to continue to configure PPPoE.

A new screen will appear that allows you to enter more settings for PPPoE, which you should have obtained from your ISP.

Idle timeout: The time the connection is allowed to be idle before it is reset.

Connect on NetSentron Restart: This should be checked for most installations.

Connection debugging: Leave *this unchecked unless you* need debugging information in the log files*.*

Reconnection: Select Persistent.

Holdoff time: Leave at 30 seconds

Maximum retries: Leave at 5

Dial on Demand for DNS: Leave this unchecked

Additional PPPoE **Settings**: Select PPPoE plugin and leave the other input boxes empty.

Authentication: Enter the username that your ISP gave you.

Enter the password that your ISP gave you.

Select PAP or CHAP from the Method drop down list.

Leave Script Name blank.

DNS: ***Select Automatic*** unless you wish to over ride the DNS supplied by your ISP. (If you wish to enter your own DNS, select Manual, then enter your DNS entries in the provided input boxes.)

Once you have everything configured, click ***Save*** **and *you will*** be returned to the setup net page. At this point you should click on the Home button. If everything is configured correctly, there should be Connect , Disconnect and Refresh buttons showing on the page. If you have a configuration error, you will need to go back to System -> setup net, then click on **Setup PPPoE**, make sure your settings are correct and click **Save**.

If the **buttons** are there, click on Connect and you should see the phrase Connected (0d 0h 0m ##s) – Broadband. Below that it should show an IP address. If you go back to System -> setup net, the proper IP address, gateway and DNS will now show up in the page. You can override the DNS settings in either the PPPoE setup page or the Setup net page.

If you wish to over ride the ISP supplied DNS servers, you can check the Override *ISP supplied DNS entries* and then enter a *Primary* & *Secondary DNS* entry.

If you change the DNS settings, click Update to save the changes. The NetSentron will reset the network settings, this may take a moment or two.

Configuring ***the External*** Network – Verifying ***Your*** Settings

After changing the external network settings, you should now reboot the NetSentron. To reboot, follow these steps:

From the NetSentron Interface, click the System button. Then the shutdown button and the Shutdown page appears.
Click the Reboot button.
Wait a few minutes for the NetSentron to restart all of its services and then log back into the administrative guide.

Verify that your NetSentron is connected to the internet by clicking on the **Home** button. You should see an IP address showing on the home page. If you have an IP address, then you can bring up a new page in your browser and try surfing the internet.
If you do not have an IP address showing, then there is probably a configuration error. Go back through your settings and double check them.

3. Once you have entered the IP address or the Dynamic DNS name in to the Local VPN Hostname/IP box, you will need to check the top `Enabled` box. The lower Enabled box is used when setting up a connection on a wireless network. This is explained in the Wireless section of Chapter 7.

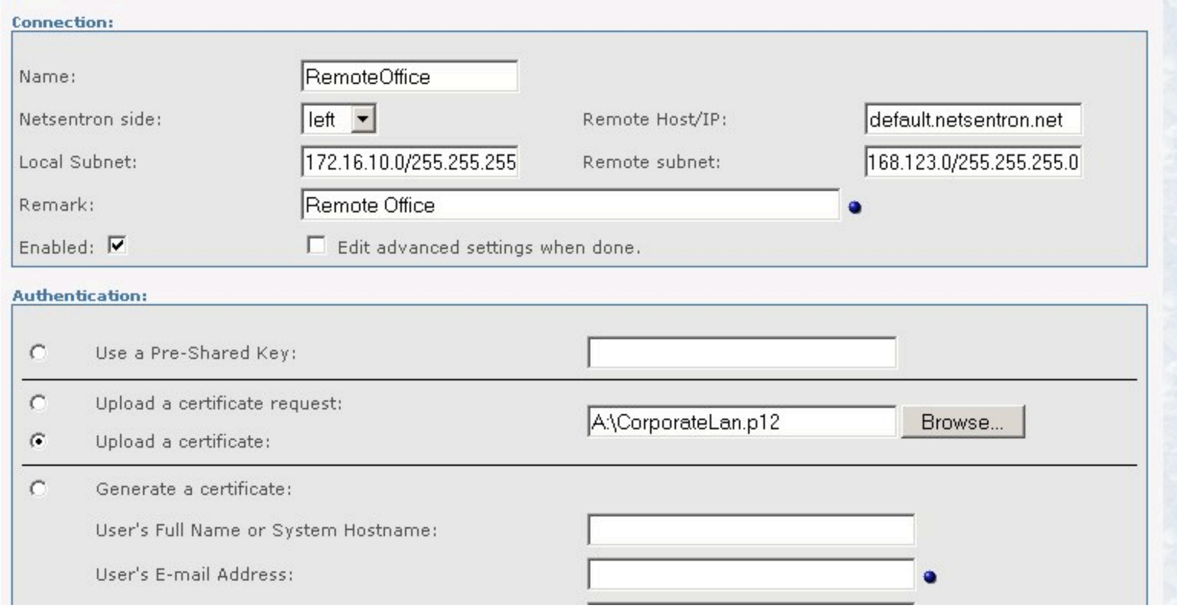
4. In the `Connection Status and Control` panel click the Add button.The Connection type panel appears. You are given two options, Host-to-Net connection or Net-to-Net VPN. The Host to Net is for roadwarrior and the Net to Net is for creating tunnels between two NetSentrons or another IPSEC compliant devices.

5. Select the Net-to-Net for this example and click Add button. The VPN Configurations page appears. This is where you will enter configuration settings for a VPN connection from one NetSentron to another NetSentron. Fill in the fields.
   8.4: VPN Configurations Page – Local Side, below, shows what the Local side of a VPN configuration should look like.
6. First you will need to key in connection Name. For example you could call your connection "head office".

> **NOTE**
>
> You cannot use any spaces, numbers or symbols in your name. Only

letters are accepted.

8.4: VPN Configurations Page – Local Side



Connection:

Name: RemoteOffice

Netsentron side: left

Remote Host/IP: default.netsentron.net

Local Subnet: 172.16.10.0/255.255.255

Remote subnet: 168.123.0/255.255.255.0

Remark: Remote Office

Enabled: ☑

☐ Edit advanced settings when done.

Authentication:

○ Use a Pre-Shared Key:

○ Upload a certificate request:

● Upload a certificate: A:\CorporateLan.p12

○ Generate a certificate:

User's Full Name or System Hostname:

User's E-mail Address:

7. In the NetSentron side box the option left is chosen by default. Just leave it at left. This options changes which side of the configuration is local (left) or remote (right)

8. In the Remote Host/IP box, enter the Red (WAN) address or the Hostname/Dynamic DNS Name of the NetSentron on the remote side of the VPN.

9. The Local Subnet specifies which computers on your GREEN (LAN) have access to the VPN and which can be accessed from the remote side of the VPN. If you want all PCs to access the VPN, then leave the default setting in there. Standard IP Addressing for private networks controls the number of computers that can access the VPN.

10. The Remote Subnet specifies which computers on the GREEN (LAN) network of the remote NetSentron can be accessed through the VPN. It is similar to the Local Subnet, and the same rules apply.

11. In the remark box key in a useful comment to explain what the VPN configuration is all about. For example you could key in ***Corporate Headquarters*** or another descriptive phrase to help other administrators understand what the VPN tunnel is for. Any combination of letters, numbers, or symbols will work in this field.

12. Next, check the `Enabled` box in the lower left side of the Connection panel. If the `Enabled` box is not checked the configuration will not work.

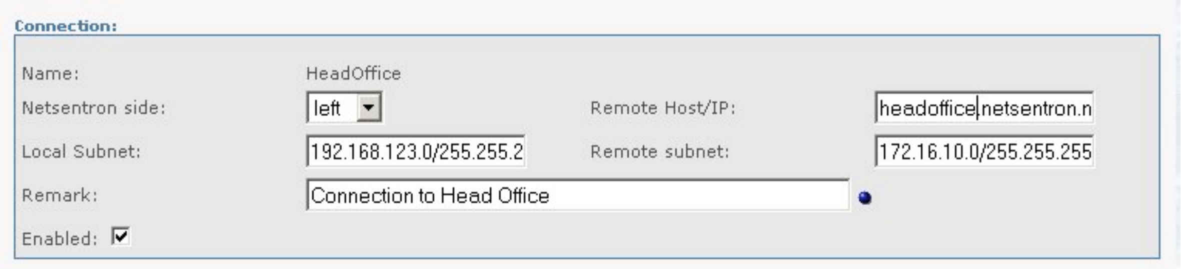
13. The final step to configure the local side of the NetSentron is to enter a Pre-Shared key. This is basically a password that allows the tunnel to be created between the two Networks. You may choose any combination of letters and numbers (underscores may also be used). **Do not enter any spaces**. Try to make it as long as possible. You will also need to write it down, as you will need to enter this information on the remote end. **Keep this key a secret**. The minimum recommended size is 32 characters, and you can enter up to 60 characters.

14. Click the Save button, located at the bottom of the page. The local side of the VPN has been configured.

15. Next, you will need to configure the remote NetSentron on the other side of the VPN. To setup the remote side follow steps 1 thru 13, except this time the local and remote are switched around, and the Remote Host/IP will be the RED (WAN) address of the NetSentron that you just configured. See *Figure 8.5: VPN Configurations Page – Remote Side* below. Notice that the Local and Remote Subnets have been reversed. *See 8.4: VPN Configurations Page – Local Side* on page 202 for a comparison. The only other change is the Remote Host/IP has

changed.

Figure 8.5: VPN Configurations Page – Remote Side



Connection:

Name: HeadOffice

Netsentron side: left ▾

Remote Host/IP: headoffice.netsentron.n

Local Subnet: 192.168.123.0/255.255.2

Remote subnet: 172.16.10.0/255.255.255

Remark: Connection to Head Office ●

Enabled: ☑

16. Once you have entered all the configuration settings for the remote side, click the Save button. If everything has been configured, then the VPN should be up and running. The status should now be showing OPEN and has turned green from the previously CLOSED red indicator. *See Figure 8.1: VPN Display – Connection and Status Control,* page 194, for an example of an open VPN.

Look on the following pages for some useful tips.

TIP 1

If your VPN is not running at this point, you will need to start an SSH session to examine the log file to see what is wrong with it. (Please see the section on SSH below to learn how to connect to the NetSentron using SSH)

Log into the NetSentron as root.

Then change directories to /var/log: **cd /var/log**

Now examine the contents of the secure file using the following command:

tail –n 100 secure

This will show you the last 100 lines of the file (this file grows in size rapidly and using a regular cat command to examine the contents would take too long. This is also the reason it is not in the Web GUI of the NetSentron)

If your connection was successful, you should see something like this at the end of the file:

```
Jan 14 07:28:51 ns200firewall pluto[564]: "RemoteOffice" #80: responding to Main Mode

Jan 14 07:28:51 ns200firewall pluto[564]: "RemoteOffice" #80: NAT-Traversal: Result using draft-ietf-ipsec-nat-t-ike-02/03: no NAT detected

Jan 14 07:28:51 ns200firewall pluto[564]: "RemoteOffice" #80: Main mode peer ID is ID_IPV4_ADDR: '24.70.136.39'

Jan 14 07:28:51 ns200firewall pluto[564]: "RemoteOffice" #80: sent MR3, ISAKMP SA established

Jan 14 07:28:51 ns200firewall pluto[564]: "RemoteOffice" #81: responding to Quick Mode

Jan 14 07:28:51 ns200firewall pluto[564]: "RemoteOffice" #81: Dead Peer Detection (draft-ietf-ipsec-dpd-03) enabled
Jan 14 07:28:51 ns200firewall pluto[564]: "RemoteOffice" #81: IPsec SA established
```

The important thing here is the last line that states IPsec SA established – this tells you that a successful tunnel has been established. If you cannot communicate to the other side, then your configuration is incorrect: go back and double check your configuration.

If it does not show IPsec SA established, then something has gone wrong. Unfortunately the error messages generated by the VPN software are a little cryptic at times. Some of the common messages and their meanings are discussed below.

TIP 2

If you are using windows and wish for the remote computers to show up in the network neighborhood, then you will need a WINS server set up at one end of the tunnel. Setting up a WINS server is beyond the scope of this manual – please consult your Microsoft help files on how to set up a WINS server.

NET-to-NET VPN Error Messages – some of the more common ones

ERROR MESSAGE	CAUSE	PROCEDURE
Jan 14 07:55:22 ns200firewall pluto[564]: "RemoteOffice" #87	Probable authentication failure (mismatch of preshared secrets?): malformed payload in packet	You have entered the wrong secret key at one end of the VPN. Double check your configuration on both ends and insures that the key is the same at both ends. Then click the restart button at each end.

Jan 14 07:57:52 ns200firewall pluto[564]: packet from 24.70.136.39:500:	Quick Mode message is for a non-existent (expired?) ISAKMP SA	This is a little more cryptic than the last one. Basically, one end of the VPN tunnel has refused to release the Security Association Key, and the other end knows it has expired or belongs to a connection that is no longer valid. This can be fixed be restarting the VPN using the blue arrows button. Sometimes both ends of the VPN tunnel will need to be restarted.
Jan 14 08:00:30 ns200firewall pluto[564]: "RemoteOffice" #98: cannot respond to IPsec SA request because no connection is known for 172.16.10.0/24===223.219.54.116...24.70.136.39===192.168.123.0/24 Jan 14 08:00:30 ns200firewall pluto[564]: "RemoteOffice" #98: sending encrypted notification INVALID_ID_INFORMATION to 24.70.136.39:500	Basically what the error is saying is that there is no connection configured for the above routing. (The routing is shown in the 172.16.10.0/24===223.219.54.116...24.70.136.39===192.168.123.0/24 part of the error message.) In plain English, you messed up one of the Local or Remote Subnets. In this case I did this purposely by setting the Remote Subnet to 192.168.0.0/255.255.255.0 knowing full well that the remote end was 192.168.123.0/255.255.255.0 Because the wrong remote subnet was specified, the VPN packets could not travel the path they expected to travel.	Re-enter the correct remote subnet.

Net-to-Net VPN – Using x509 Certificates

This section will show you how to connect two NetSentrons using a VPN that is authenticated with x509 Certificates. It is assumed that you have already gone through the section that discussed using x509 certificates and are familiar with generating, exporting, and working with certificates.

Configuring NetSentron for Roadwarrior Connection - Using x509

Certificates and

Creating x509 Certificates*,* above.

From this point on, it is assumed that you have two NetSentrons with the Host/Root certificates generated on both. If you do not, please refer to the sections listed in the above paragraph.

Requirements

You will need Web-based GUI access to both NetSentrons to complete this task. We will assume that you are behind one NetSentron already, and have external access to the remote NetSentron. Please see the section on

External **Access**, above, to learn how to access a NetSentron remotely.

Example:

For this example, we will assume that our NetSentrons are called Head Office and Remote Office. It is extremely important to keep track as to which is going to be the Head Office and which NetSentron is going to be the Remote Office so as to not get them confused.

Exporting the Certificates

The first step will be to export the certificate. Go to the VPN page of the Head Office NetSentron, and scroll down to Certificate Authorities. You should see two entries: the Root Certificate and a Host Certificate. You need to export the certificates.

1. Click on the 💾 icon on the same row as the Root Certificate. A dialog will appear that asks if you wish to save a file called cacert.pem. You want to save this file, but you will need to re-name it first. Change the name to ***HO_cacert.pem*** or some other name that allows you to remember that it is from the Head Office NetSentron.

> **NOTE**
>
> Iif you click on the 💾 icon and a certificate is displayed, rather than a download dialog, try right clicking and then use **Save As** to save the certificate

2. Next, click on the 💾 icon for the Host Certificate. Another dialog box will appear asking you to save a file called hostcert.pem. Again re-name this to something that indicates that it came from the Head Office NetSentron. (i.e. ***HO_hostcert.pem)***.

> **NOTE**
>
> If you click on the 💾 icon and a certificate is displayed, rather than a download dialog, try right clicking and then use **Save As** to save the certificate.

3. Now you will need to connect to the Remote Office NetSentron and export the Host and Root Certificates there. Remember to name them something useful that reminds you that they belong to the Remote Office NetSentron. For example you could call them ***RO_cacert.pem*** and ***RO_hostcert.pem***.

Import the Root Certificates to each NetSentron

The Root Certificates have to be imported into each NetSentron so they know about who signed the Host Certificates that we will be importing later on.

1. Go back to the VPN page of the Head Office NetSentron and scroll down to the Certificate Authorities section. You will see a couple of text boxes at the bottom with a Browse... button next to them.

2. In the text box labeled `CA Name`, enter a meaningful name for the Remote Office. For example you can use ***RemOffice***.

3. Now click on the Browse... button. Navigate to where you stored the certificates that we exported in the previous section, *Exporting the Certificates*, below. Select the `Root Certificate` that you exported from the Remote Office NetSentron, RO_cacert.pem and then click on the Upload CA Certificate button.

4. It will take a few seconds for the certificate to be imported into the NetSentron. When it has completed, you should now see a third row in the Certificate Authorities panel.

   Repeat the steps 1 through 3 only on the Remote Office NetSentron, but give the Certificate Authority a different name than you did on the Head Office box. Then import the Head Office Root Certificate. In this example it would be ***HO_cacert.pem.***

Configure a net-to-net VPN

Configuring an x509 net-to-net VPN is almost the same as connecting using a Pre-Shared key except instead of entering a Pre-Shared key, we will be selecting the Host Certificates and uploading them. If you have forgotten how to set up a Net-to-Net VPN, please see the section titled *Net-to-Net VPN – Using Pre-Shared Secrets,* page 196, for a refresher.

From this point on we will assume that you have configured the IP Address and Left/Right subnets for the VPN. Now you will move on to importing the host certificate.

1. First you will need to bring up the GUI on the Head Office NetSentron and then click on the VPN's button.
2. In the `Connection Status Control` panel, click on the Add button. The `Connection Type` panel appears.
3. Click on the **Net-to-Net Virtual Private Network radio** button and then press the Add button. The `Connection and Authentication` panels appear.
4. Key in the necessary values for the Connection area. Once that is done, select the **Upload Certificate radio button** and then click the Browse... button.

   Locate the Host Certificate you exported from the Remote Office NetSentron. Select the certificate and then hit the save button.
5. Next, connect to the Remote NetSentron and repeat steps 1 through 4, except this time you will be importing HO_hostcert.pem the Root Certificate from the Head Office NetSentron. Once completed, you should now have a running x509 based Net-to-Net VPN operating.

You can test this by attempting to ping the other side of the VPN.

TIP 3

A good knowledge and understanding of TCP/IP and subnets is required to work with VPNs successfully. It is beyond the scope of this manual to teach this subject, but it is expected that the end user is at least familiar with how subnets are created and what the numbering system represents.

NOTE

There are many more error messages that the VPN can create, too many to list here, and it is something that is learned with time. If you get stuck, you can call a KDI technical representative at 1-800-661-1755, or e-mail at support@netsentron.com and they can assist you with your problems.

NetSentron to Roadwarrior VPN

The Roadwarrior VPN is a type of connection that allows a VPN tunnel to be created from a computer anywhere on the Internet. Salespeople are often on the road - hence the name Roadwarrior – often use this particular type of VPN on laptops.

NOTE

If you are using a Pre-Shared Key for Roadwarrior, you can only configure one Roadwarrior connection and all Roadwarriors will need to share this same key. It is recommended that you use x509 certificates for Roadwarriors. x509 certificates are much more secure and they allow you to assign different certificates for each Roadwarrior.

For instructions on how to set up a Roadwarrior VPN using x509 certificates, see below.

Roadwarrior Connections – Using Pre-Shared Secrets

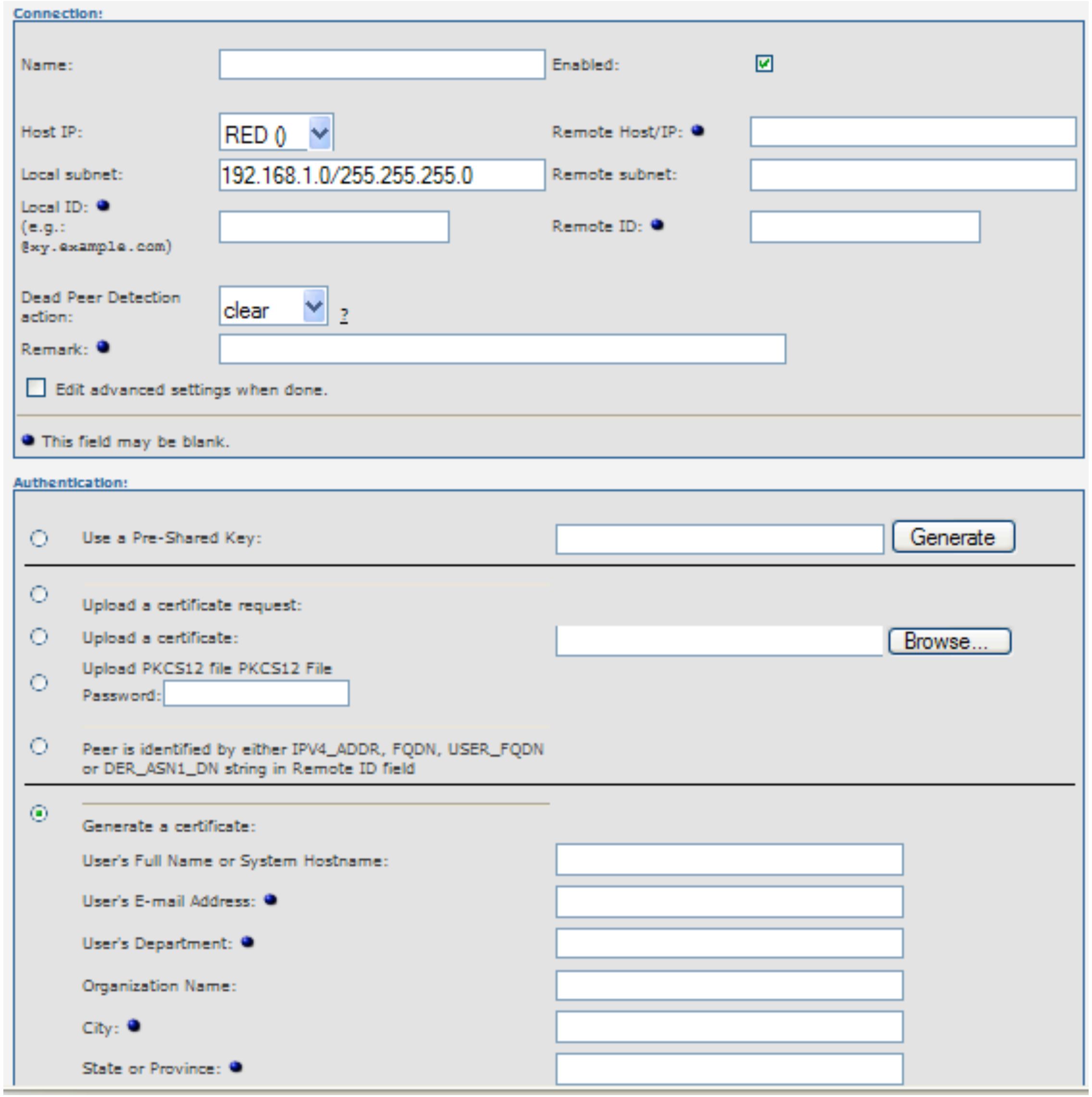
The following are instructions on how to setup your NetSentron to allow a Roadwarrior connection using a pre-shared secret.

1. From the Administration Interface, click on the VPN's button. The VPN page appears. See *Figure 8.2: VPN Page*.

2. In the `Connection Status and Control` panel click the Add button. The Connection type panel appears. You are given two options, `Host-to-Net connection` or `Net-to-Net VPN`. For a Roadwarrior connection you will be choosing Host-to-Net Virtual Private Network (Roadwarrior).

3. Use your mouse to select `Host-to-Net Virtual Private Network`, and click the Add button. The VPN Configurations page appears. *See Figure 8.5: VPN Configurations Page – Roadwarrior, on the next page.* This is where you will enter configuration settings for a Roadwarrior VPN. Fill in the required fields.

Figure 8.5: VPN Configurations Page – Roadwarrior



Connection:

Name: Enabled: ☑

Host IP: RED () Remote Host/IP: ●

Local subnet: 192.168.1.0/255.255.255.0 Remote subnet:

Local ID: ● (e.g.: @xy.example.com) Remote ID: ●

Dead Peer Detection action: clear ?

Remark: ●

□ Edit advanced settings when done.

● This field may be blank.

Authentication:

○ Use a Pre-Shared Key: Generate

○ Upload a certificate request:

○ Upload a certificate: Browse...

○ Upload PKCS12 file PKCS12 File Password:

○ Peer is identified by either IPV4_ADDR, FQDN, USER_FQDN or DER_ASN1_DN string in Remote ID field

◉ Generate a certificate:

User's Full Name or System Hostname:

User's E-mail Address: ●

User's Department: ●

Organization Name:

City: ●

State or Province: ●

4. First you will need to key in connection name. For example you could call your connection 'remoteoffice'.

NOTE

You cannot use any spaces, numbers or symbols in your name. Only letters are accepted.

5. The Local Subnet specifies which computers on your GREEN (LAN) have access to the VPN and which can be accessed from the remote side of the VPN. If you want all PCs to access the VPN, then leave the default setting in there. Standard IP Addressing for private networks controls the number of computers that can access the VPN.

6. The Remote Host/IP allows the administrator to restrict the Roadwarrior connection to one specific IP address or host. This field is optional.

7. In the `Remark` field, key in a useful comment to explain what the VPN configuration is all about. For example you could key in '*Corporate Headquarters'* or another descriptive phrases to help other administrators understand what the VPN tunnel is for. Any combination of letters, numbers, or symbols will work in this field.

8. Next, check the `Enabled` box in the lower left side of the `Connection` panel. If the `Enabled` box is not checked the configuration will not work.

9. The final step is to enter a Pre-Shared key. This is basically a password that allows the tunnel to be created between the two Networks. You may choose any combination of letters and numbers (underscores may also be used). **Do not enter any spaces**. Try to make it as long as possible. You will also need to write it down, as you will need to enter this information on the remote end. **Keep this key a secret**. The minimum recommended size is 32 characters, and you can enter up to 60 characters.

NOTE

If you are using a Pre-Shared Key for Roadwarrior, you can only configure one Roadwarrior connection and all Roadwarriors will need to share this same key. It is recommended that you use x509 certificates for Roadwarriors as they are much more secure and allow you to assign different certificates for each Roadwarrior. See the x509 section for more information.

10. Click the Save button, located at the bottom of the page. Your

NetSentron has now been configured to allow for Roadwarrior connections.

Windows 2000/XP Roadwarrior Connections with built-in IPSEC, Using Linsys VPN Client

Windows 2000 and XP come with their own implementations of IPSEC (IP Security) protocol that allows you to connect securely to your network behind a NetSentron.

NOTE

While every effort has been made to simplify VPN connections on the NetSentron, VPNs are a very complex subject. Therefore, those attempting to make this kind of connection should have some experience with networking and VPN concepts before attempting this.

Using Pre-Shared Secrets

The first connection we will describe is the one that uses the Pre-Shared Secrets. This method can be compared to setting up a connection with a password, as that is really all the Pre-Shared Secret is. This is the less secure method of creating a VPN and we recommend that you use x509 Certificates as a more secure connection method. Also, you can only configure one Pre-Shared Secret Roadwarrior connection, and ALL Roadwarriors must share this same key: that is one of the reasons why it is considered less secure. Using x509 Certificates you can have as many Roadwarrior connections as you wish and each connection has its own certificate.

Requirements

- To connect to the NetSentron, we are going to use a VPN client created by Enrique E. Martinez. This is a freely downloadable and usable VPN client released under the GPL. Download and install the tool as instructed. You can download this tool from the following websites:
  - From the NetSentron website: (http://www.netsentron.com/utilities.html)
  - Or from Sourceforge

(http://sourceforge.net/projects/lsipsectool).

- Please insure that your Windows PC is fully patched and up to date.

NOTE

Those using Windows XP with Service Pack 2 or newer may need a hotfix from Microsoft to allow ICMP to flow across the VPN. Please http://support.microsoft.com/?kbid=889527 for more information.

- You will need to create a Host to Net (Roadwarrior) VPN connection Please refer to *Roadwarrior Connections – Using Pre-Shared Secrets*, above*,* in this manual*.*
- You will need to write down the Red (WAN) IP Address of your NetSentron, the Green (LAN) address of your NetSentron , the Pre-Shared Key and the allowable range that you will allow your Roadwarrior client to connect to (this is accomplished through an ip/netmask combination such as 192.168.1.0/255.255.255.0, which would allow the VPN Client to connect to the entire 192.168.1.x subnet). You can find this information on the VPN page. To locate the VPN page go to *VPN Connection and Status Control,* above*.* Use the table below to key in the required information.

Table 1: VPN – Windows 2000/XP IPSEC Pre-Shared Secret Reference Table

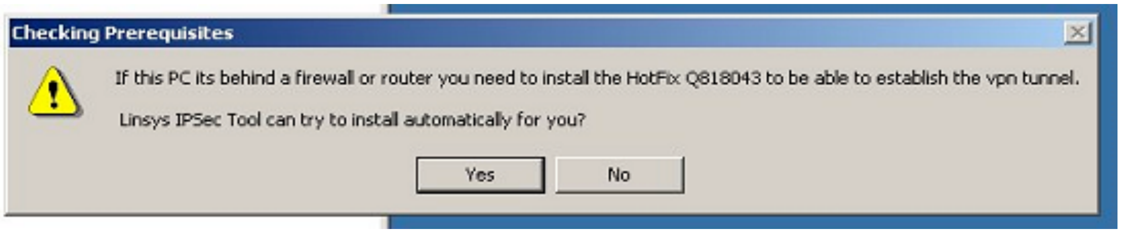
RED (WAN) Address:________________________
GREEN (LAN) Address:______________________
Pre-Shared Key:___________________________
Local Subnet: ____________________________
Remote Subnet: ___________________________

- Once you have updated your Windows box, installed the required VPN client and collected the required information, you are ready to proceed.

From your Windows machine, start up the Linsys VPN Client.

NOTE
 If your machine is not up to date or properly patched, the VPN client may tell you this and ask you if you want to attempt to update your system, as shown in *Figure 8.5: Windows Checking Prerequisites,* below.

Figure 8.6: Windows Checking Prerequisites



Checking Prerequisites

If this PC its behind a firewall or router you need to install the HotFix Q818043 to be able to establish the vpn tunnel.

Linsys IPSec Tool can try to install automatically for you?

If you wish to let the VPN Client search for and install the patch, click the Yes button. If not, take note of the HotFix number (use the table below), click the No button and then exit the VPN client. To find out more about hotfix go http://www.microsoft.com/ and search for the patch, download it manually, and then install it.

Table 2: VPN – Windows 2000/XP IPSEC HotFix Number

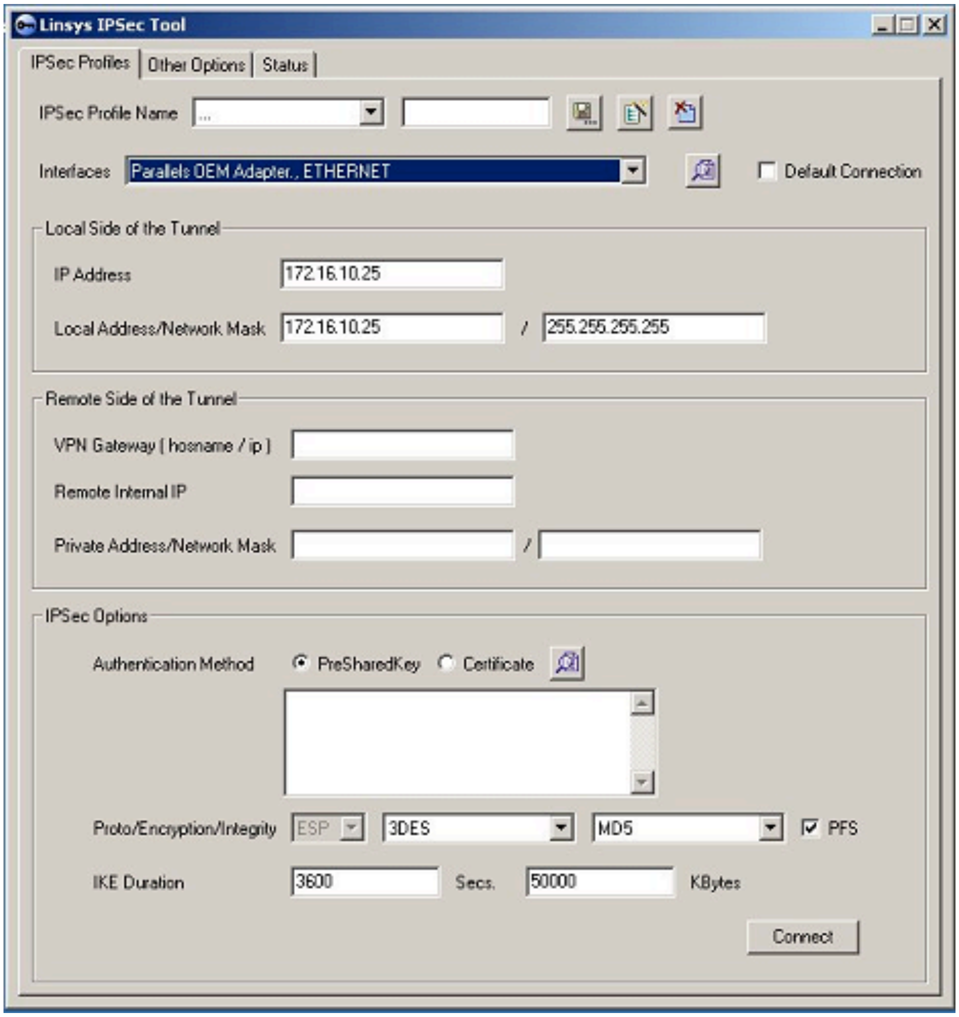
HotFix Number:_______________________

With the Linsys VPN Client started the first step is to enter is a name for the VPN. This should be entered in the empty box to the right of the IPSec Profile Name.

NOTE

If you have more than one Ethernet card, use the Interfaces drop down list and then select the card you want by clicking on it. Also note that when you select your Ethernet card from the drop down list, the IP addresses for the Local Side of the Tunnel will automatically be entered. Please verify that they are correct.

Figure 8.7: Linsys IPSec Tool – Configuring Using PreShared Key



IPSec Profile Name: ...

Interfaces: Parallels OEM Adapter., ETHERNET

☐ Default Connection

Local Side of the Tunnel

IP Address: 172.16.10.25

Local Address/Network Mask: 172.16.10.25 / 255.255.255.255

Remote Side of the Tunnel

VPN Gateway (hosname / ip):

Remote Internal IP:

Private Address/Network Mask: /

IPSec Options

Authentication Method: ● PreSharedKey ○ Certificate

Proto/Encryption/Integrity: ESP 3DES MD5 ☑ PFS

IKE Duration: 3600 Secs. 50000 KBytes

Next, you will need to enter the information for the Remote Side of the tunnel. This is the information you gathered and entered into *Table 2,* above.

- In the `IP Address` field, enter the hostname or IP Address of your NetSentron. This is the RED (WAN) address. This goes into the VPN Gateway (hostname/ip) field.
- In the `Remote Internal IP` field, enter the GREEN (LAN) address of your NetSentron.
- In the `Private Address/Network Mask` field, enter the range of IP addresses you wish to allow the VPN client access to on the NetSentron network. Specifying the correct netmask does this). If the network behind the NetSentron is 192.168.1.1 – 192.168.1.254 and you wish to allow the VPN client access to all machines on that

network, then you would enter 192.168.1.0/255.255.255.0

Now you will need to enter information into the IPSec Options area.

- Check PreSharedKey radio button.
- In the field below the PreSharedKey radio button, enter the Pre-Shared Key that you entered on the NetSentron VPN configuration.
- Leave the Proto/Encryption/Integrity options as they are (3DES/MD5/ PFS Enabled)
- Adjust the IKE Duration to 3600 from the default 3500

Now it is time to save your settings. Click on the disk icon next to the profile name near the top of the dialog box. You are now ready to test your VPN connection using a pre-shared key. Go to *Testing Roadwarrior connection with IPSec (x509 certificate/pre-shared key)*, below.

Using x509 Certificates

x509 Certificates are the preferred way of connecting your Roadwarrior client to the NetSentron. This is for a couple of reasons, the main one being that each client can have their own certificate and you can revoke certificates privileges at any time. The alternative, Pre-Shared Keys, would require you to have to call up each of your clients and have them change their key.

Requirements

- To connect to the NetSentron, we are going to use a VPN client created by Enrique E. Martinez. This is a freely downloadable and usable VPN client released under the GPL. Download and install the tool as instructed. You can download this tool from the following websites:
  - From the NetSentron website: (http://www.netsentron.com/utilities.html)
  - Or from Sourceforge (http://sourceforge.net/projects/lsipsectool).
- Please insure that your Windows PC is fully patched and up to date.

NOTE

Those using Windows XP with Service Pack 2 or newer may need a hotfix from Microsoft to allow ICMP to flow across the VPN. Please see http://support.microsoft.com/?kbid=889527 for more information.

- You will need to create a Host to Net (Roadwarrior) VPN connection Please refer to *Roadwarrior Connections – Using Pre-Shared Secrets*, above, in this manual.

- You will need to write down the Red (WAN) IP Address of your NetSentron, the Green (LAN) address of your NetSentron, the x509 Certificate and the allowable range that you will allow your Roadwarrior client to connect to (this is accomplished through an ip/netmask combination such as 192.168.1.0/255.255.255.0, which would allow the VPN Client to connect to the entire 192.168.1.x subnet). You can find this information on the VPN page. To locate the VPN page go to *VPN Connection and Status Control*, above. Use the table below to key in the required information.

Table 3: VPN – Windows 2000/XP IPSEC Certificate Reference Table

RED (WAN) Address:______________________
GREEN (LAN) Address:____________________
X509 Certificate:_________________________
Local Subnet: ____________________________
Remote Subnet: __________________________

Once you have updated your Windows box, installed the required VPN client and collected the required information, you are ready to proceed. (*Go back to Table 1 to confirm you have all the requirements*)

1. The first thing you will need to do is to need to get the certificate that you created for the VPN connection on the NetSentron over to your Windows PC. This can be done in a variety of ways, the easiest way is to start a browser and connect to the Web based interface of your NetSentron. Then go to the VPN section, find the VPN connection that you have previously configured and click on the blue disk icon. This should start the Save as Dialog in your browser. Save this certificate somewhere you can retrieve it from. The certificate should be save in

P12 format (i.e. it should have an extension of P12)

2. Now, you will Copy the certificate over to your Windows PC. Do not forget where you saved it
3. From your Windows machine, start up the Linsys VPN Client.

NOTE

If your machine is not up to date or properly patched, the VPN client may tell you this and ask you if you want to attempt to update your system, as shown in *Figure 8.5,* above.

If you wish to let the VPN Client search for and install the patch, click the ***Yes*** button. If not, take note of the HotFix number (*use Table 2, above*), click the ***No*** button and then exit the VPN client. To find out more about hotfix go http://www.microsoft.com/ and search for the patch, download it manually, and then install it.

4. With the Linsys VPN Client started the first step is to enter is a name for the VPN. This should be entered in the empty box to the right of the IPSec Profile Name.

NOTE

If you have more than one Ethernet card, use the Interfaces drop down list and then select the card you want by clicking on it. Also notice that when you select your Ethernet card from the drop down list, the IP addresses for the Local Side of the Tunnel will automatically be entered. Please verify that they are correct.

5. Next, you will need to enter the information for the Remote Side of the tunnel. This is the information you gathered and entered into *Table* above.

- In the IP Address field, enter the hostname or IP Address of your NetSentron. This is the RED (WAN) address. This goes into the VPN Gateway (hostname/ip) field.
- In the Remote Internal IP field, enter the GREEN (LAN) address of

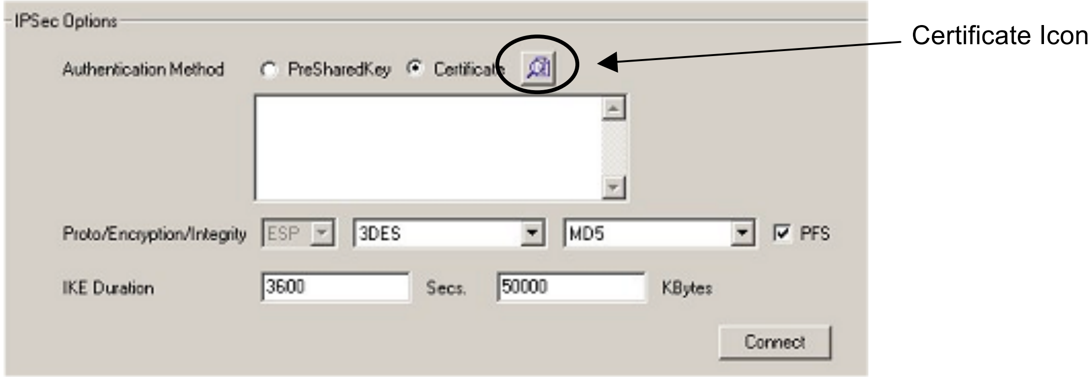
your NetSentron.

- In the Private Address/Network Mask field, enter the range of IP addresses you wish to allow the VPN client access to on the NetSentron network. (Specifying the correct netmask does this). If the network behind the NetSentron is 192.168.1.1 – 192.168.1.254 and you wish to allow the VPN client access to all machines on that network, then you would enter 192.168.1.0/255.255.255.0

6. Now you will need to enter information into the IPSec Options area.

7. Check the Certificate radio button.

Figure 8.8: Linsys IPSec Tool – Configuring Using Certificate



IPSec Options

Authentication Method ○ PreSharedKey ● Certificate

Proto/Encryption/Integrity: ESP, 3DES, MD5, ☑ PFS

IKE Duration: 3600 Secs. 50000 KBytes

8. Next, click on the icon to the right of the word `Certificate`. (It looks like a magnifying glass over a newspaper) This will bring up the Certificates dialog.

9. Click on **My Certificates** and all of the Root Authority Certificates should disappear leaving only your certificates. If this is you first time importing a certificate, the text area will be blank.

10. Next, click on the ✚ icon. The Import Certificates dialog box appears.

11. Click on the folder icon to browse to the directory where you stored the P12 certificate from the NetSentron. Enter the password that you entered on the NetSentron to secure the certificate.

12. Check the `Exportable` option, and then click the ➡ icon. A dialog will pop up with some Spanish messages and an OK button. The dialog is telling you that the certificate has been imported properly.

13. Click the **OK** button. You should be returned to the `Certificates` dialog and the Certificate from the NetSentron should be showing up in the list.

14. Highlight the certificate you just imported and then double click on it. You are returned to the main Linsys window. You should see some new entries under the Certificates radio button, something that looks like C="CA", O="KDI", CN="KDI CA"

> **NOTE**
>
> Your entries will differ based on what you entered in your NetSentron when you created the ROOT Certificate. As long as something is entered there that looks similar to what is above, everything is ok.

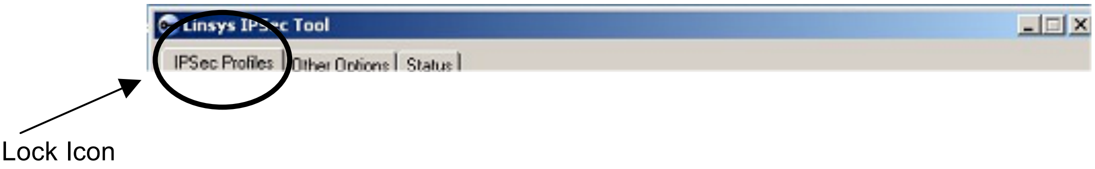
15. Click on the save icon to save your settings. You are now ready to test your VPN using an x509 certificate.

Testing Roadwarrior connection with IPSec (x509 certificate/pre-shared key)

Once you have configured your Windows 2000/XP with built-in IPSec, you are now ready to connect, however, there are a couple of things you can do to help assist in debugging if problems arise.

1. From the Lynsys VPN Client, right click on the lock icon in the taskbar. *See Figure 8.9: Linsys IPSec Tool-Lock Icon*

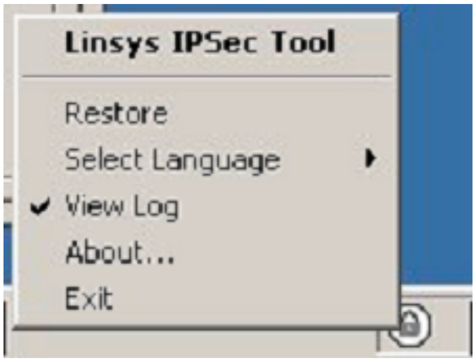
Figure 8.9: Linsys IPSec Tool – Lock Icon



2. A selection box will appear. *See Figure 8.10 below.*

3. Click on **View Log**. The Log Viewer for the VPN Client appears. This log can be extremely helpful in determining connection problems when connecting to the NetSentron.

Figure 8.10: Linsys IPSec Tool – Selection Box

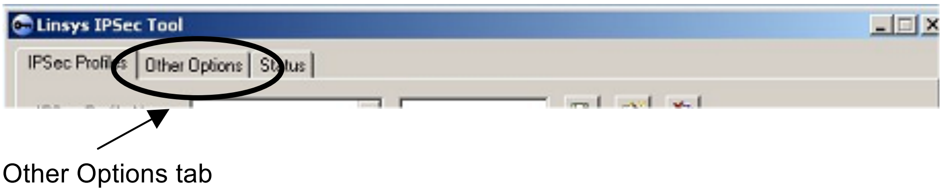


4. Next, click on the Other Options tab located on the top of the VPN Client. *See Figure 8.11,* below.

5. Select `Debug Enabled`. This will output extra information to the View Log Window.

> **NOTE**
>
> After attempting to connect to the NetSentron, you can also click on Restore to bring the VPN Client back up on the Desktop. Clicking Connect again will disconnect the VPN Client if connected, or it will stop it from attempting any further connections.

Figure 8.11: Linsys IPSec Tool – Other Options Tab

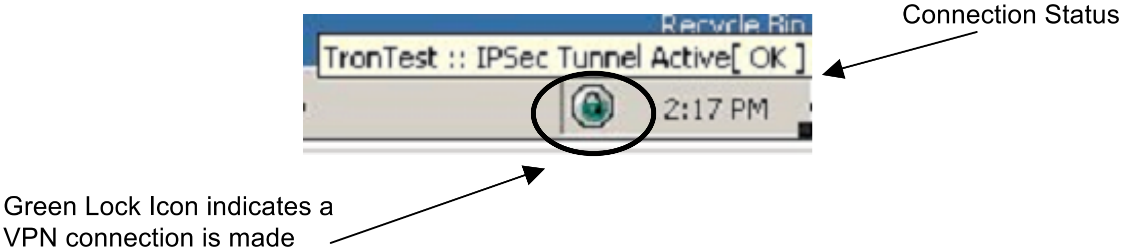


6. At this point if everything is configured correctly, you should have a working VPN. The Lock Icon in the task bar turning a greenish color

will indicate this. *See Figure 8.12 on the next page.*

> **Note**
>
> If you put the mouse over the icon, it should also show the connection status.

Figure 8.12: Linsys IPSec Tool – Green Lock Icon

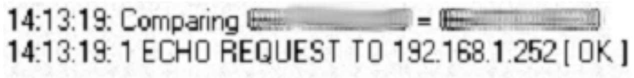


TronTest :: IPSec Tunnel Active[OK]

Sample Good Connections:

See Figure 8.13: Linsys IPSec Tool Log Window – Good Connection below for an example of a good connection

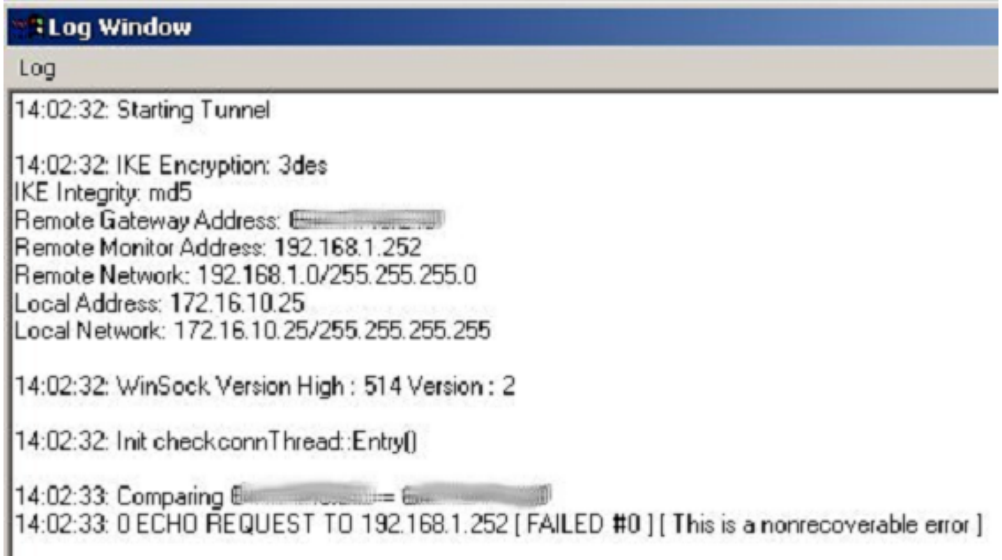
Figure 8.13: Linsys IPSec Tool Log Window – Good Connection



```
14:13:19: Comparing [redacted] = [redacted]
14:13:19: 1 ECHO REQUEST TO 192.168.1.252 [ OK ]
```

See Figure 8.14: Linsys IPSec Tool Log Window – Bad Connection on the next page for an example of a bad or problematic connection. If this is the case, then double check all your settings and try again.

Figure 8.14: Linsys IPSec Tool Log Window – Bad Connection



```
14:02:32: Starting Tunnel

14:02:32: IKE Encryption: 3des
IKE Integrity: md5
Remote Gateway Address: [redacted]
Remote Monitor Address: 192.168.1.252
Remote Network: 192.168.1.0/255.255.255.0
Local Address: 172.16.10.25
Local Network: 172.16.10.25/255.255.255.255

14:02:32: WinSock Version High : 514 Version : 2

14:02:32: Init checkconnThread::Entry()

14:02:33: Comparing [redacted] = [redacted]
14:02:33: 0 ECHO REQUEST TO 192.168.1.252 [ FAILED #0 ] [ This is a nonrecoverable error ]
```

Configuring NetSentron for Roadwarrior Connection - Using x509 Certificates

Creating a Roadwarrior connection using an x509 certificate is similar to the Roadwarrior Pre-Shared Key set up; however, the difference is that you will need to generate a certificate instead of entering a Pre-Shared Key. If you have not already created an x509 certificate refer to

Creating x509 Certificates on page 230.

If you have already created an x509 certificate, follow the instructions below to set up a Roadwarrior VPN.

1. From the Administration Interface, click on the VPN's button. The VPN page appears.

2. In the `Connection status and Control` panel click the Add button. The Connection type panel appears. You are given two options, `Host-to-Net connection` or `Net-to-Net VPN`.

   For a Roadwarrior connection you will be choosing Host-to-Net Virtual Private Network (Roadwarrior).

3. Use your mouse to select `Host-to-Net Virtual Private Network`, and click Add button. The `VPN Configurations` page appears. This is where you will enter configuration settings for a Roadwarrior VPN. Fill in the required fields.

4. First you will need to key in connection Name. For example you could call your connection 'remoteoffice'.

> **Note**
>
> You cannot use any spaces, numbers or symbols in your name. Only letters are accepted.

5. The Local Subnet specifies which computers on your GREEN (LAN) have access to the VPN and which can be accessed from the remote side of the VPN. If you want all PCs to access the VPN, then leave the default setting in there. Standard IP Addressing for private networks controls the number of computers that can access the VPN.

6. The Remote Host/IP allows the administrator to restrict the Roadwarrior connection to one specific IP address or host. This field is optional.

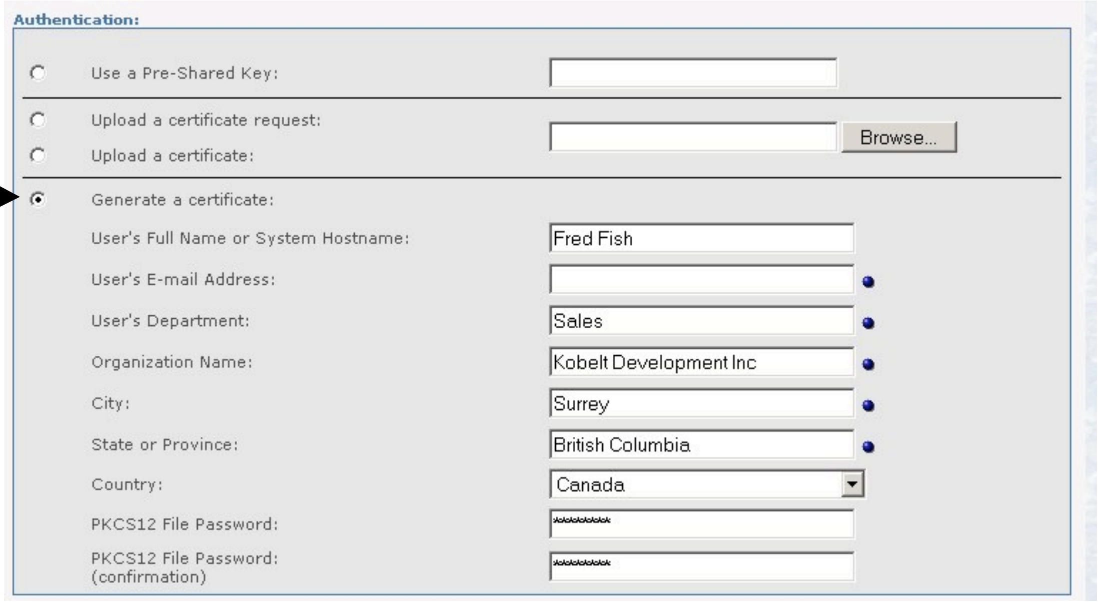
7. In the remark field, key in a useful comment to explain what the VPN configuration is all about. For example you could key in 'Corporate Headquarters' or another descriptive phrases to help other administrators understand what the VPN tunnel is for. Any combination of letters, numbers, or symbols will work in this field.

8. Next, check the `Enabled` box in the lower left side of the Connection panel. If the `Enabled` box is not checked the configuration will not work.

9. In the `Authentication` panel, select the radio button next to **Generate a certificate**. *See Figure 8.15: VPN – Authentication Panel,* on the next page.

Figure 8.15: VPN – Authentication Panel

Generate a certificate is selected



Authentication:

○ Use a Pre-Shared Key:

○ Upload a certificate request:

○ Upload a certificate:

● Generate a certificate:

User's Full Name or System Hostname: Fred Fish

User's E-mail Address:

User's Department: Sales

Organization Name: Kobelt Development Inc

City: Surrey

State or Province: British Columbia

Country: Canada

PKCS12 File Password: ********

PKCS12 File Password: (confirmation) ********

10. In the `User's Full Name` or `System Hostname` field key in the user name or some other descriptive comment. This will also be the name of the certificate.

11. In the `User's E-mail Address` field is optional and best left blank.

12. `User's Department` field is optional; you may enter data there if needed.

13. In the `Organization Name` field, key in the name of your company.

14. In the `City` field, key in your city. This field is optional; however, it makes for better identification.

15. In the `State or Province` field, key in your state or province name. This field is also optional. Note: Key in the full name i.e British Columbia not BC.

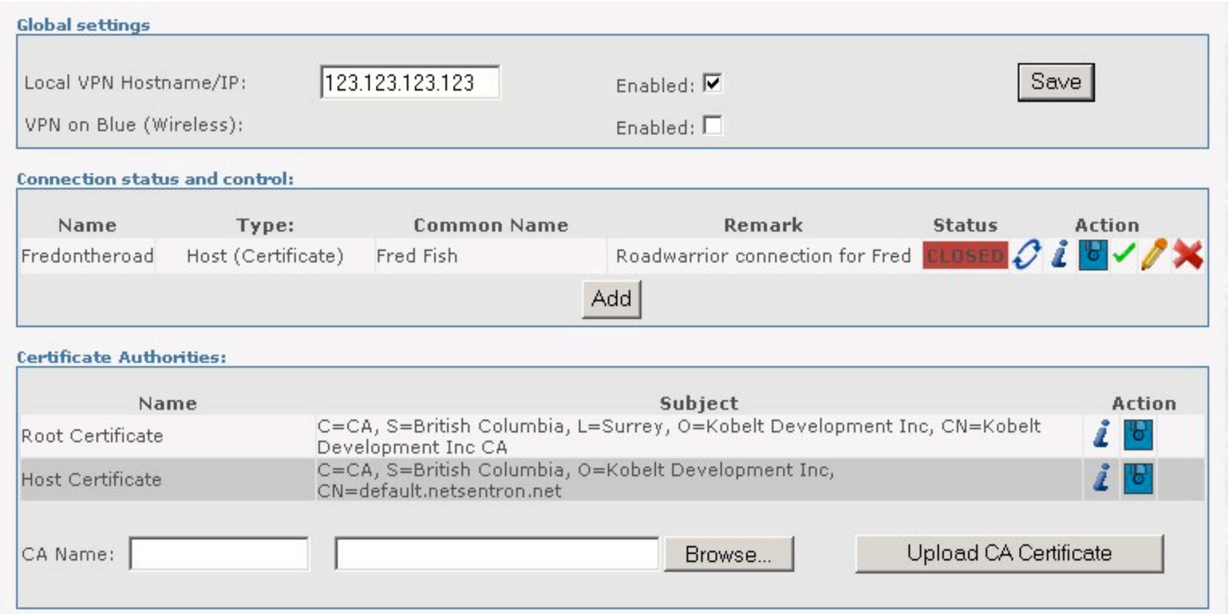
16. In the `Country` field, use the drop down menu to select your country.

17. In the PKCS12 File Password field, key in a password. Re-enter the password in the confirmation field below.

> **NOTE**
>
> If you forget this password, you will have to create a new certificate.

18. Click the Save button. If there are no errors you will be returned to the VPN page. For an example of what your VPN Certificate Authorities panel should look like refer to *Figure* below. Your NetSentron is now set up to allow Roadwarriors using x509 certificates.

Figure 8.16: VPN – Authentication Panel



Global settings

Local VPN Hostname/IP:	123.123.123.123	Enabled: ☑	Save
VPN on Blue (Wireless):		Enabled: ☐	

Connection status and control:

Name	Type:	Common Name	Remark	Status	Action
Fredontheroad	Host (Certificate)	Fred Fish	Roadwarrior connection for Fred	CLOSED	↻ i 💾 ✓ ✎ ✗

Add

Certificate Authorities:

Name	Subject	Action
Root Certificate	C=CA, S=British Columbia, L=Surrey, O=Kobelt Development Inc, CN=Kobelt Development Inc CA	i 💾
Host Certificate	C=CA, S=British Columbia, O=Kobelt Development Inc, CN=default.netsentron.net	i 💾

CA Name: | Browse... | Upload CA Certificate

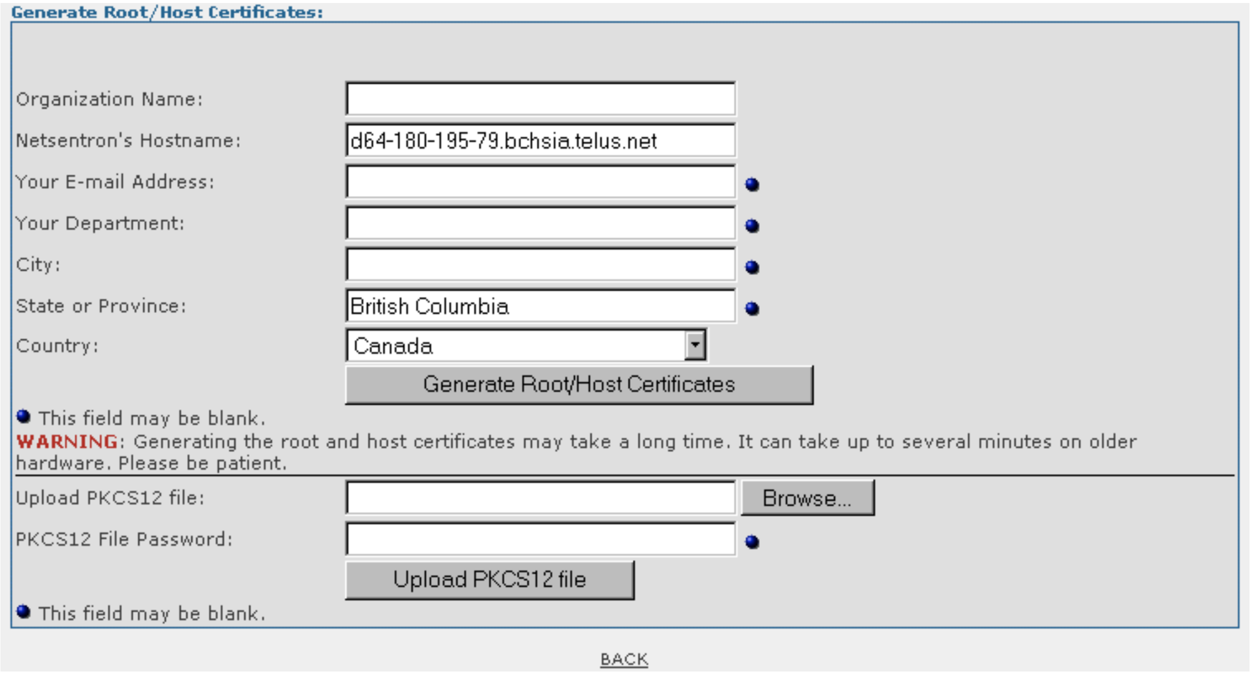
x509 Certificates

To use x509 certificates on the NetSentron, we need to create a Certificate Authority to generate certificates. You can generate the certificate yourself or you can have a Certificate Authority generate one for you. Follow the instructions below to create your own Certificate.

Creating x509 Certificates

1. From the Administration Interface, click on the VPN's button. The VPN page appears.
2. Click the Generate Root/Host Certificates button. `The Generate Root/Host Certificates` panel appears. *See Figure below*. Fill in the required fields.

Figure 8.17: Generate Root/Host Certificates Panel



Generate Root/Host Certificates:

Organization Name:	
Netsentron's Hostname:	d64-180-195-79.bchsia.telus.net
Your E-mail Address:	●
Your Department:	●
City:	●
State or Province:	British Columbia ●
Country:	Canada

● This field may be blank.
WARNING: Generating the root and host certificates may take a long time. It can take up to several minutes on older hardware. Please be patient.

Upload PKCS12 file:	
PKCS12 File Password:	●

● This field may be blank.

3. In the `Organization Name` field you **must** key in your company name.
4. In the `Netsentron's Hostname` field you **must** key in your NetSentron Hostname.

> **NOTE**
>
> This field may already have data in it; just key in your data over it. Your E-mail Address field is optional and best left blank. Your Department field is also optional.

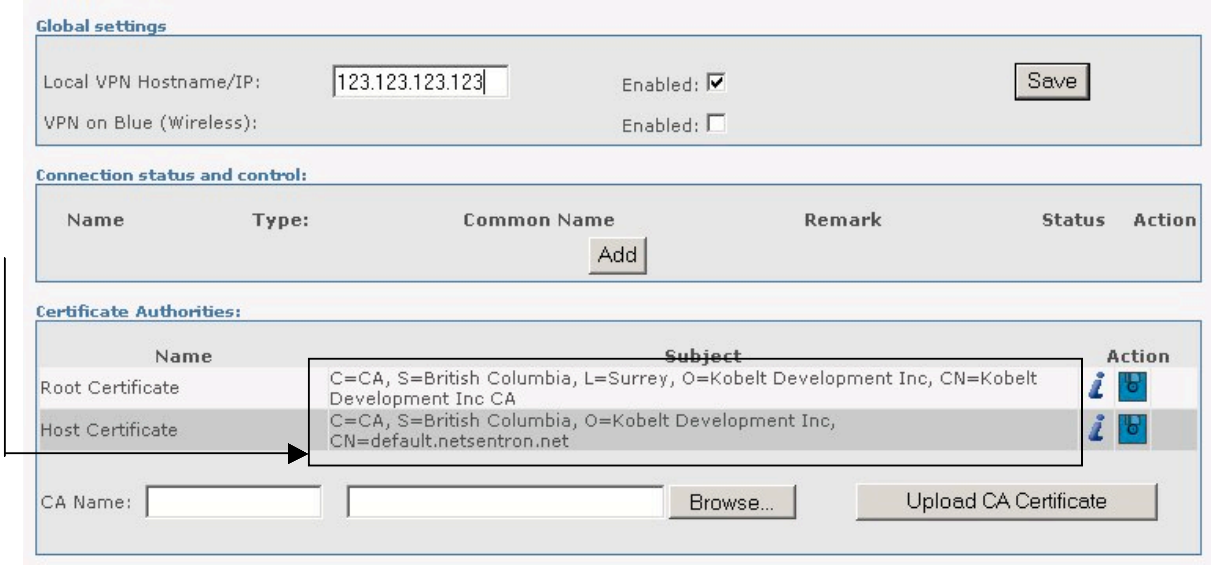
5. In the `City` field, key in your city. This field is optional; however, it makes for better identification.

6. In the `State or Province` field, key in your state or province name. This field is also optional

7. In the `Country` field, use the drop down menu to select your country. You **must** have a country selected.

8. Once you have entered the information into the fields, click on the Generate Root/Host Certificates button. The NetSentron will work for a few seconds and then you are returned to the VPN display. The Root Certificate is displayed in the `Certificate Authorities` panel. *See Figure below.*

Figure 8.18: VPN – Certificate Authorities Panel



Global settings

Local VPN Hostname/IP: 123.123.123.123 Enabled: ☑ Save

VPN on Blue (Wireless): Enabled: ☐

Connection status and control:

Name	Type:	Common Name	Remark	Status	Action

Add

Certificate Authorities:

Name	Subject	Action
Root Certificate	C=CA, S=British Columbia, L=Surrey, O=Kobelt Development Inc, CN=Kobelt Development Inc CA	ℹ 💾
Host Certificate	C=CA, S=British Columbia, O=Kobelt Development Inc, CN=default.netsentron.net	ℹ 💾

CA Name: Browse... Upload CA Certificate

As you can see, the information you entered on the previous page is now contained in the certificates.

9. Click on the ℹ information icon to read the contents of your certificates in detail. Now you can set up a Roadwarrior VPN Connection using an x509 certificate.

Windows 2000/XP Roadwarrior Connections with built-in IPSec –Using the Green Bow VPN Client

Windows 2000 and XP come with their own implementations of IPSec (IP Security) protocol. That allows you to connect securely to your network behind a NetSentron.

NOTE
While every effort has been made to simplify VPN connections on the NetSentron, VPNs are a very complex subject and as such someone attempting to make this kind of connection should have some experience with Networking concepts and VPN concepts before attempting this kind of connection.

Using Pre-Shared Secrets

The first connection we will describe is the one that uses the Pre-Shared Secrets. This method can be compared to setting up a connection with a password, as that is really all the Pre-Shared Secret is. This is the less secure method of creating a VPN and we recommend that you use x509 Certificates as a more secure connection method. Also, you can only configure one Pre-Shared Secret Roadwarrior connection, and ALL Roadwarriors must share this same key, that is one of the reasons why it is considered less secure. Using x509 Certificates you can have as many Roadwarrior connections as you wish and each connection has its own certificate.

Requirements

To connect to the NetSentron, we are going to use VPN client the Green Bow.

This is a licensed program and has a one-time license fee. You can download this tool from the following website:

- http://www.thegreenbow.com

Please insure that your Windows PC is fully patched and up to date.

You will need to create a Host to Net *(Roadwarrior)* VPN connection *Please refer to Roadwarrior Connections – Using Pre-Shared Secrets,* above, in this manual*.* You will need to write down the Red (WAN) IP Address of your NetSentron, the Green (LAN) address of your NetSentron, the Preshared Key and the allowable range that you will allow your Roadwarrior client to connect to (this is accomplished through an ip/netmask combination such as 192.168.1.0/255.255.255.0, which would allow the VPN Client to connect to the entire 192.168.1.x subnet). You can find this information on the VPN page. To locate the VPN page go to *VPN Connection and Status Control,* above, in this manual*.* Use the table below to key in the required information.

Table 4: VPN – Windows 2000/XP IPSec Pre-Shared Secret Reference Table

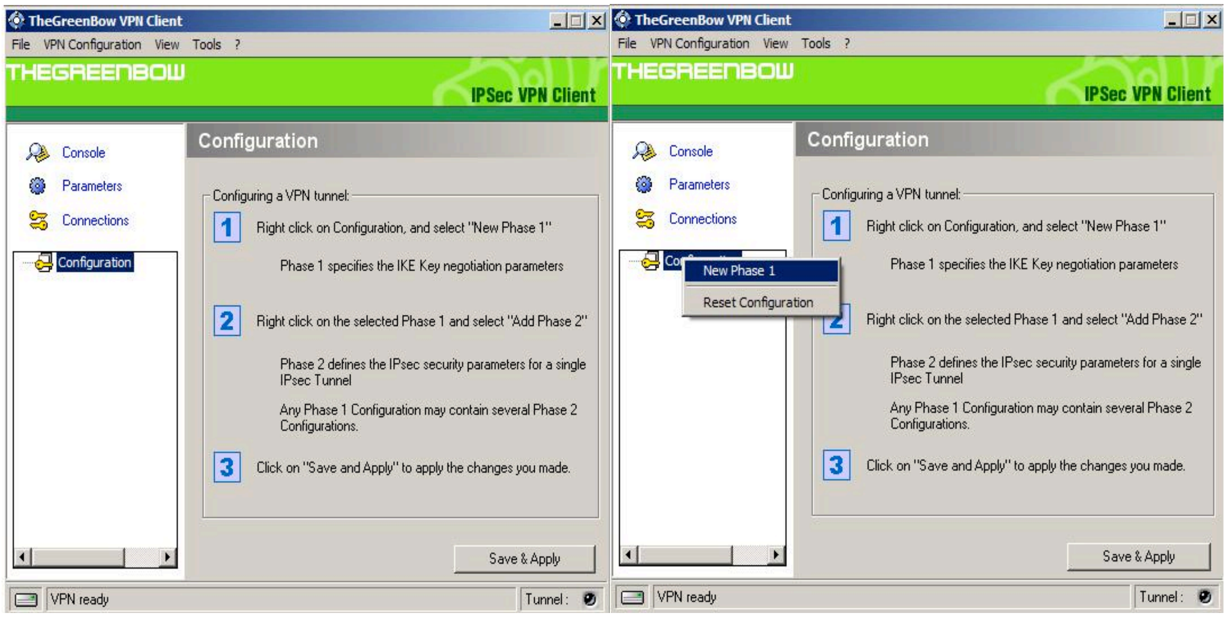
RED (WAN) Address:________________________
GREEN (LAN) Address:______________________
X509 Certificate:___________________________
Local Subnet: ______________________________
Remote Subnet: ____________________________

Once you have updated your Windows box, installed the required VPN client and collected the required information, you are ready to proceed.

1. From your Windows machine, start up the Green Bow VPN Client.

2. Next, with the Green Bow VPN Client started, right click on the configuration icon and left click on "New Phase".

Figure 8.19: Initial Screen Figure: New Phase 1



Configuration

Configuring a VPN tunnel:

1 Right click on Configuration, and select "New Phase 1"

Phase 1 specifies the IKE Key negotiation parameters

2 Right click on the selected Phase 1 and select "Add Phase 2"

Phase 2 defines the IPsec security parameters for a single IPsec Tunnel

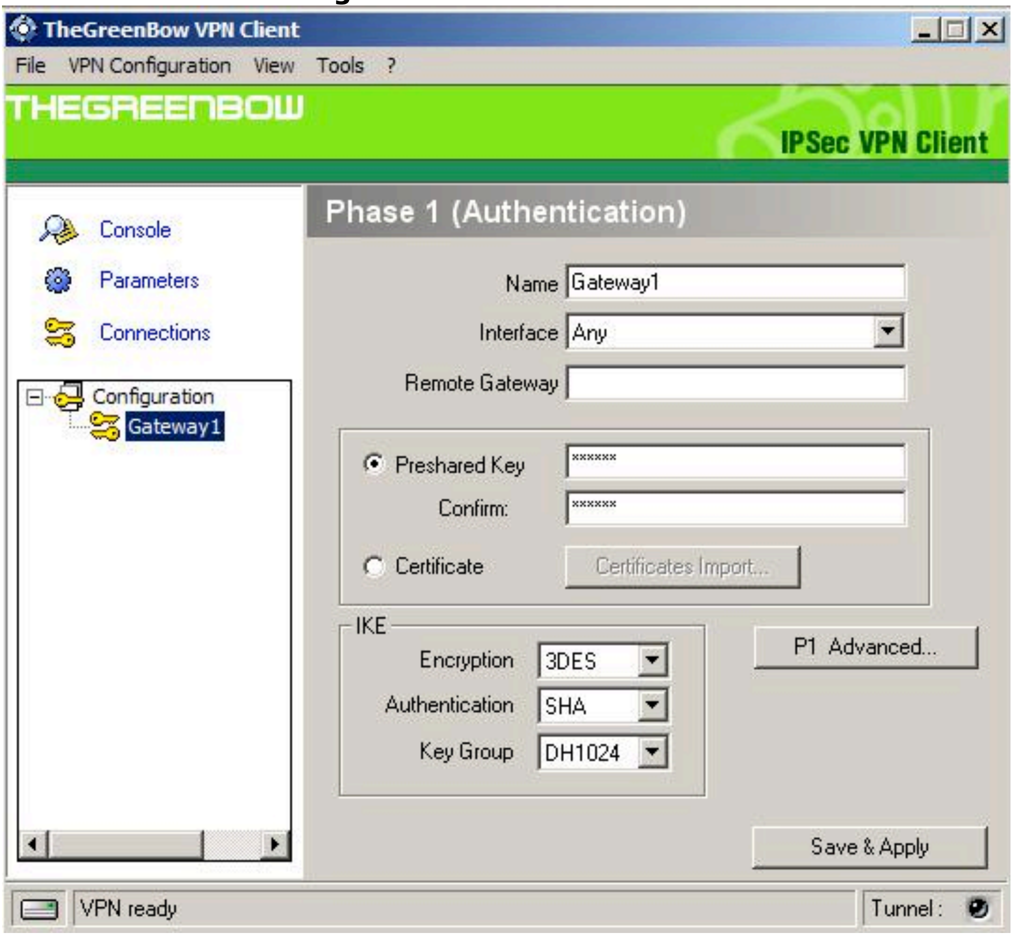
Any Phase 1 Configuration may contain several Phase 2 Configurations.

3 Click on "Save and Apply" to apply the changes you made.

1. Next you will need to fill out the empty boxes on the right of the screen. You will need to enter a name of the VPN in the name field. (Interface should have "Any" in the field.) Remote Gateway will be the external IP of the location that you are trying to connect to, and this will be your ISP IP Address.

2. You will next need to choose if you are using a Preshared Key or Certificate.

Figure 8.20: Initial Phase



Phase 1 (Authentication)

Name: Gateway1

Interface: Any

Remote Gateway:

● Preshared Key: ******

Confirm: ******

○ Certificate

IKE

Encryption: 3DES

Authentication: SHA

Key Group: DH1024

VPN ready

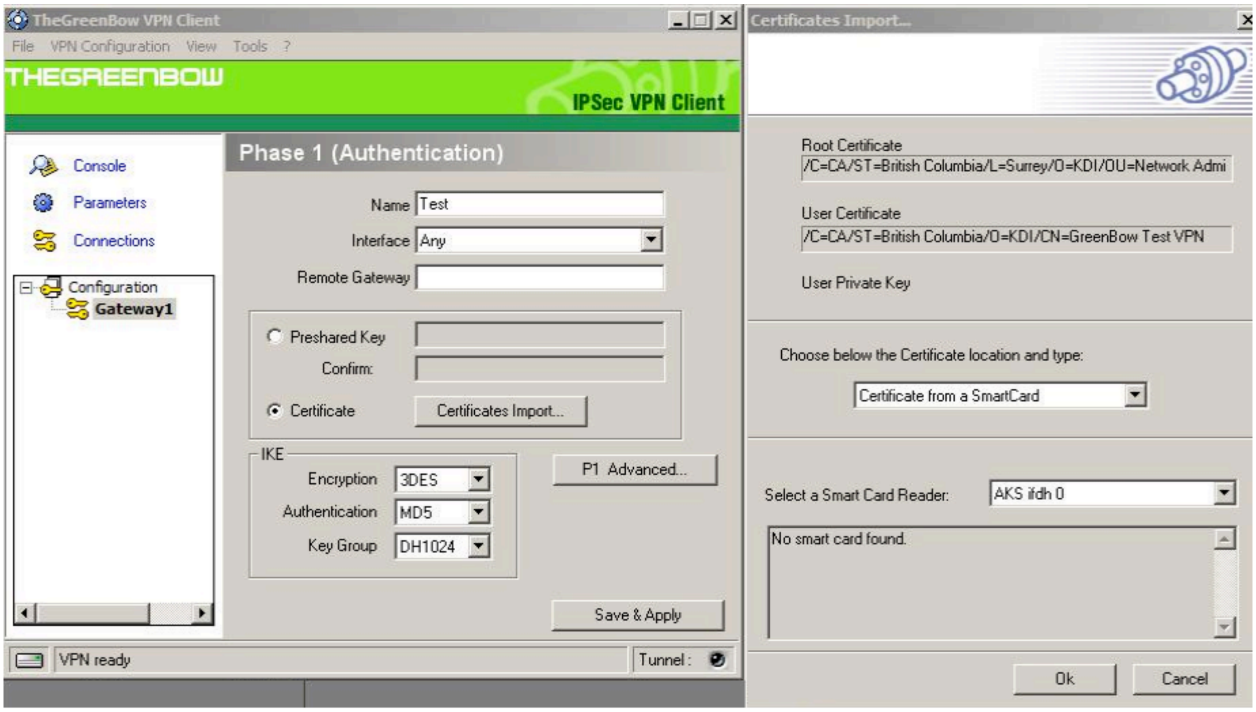
Tunnel :

1

3. If you choose a Preshared Key enter this into the two fields to confirm that the correct key has been entered.

4. If you choose `Certificate`, then click on the **Certificate Input** button. Another window will open and you must specify where you are importing the certificate from.

Figure 8.21: Changes and Certificate Import



Name: Test
Interface: Any
Remote Gateway:
○ Preshared Key
Confirm:
● Certificate
IKE
Encryption: 3DES
Authentication: MD5
Key Group: DH1024
VPN ready
Tunnel :

Root Certificate
/C=CA/ST=British Columbia/L=Surrey/O=KDI/OU=Network Admi
User Certificate
/C=CA/ST=British Columbia/O=KDI/CN=GreenBow Test VPN
User Private Key

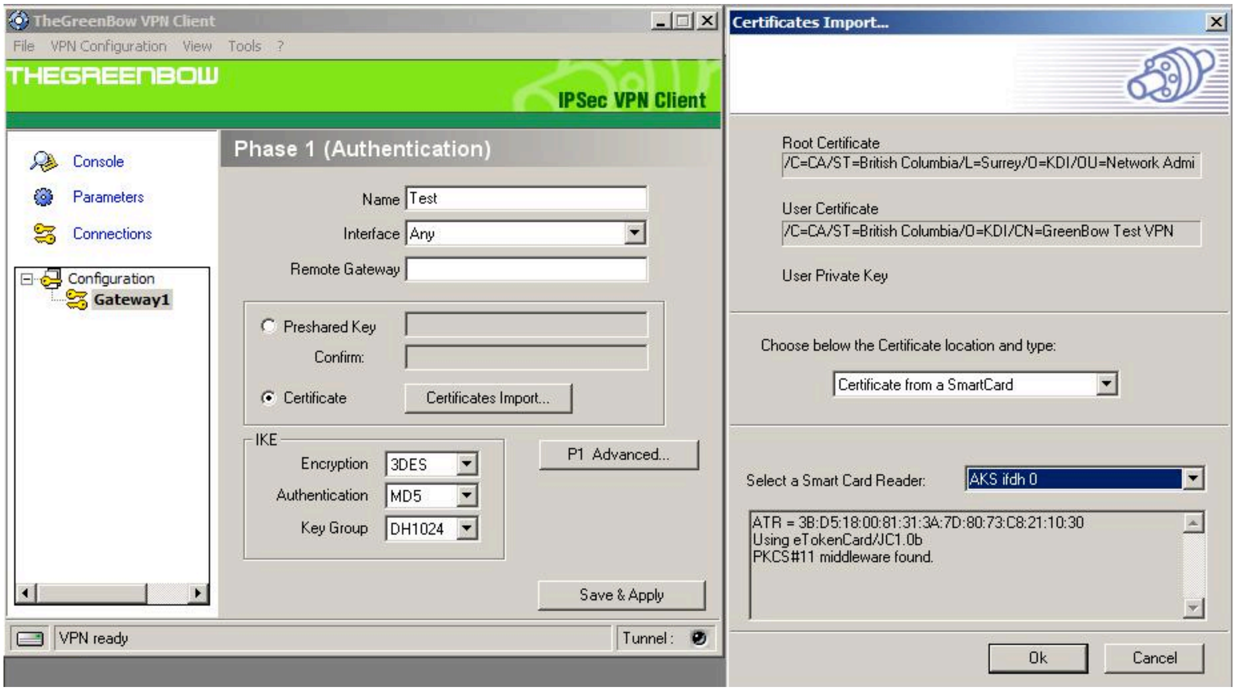
Choose below the Certificate location and type:
Certificate from a SmartCard

Select a Smart Card Reader: AKS ifdh 0

No smart card found.

5. Once the Certificate has been imported it will look like *Figure 8.22-Certificate Import* below.

Figure 8.22: Certificate Import



Name: Test

Interface: Any

Remote Gateway:

○ Preshared Key

Confirm:

● Certificate

IKE

Encryption: 3DES

Authentication: MD5

Key Group: DH1024

VPN ready

Tunnel :

Root Certificate
/C=CA/ST=British Columbia/L=Surrey/O=KDI/OU=Network Admi

User Certificate
/C=CA/ST=British Columbia/O=KDI/CN=GreenBow Test VPN

User Private Key

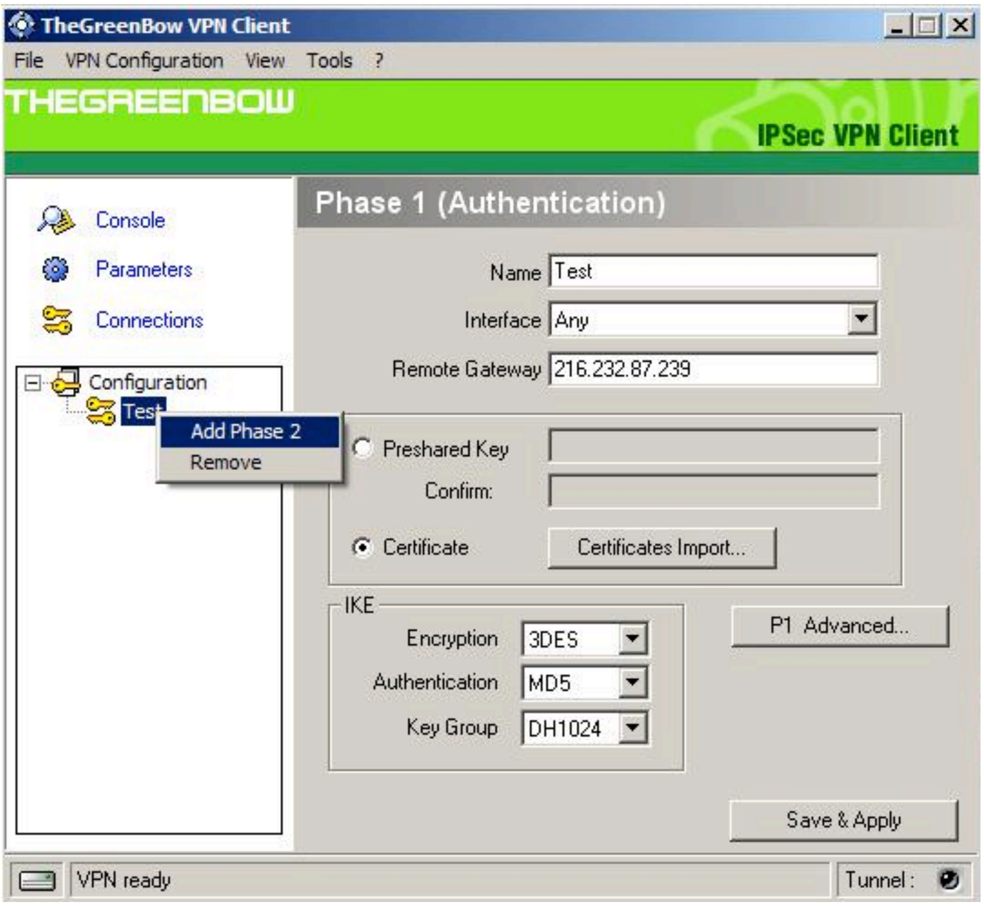
Choose below the Certificate location and type:
Certificate from a SmartCard

Select a Smart Card Reader: AKS ifdh 0

```
ATR = 3B:D5:18:00:81:31:3A:7D:80:73:C8:21:10:30
Using eTokenCard/JC1.0b
PKCS#11 middleware found.
```

6. Next, on the VPN connection you just made you must setup the IP Sec Configuration. Right click on the entry under the configuration icon and left click on **Add Phase 2.**

Figure 8.23: New Phase 2



Phase 1 (Authentication)

Name: Test

Interface: Any

Remote Gateway: 216.232.87.239

○ Preshared Key

Confirm:

● Certificate

IKE

Encryption: 3DES

Authentication: MD5

Key Group: DH1024

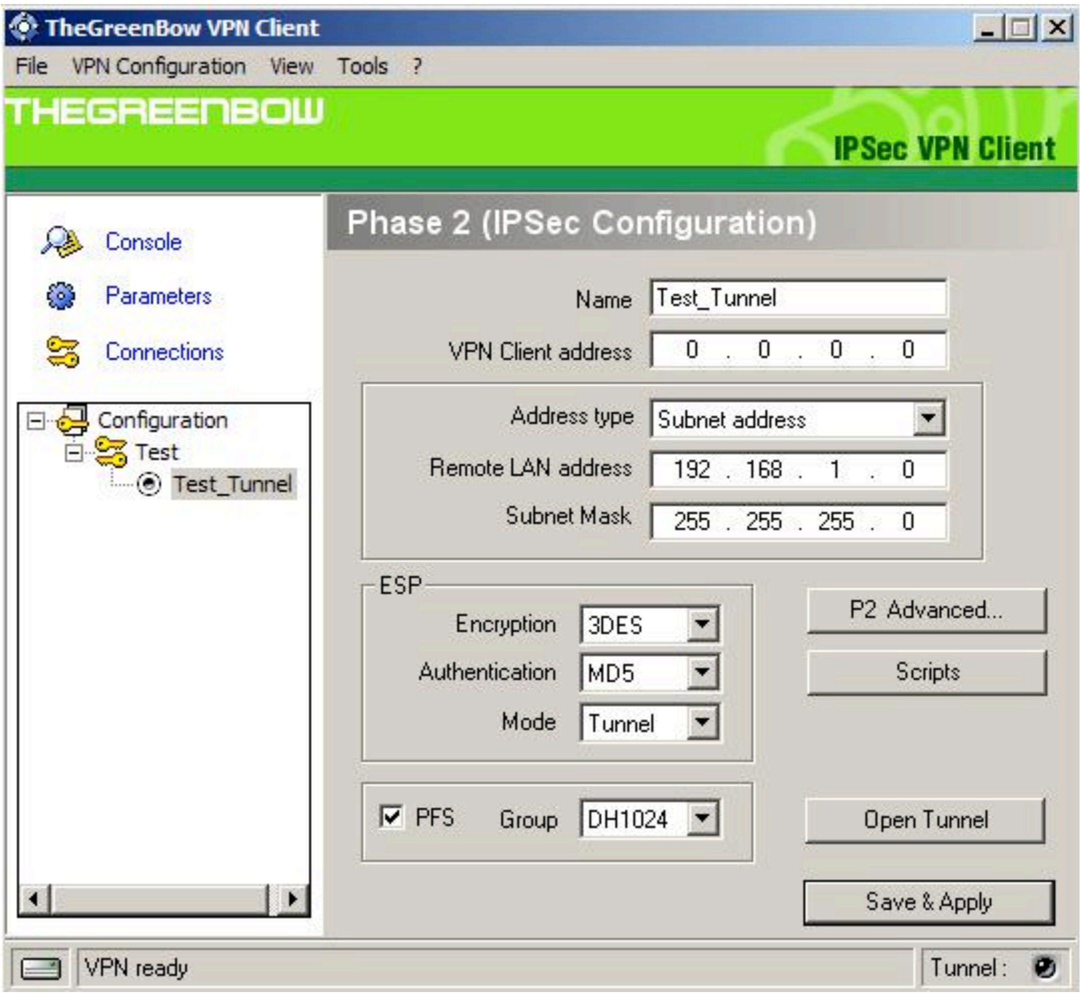
VPN ready

Tunnel :

7. For proper communication between the NetSentron and the Green Bow VPN Client, you will need to make certain that the ESP Authentication is set up at MD5 and that PFS is checked. Press save and then apply. Test out your Roadwarrior VPN.

NOTE
Make sure you do not test it within your local segment.

Figure 8.24: Initial Phase 2



Phase 2 (IPSec Configuration)

Name: Test_Tunnel

VPN Client address: 0 . 0 . 0 . 0

Address type: Subnet address

Remote LAN address: 192 . 168 . 1 . 0

Subnet Mask: 255 . 255 . 255 . 0

ESP

Encryption: 3DES

Authentication: MD5

Mode: Tunnel

☑ PFS Group: DH1024

VPN ready

Using x509 Certificates

x509 Certificates are the preferred way of connecting your Roadwarrior client to the NetSentron. This is for a couple of reasons, the main one being that each client can have their own certificate and you can revoke certificates privileges at any time. Whereas with Pre-Shared Keys, you would have to call up each of your clients and have them change their key.

Requirements

To connect to the NetSentron, we are going to use a VPN client created by The Green Bow. Please refer to *Roadwarrior Connections – Using Pre-Shared Secrets,* above.

You will need to write down the Red (WAN) IP Address of your NetSentron, the Green (LAN) address of your NetSentron, the x509 Certificate and the allowable range that you will allow your Roadwarrior client to connect to (this is accomplished through an ip/netmask combination such as 192.168.1.0/255.255.255.0, which would allow the VPN Client to connect to the entire 192.168.1.x subnet). You can find this information on the VPN page. To locate the VPN page go to *VPN Connection and Status Control, above,* in this manual. Use the table below to key in the required information.

Table 6: VPN – Windows 2000/XP IPSec Certificate Reference Table

RED (WAN) Address:______________________
GREEN (LAN) Address:_____________________
X509 Certificate:_________________________
Local Subnet: ____________________________
Remote Subnet: __________________________

Once you have updated your Windows box, installed the required VPN client and collected the required information, you are ready to proceed.

1. The first thing you will need to do is to need to get the certificate that you created for the VPN connection on the NetSentron over to your Windows PC. This can be done in a variety of ways, the easiest way is to start a browser and connect to the Web based interface of your NetSentron. Then go to the VPN section, find the VPN connection that you have previously configured and click on the blue disk icon. This should start the Save as Dialog in your browser. Save this certificate somewhere you can retrieve it from. The certificate should be saved in P12 format (i.e. it should have an extension of P12)

2. Now, you will copy the certificate over to your Windows PC. Do not forget where you saved it.

3. From your Windows machine, start up the Linsys VPN Client.

NOTE

If your machine is not up to date or properly patched, the VPN client may tell you this and ask you if you want to attempt to update your system. If you wish to let the VPN Client search for and install the patch, click the ***Yes*** button. If not, take note of the HotFix number, click the ***No*** button and then exit the VPN client. To find out more about hotfix go to http://www.microsoft.com/ and search for the patch; download it manually, and then install it.

4. With the Linsys VPN Client started the first step is to enter is a name for the VPN. This should be entered in the empty box to the right of the IPSec Profile Name.

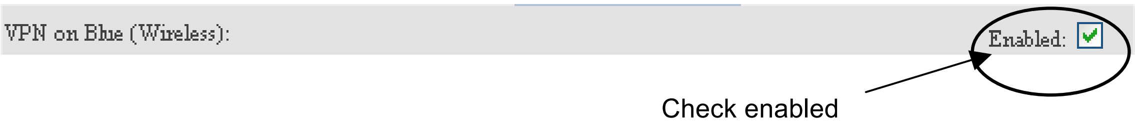
BLUE (Wireless) VPN - Using the Linsys VPN Client

This section explains how to setup your clients on the BLUE LAN giving them access to the Internet and as well as resources on the GREEN LAN using a VPN. From this point on it is assumed that you have read the Blue (Wireless) setup section of the manual and that the BLUE LAN is setup and running. It is also assumed from this point that you have read the section on Linsys VPN client and are familiar with its configuration as well as the configuration of a VPN on the NetSentron. (If you are not familiar please see the sectionw **for Roadwarrior connections.**

Windows 2000/XP Roadwarrior Connections with *built-in IPSEC*, above).

1. The first step is enabling the BLUE VPN on the NetSentron. Open up a browser and log into your NetSentron (GUI).
2. From your NetSentron GUI click on the VPN's button. The VPN page appears.
3. In the Global Settings panel, check the enabled box labeled VPN on BLUE (Wireless). *See Figure 8.25 below.*

Figure 8.25: VPN – Global Settings – Wireless Enabled



VPN on Blue (Wireless): Enabled: ☑

Check enabled

4. Click on the Save button to restart the VPN Server.

5. Next, you will need to create a Host-to-Net (Roadwarrior) VPN. In the Connection status and control panel, click the Add button. The `Connection Type` panel appears.

6. Select the radio button next to Host-to-Net Virtual Private Network (RoadWarrior) and click the Add button. The `Connection and Authentication` panels appear.

7. In the `Name` field, key in a name for the VPN connection you are creating.

> **NOTE**
>
> The name must start with a letter and not contain spaces or non-text characters.

8. For the Interface select *BLUE*.

9. In the `Local Subnet` field key in the following: ***0.0.0.0/0.0.0.0***

10. Leave the `Remote Host/IP` field blank unless you want to limit the VPN to a specific host.

11. In the remark field, key in something that will remind you what or who this VPN is for.

12. Select ***Clear*** from the drop down menu to the right of the `Dead Peer Detection` action field.

13. In the `Perfect Forward Secrecy` field, use the drop down menu to select **Yes.**

14. The next step is to choose between `Pre-Shared Key` and a `Certificate`. A Pre-shared key only allows for one key, which has to be shared by all clients. This is not a wise choice and the preferred method is to use a Certificate for each client. If you are unfamiliar with either choice see *Using Pre-Shared Secrets* and/or Using x509 Certificates on page 214.

15. Once all of your settings have been entered, click the Save button. Your new VPN connection is configured and waiting for a client to connect. You can view your new connection in Connection status and control panel.

Linsys VPN Client Configuration

Now you will need to configure the Linsys VPN client. Please refer to the section of the NetSentron manual that explains how to install and configure the Linsys VPN client as this section will only tell you what settings are required to get the VPN to connect.

Start the Linsys tool and then key in the following settings:

- In the Interfaces field, select the ***wireless adapter***.

- The entries in Local Side of the Tunnel should be automatically filled in.
- In the VPN Gateway (hostname / ip) field, key in the ***BLUE (Wireless) Network adapter address***
- In the Remote Internal IP field, key in the ***GREEN (LAN) Network adapter address***
- In the Private Address/Network Mask field, key in ***0.0.0.0 / 0.0.0.0***
- Under IPsec Options, select ***PreShared Key*** or ***Certificate***.
    - If `PreShared Key`, enter it in the text area
    - If `Certificate`, click on the magnifying glass next to the word certificate, then hit the plus button on the new dialog. Next browse to your certificate from the NetSentron and enter the password you set on the NetSentron. That should import the certificate. You should be returned to the Certificates dialog. Select **My Certificates** and you should see your newly imported certificate in the list. Double click on it and it will automatically configure the necessary parameters.

- Set the remaining fields on this panel as follows:
  3DES, MD5, PFS (checked), 3600 and 50000

Click on the `Other Options` tab to make sure `Debug` is ***enabled***. If not, enable it.

- Next, click on the `IPSec profiles` tab. Click on the **Save** icon to save your settings.
- Now that your settings have been entered and saved, right click on the Linsys Icon in the task bar. A selection box appears.
- Click on view log, this will bring up log view which will help with diagnosing problems.
- Finally, click on the Connect button. You should get a working connection to the GREEN LAN and all machines on the LAN should be accessible by their IP Addresses.

NOTE

Like any other IPSEC VPN, you will need a WINS server for Network

Neighbourhood to function properly. Otherwise all connections need to be done using the IP Address of the machines.

On some versions of Windows XP, you cannot ping machines on the other end of the VPN, even with the firewall down or ICMP bypass enabled. In this case you will need a hotfix. More information can be obtained here:

http://support.microsoft.com/?kbid=889527

NetSentron-to-Linksys VPN – Using BEFSX41 or Linksys BEFVP41

The NetSentron allows for a NetSentron-to-Linksys VPN connection using models BEFSX41 or BEFVP41. Both models are very similar and both work equally well with the NetSentron (The Linksys BEFSX41 has a Dynamic DNS client built in. This means that you can specify a hostname on the NetSentron for the Linksys. As of this writing, the Linksys BEFVP41 does not have a built in Dynamic DNS Client and therefore you need to use an IP Address on the NetSentron end to describe the Linksys). The setup for both models is identical. When referring to Linksys in this manual we will be referring to both models. Installation and set up of the Linksys products is covered in detail in their manual and is beyond the scope of this guide. Before configuring the NetSentron to Linksys VPN you must have the following completed:

- The Linksys product needs to be installed and setup

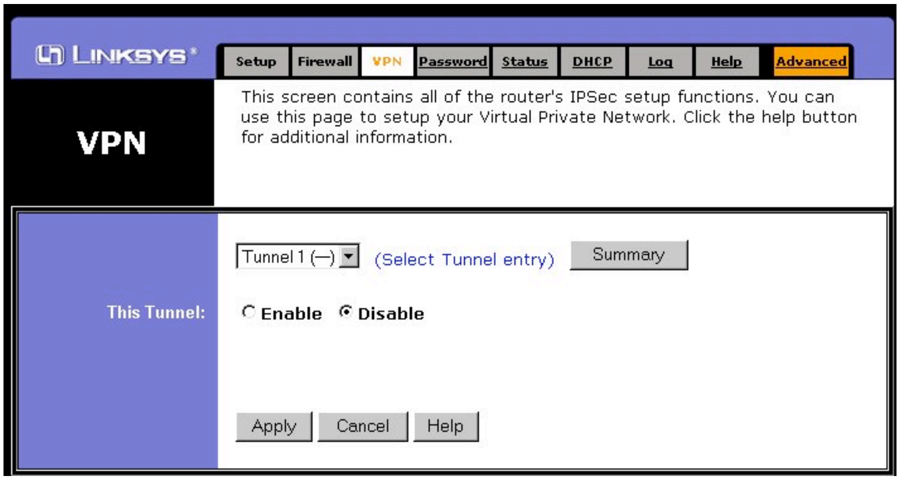
- You will need to set up a connection on your NetSentron for a Net-To-Net type connection. See the section on *Net-to-Net VPN - Using Pre-Shared* Secrets, above, and follow steps 1 thru 14.

Both Linksys products only support Pre-Shared Key connections. You will not be able to do x509 connections to the Linksys products

Once you have completed the above you are ready to configure the Linksys for a VPN connection to the NetSentron.

1. Log into the Linksys VPN Endpoint and go to the VPN page. *See Figure 8.26: VPN Page On The Linksys VPN Endpoint* on the next page.

Figure 8.26: VPN Page On The Linksys VPN Endpoint



This screen contains all of the router's IPSec setup functions. You can use this page to setup your Virtual Private Network. Click the help button for additional information.

Tunnel 1 (—) (Select Tunnel entry)

This Tunnel: ○ Enable ● Disable

Click the **Enable** radio button. A new page will appear full of VPN information fields. The following are descriptions of the fields found on this page.

Tunnel Name	Key in a descriptive name for the VPN tunnel. For example call it "Head Office"

Local Secure Group

This field describes the local network and which computers are allowed access the remote network.

You can select IP Addr, IP Range or Subnet. If you want all computers on your LAN to have access to the LAN behind the NetSentron choose Subnet. Key in the appropriate IP and Mask.

If you only want one machine to access the remote LAN, you should select IP Addr. If you wanted a range it would have been IP Range.

Remote Secure Group

This field describes the network at the NetSentron end of the tunnel, and it works just the same as the Local Secure Group. If you want complete access to the NetSentron, chose Subnet and enter the appropriate values.

Remote Security Gateway

This is where you would describe how to find the NetSentron. You may select IP Addr, FQDN (Fully Qualified Domain Name), or Any.

In a case where the NetSentron has a static IP Address you should select IP Addr.

If your NetSentron has a dynamic address, then enter the Dynamic DNS name that you have assigned to your NetSentron. *See Setting up a Dynamic DNS Name*.

Encryption

Select the 3DES radio button, **DO NOT** select DES. DES is an older and less secure form of encryption and should be avoided if possible.

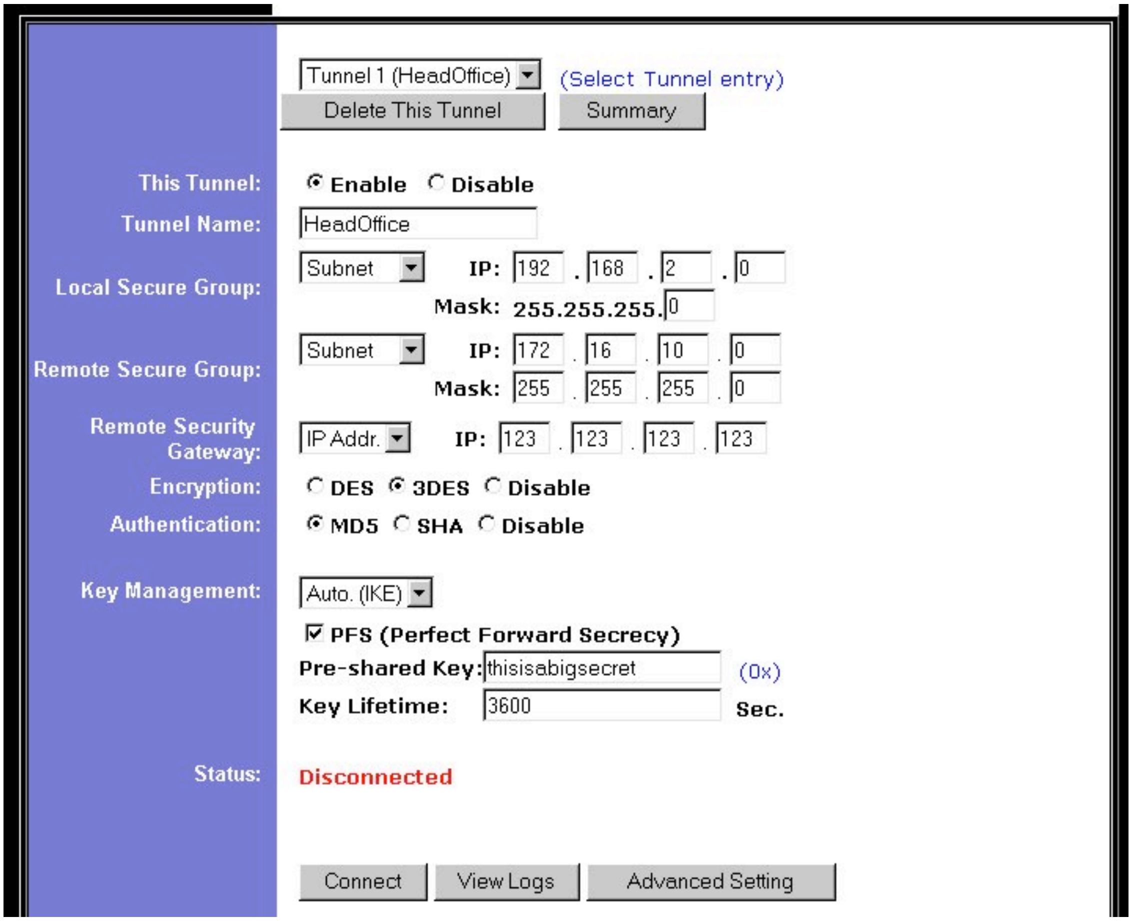
Authentication

Either MD5 or SHA can be selected, as both are acceptable. The NetSentron can use either.

Key Management	Select Auto(IKE) from the list, **DO NOT** select manual. ○ Click the PFS (Perfect Forward Secrecy) checkbox. ○ Key in the Pre-Shared Secret that you entered on the NetSentron. ○ Set the Key Lifetime to 3600 seconds (60 minutes)

2. Click the **Apply** button and your screen should tell you that it has successfully saved the settings. You will then return to the VPN screen. The settings you entered are shown. *See Figure*

Figure 8.27: Lynksys VPN Page With Settings



Tunnel 1 (HeadOffice) (Select Tunnel entry)

This Tunnel: ● Enable ○ Disable

Tunnel Name: HeadOffice

Local Secure Group: Subnet IP: 192 . 168 . 2 . 0 Mask: 255.255.255.0

Remote Secure Group: Subnet IP: 172 . 16 . 10 . 0 Mask: 255 . 255 . 255 . 0

Remote Security Gateway: IP Addr. IP: 123 . 123 . 123 . 123

Encryption: ○ DES ● 3DES ○ Disable

Authentication: ● MD5 ○ SHA ○ Disable

Key Management: Auto. (IKE)

☑ PFS (Perfect Forward Secrecy)

Pre-shared Key: thisisabigsecret (0x)

Key Lifetime: 3600 Sec.

Status: Disconnected

3. Now you need to adjust the advanced settings for everything to work properly. Click the **Advanced Setting** button at the bottom of

the page. This page allows you to control the Phase 1 and Phase 2 settings of the VPN Tunnel.

NOTE

On this page be sure to select Main Mode and NOT Aggressive Mode for Operation Mode.

Proposal 1 Settings

Within the Proposal 1 section, insure that the following are set like this:

Encryption	Select ***3DES.*** **DO NOT** select DES for reasons mentioned earlier.
Authentication	MD5 or SHA will work fine.
Group	Ensure that this is set to 1024-bit. **DO NOT** use 768-bit as that is an inferior group. (Note these numbers represent the Diffie-Hellman Group 1 and Group 2)
Key Lifetime	Set this to 3600 seconds (60 minutes), or to a larger value if you prefer; just make sure the key life on the NetSentron is set to match in the Advanced Settings.

Proposal 2 Settings

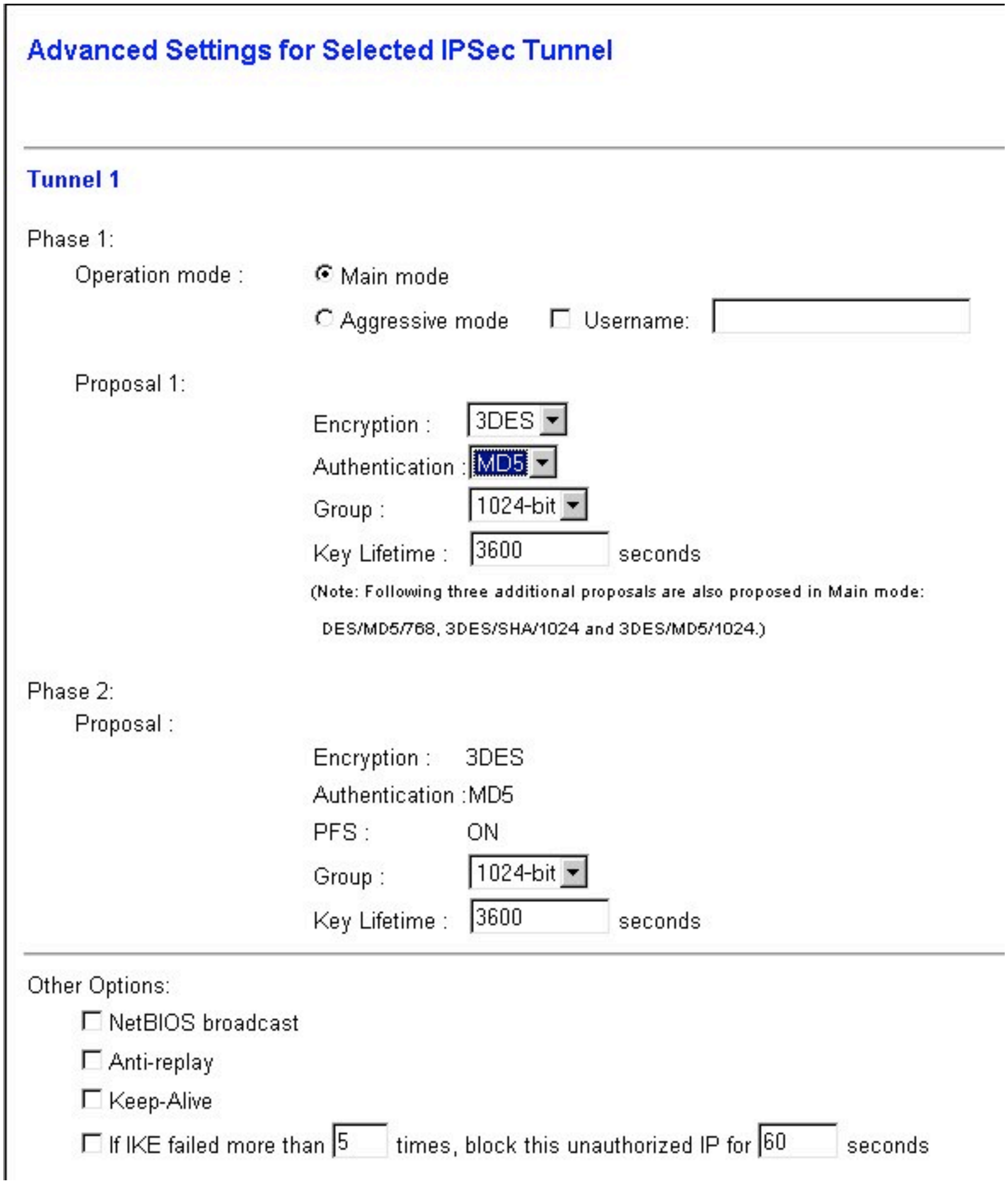
Within the Proposal 2 section, insure that the following are set like this:

Group	Ensure that this is set to 1024-bit. **DO NOT** use 768-bit as that is an inferior group. (Note these numbers represent the Diffie-Hellman Group 1 and Group 2)

Key Lifetime	Set this to 3600 seconds (60 minutes), or to a larger value if you prefer; just make sure the keylife on the NetSentron is set to match in the Advanced Settings.

4. Scroll down to the bottom and click **Apply**. Your screen should look like *Figure 8.28: Advanced Settings For Selected IPSec Tunnel on the next page.*

Figure 8.28: Advanced Settings For Selected IPSec Tunnel



Advanced Settings for Selected IPSec Tunnel

Tunnel 1

Phase 1:

Operation mode : ● Main mode
○ Aggressive mode □ Username:

Proposal 1:

Encryption : 3DES
Authentication : MD5
Group : 1024-bit
Key Lifetime : 3600 seconds

(Note: Following three additional proposals are also proposed in Main mode:
DES/MD5/768, 3DES/SHA/1024 and 3DES/MD5/1024.)

Phase 2:

Proposal :

Encryption : 3DES
Authentication :MD5
PFS : ON
Group : 1024-bit
Key Lifetime : 3600 seconds

Other Options:

□ NetBIOS broadcast
□ Anti-replay
□ Keep-Alive
□ If IKE failed more than 5 times, block this unauthorized IP for 60 seconds

5. You may now close this page and return to the Main VPN page.

6. Finally, click **Connect**. You should then see the screen refresh. Located on the Status line near the bottom of the page you should see the words `Connected` in RED.

How To Connect A Windows Machine Behind A NetSentron Using Windows VPN

Using the built in Windows VPN you can connect to your LAN at work or school with relative ease.

NOTE
The Windows built in VPN uses PPTP (point to point tunneling protocol) which is far less secure than the built in IPSEC VPN of the NetSentron – use at your own discretion.

To make this kind of VPN connection, we will need several things. On the LAN we are connecting to, a Windows 2000, XP or Vista machine that will be the VPN endpoint: a Windows 2000, XP or Vista machine on the client end. An internet connection that allows this type of VPN, many home and business services allow this kind of VPN, but many of the wireless services block this type of VPN, requiring an upgrade to allow the packets to flow.

Please mark down the IP Address of the machine on your LAN that is to be the VPN endpoint for the remote clients.

_______________________________ (VPN endpoint)

We will need to make some Port Forwarding rules to allow the VPN packets to go through the NetSentron. Log into your NetSentron and click on the Firewall menu.

- Select **GRE** from the Protocol drop down list.

- Enter the IP Address that you entered on the line above into the Destination IP. (VPN endpoint)

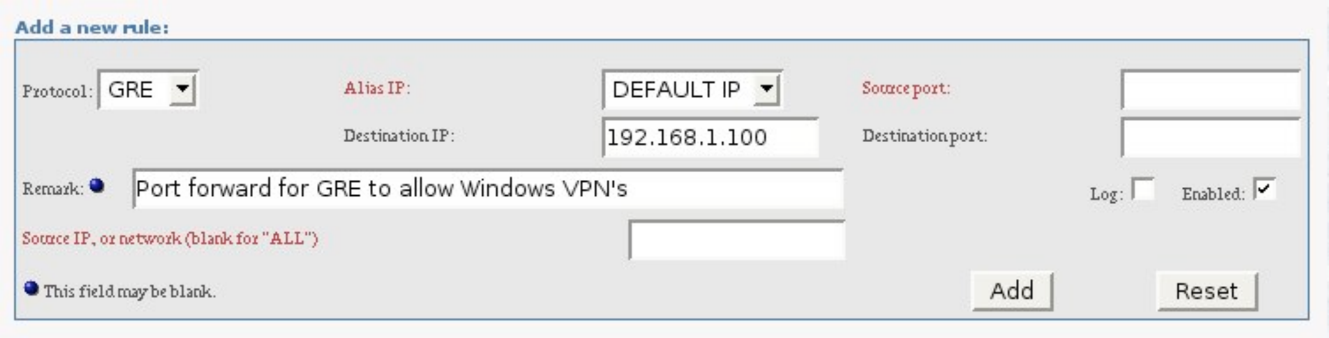
- Leave `Source and Destination Ports` empty.

- Add a remark describing what this port forward is for.

- Make sure `Enabled` is checked.

You should end up with an entry that looks like Figure 8.29 on the next page.

Figure 8.29:Port Forwarding Rule Entry



Add a new rule:

Protocol:	GRE	Alias IP:	DEFAULT IP	Source port:	
		Destination IP:	192.168.1.100	Destination port:	

Remark: ● Port forward for GRE to allow Windows VPN's

Log: □ Enabled: ☑

Source IP, or network (blank for "ALL")

● This field may be blank.

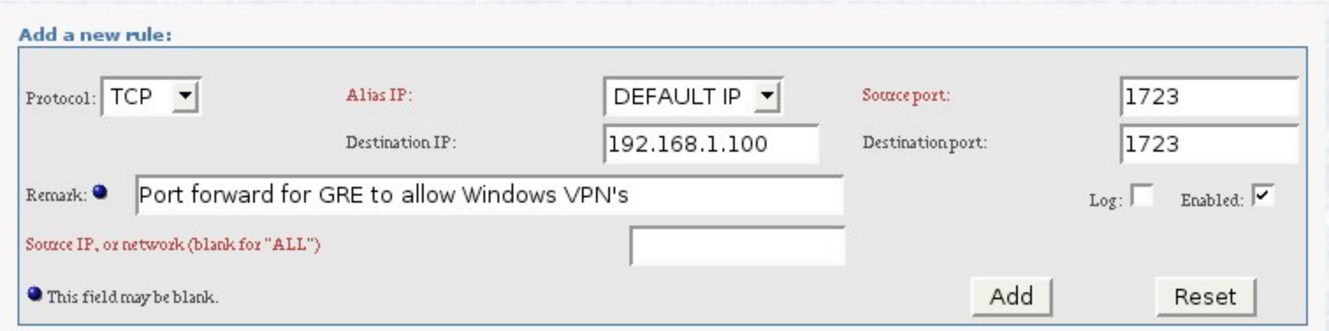
Click the **Add** button to complete this entry.

Now we need to add a port forward for port 1723, the port used by Windows VPN. To enter this information, choose the following:

- Select **TCP** from the Protocol drop down list.
- Enter the IP Address that you entered on the line above into the Destination IP. (VPN endpoint)
- Enter **1723** for `Source Port` and `Destination Port`
- Add a Remark describing what this port forward is for.
- Make sure Enabled is checked.

You should end up with an entry that looks like *Figure 8.30*

Figure 8.30: Port Forwarding Rule Entry-VPN Endpoint



Add a new rule:

Protocol:	TCP	Alias IP:	DEFAULT IP	Source port:	1723
		Destination IP:	192.168.1.100	Destination port:	1723
Remark: ●	Port forward for GRE to allow Windows VPN's			Log: □	Enabled: ☑
Source IP, or network (blank for "ALL")					

● This field may be blank.

Click **Add** to complete the entry.

NOTE

If you wish to increase security by restricting access to a specific IP Address or several IP Addresses, you can enter a Source IP when creating these entries. Please see the **Port Forwarding Section** of the manual for more details on restricting Port Forwards to specific addresses.

With the NetSentron configuration complete, we now need to focus on the Windows side of things. On the VPN endpoint (the machine on the LAN that you are trying to connect to), we need to add a new user that has restricted rights, we need to enable the machine to be a VPN endpoint, and allow the machine to connect to other machines on the LAN. We will do all that in the next section.

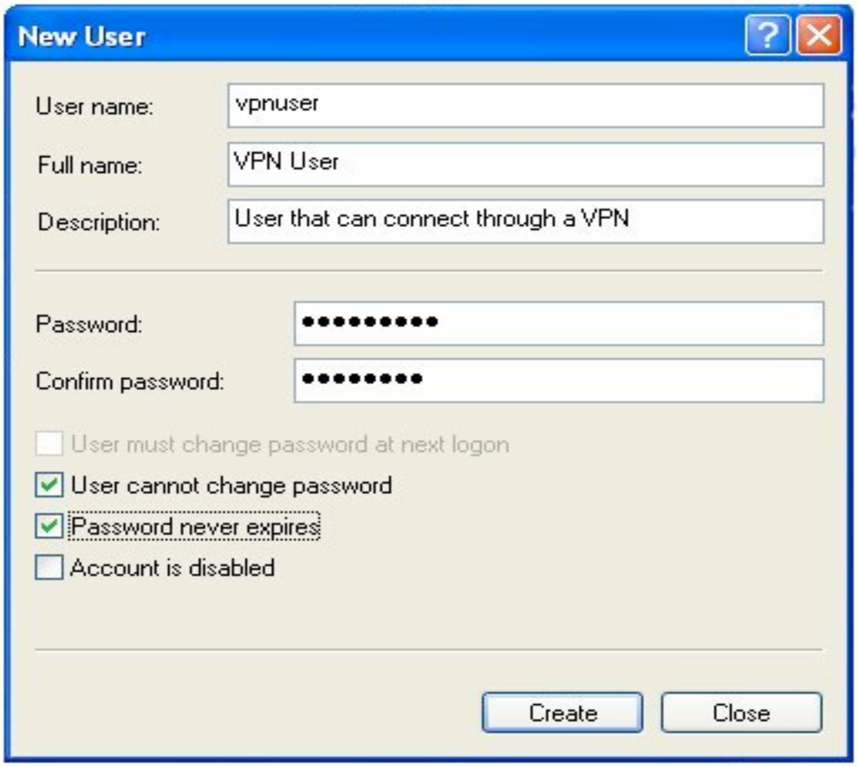
Configuring the VPN endpoint:

- Log into the Windows machine that will be the endpoint for the VPN.
- Go to Control Panel, click on `Administrative Tools`
- Click on `Computer Management`
- Find Local Users and Groups in the list, expand that entry
- Click on `Users` – you should see a list of users
- Right click and select `New User`
- Enter a User Name such as vpnuser or some other meaningful name
- Enter Full Name
- Enter a Description

- Enter a password
- Uncheck "User must change password at next logon"
- Check "Password never expires"
- Uncheck "Account is disabled"

You should end up with something that looks like *Figure 8.31* on the next page.

Figure 8.31: New User for VPN Endpoint



New User

User name: vpnuser

Full name: VPN User

Description: User that can connect through a VPN

Password: ●●●●●●●●●●

Confirm password: ●●●●●●●●●

□ User must change password at next logon

☑ User cannot change password

☑ Password never expires

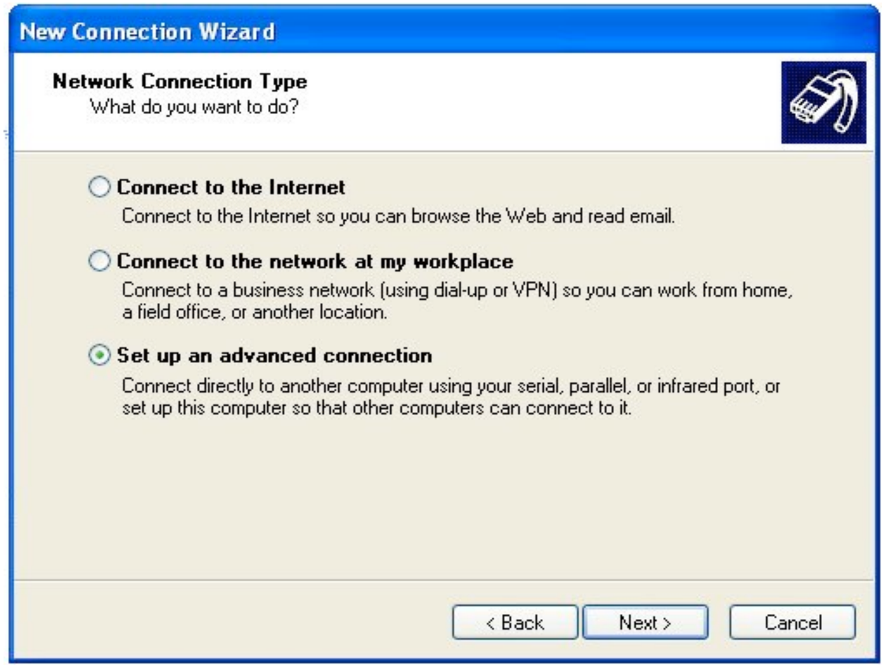
□ Account is disabled

Click **Create** to continue.

Next we want to create the actual connection. That is done from the Network Connections dialog.

- Click on Start Menu -> Control Panel -> Network Connections
- Click on `Create a new connection` from the right hand menu
- Click **Next**
- Choose `Set up an advanced connection`

You should end up with the display of a New Connection Wizard box shown in *Figure 8.32* on the next page.



New Connection Wizard

Network Connection Type
What do you want to do?

○ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

○ **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

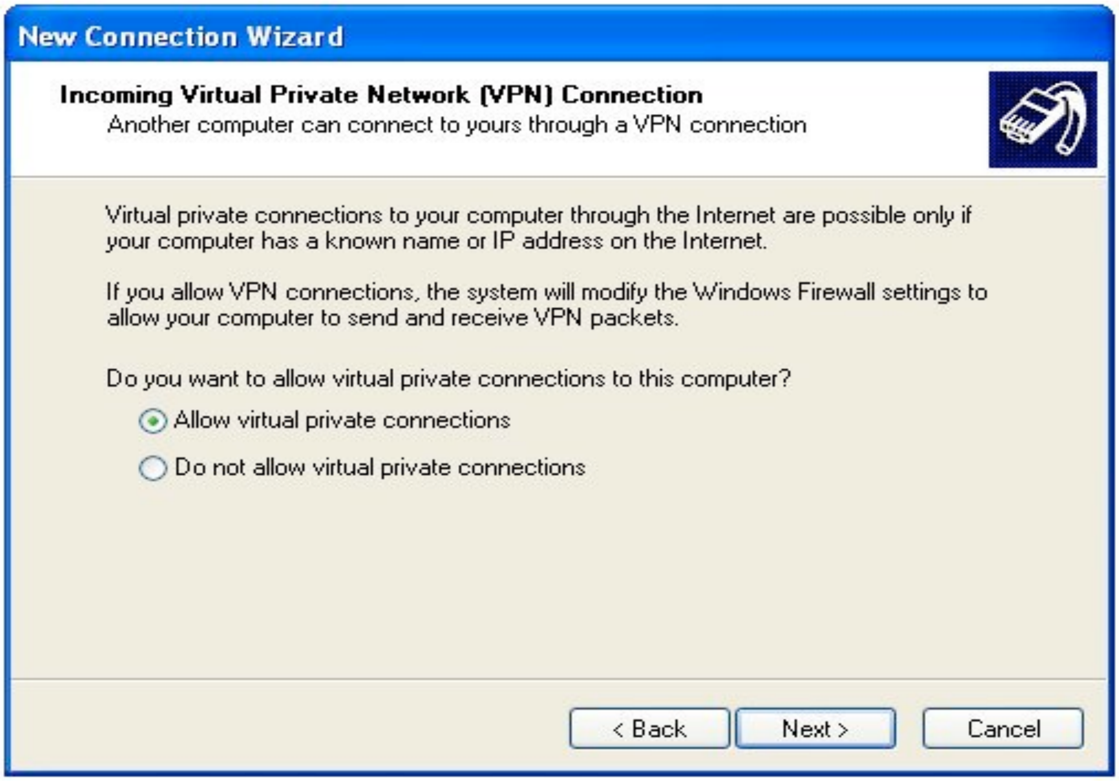
● **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

Figure 8.32: New Connection Wizard

- Click **Next**
- Choose "Accept incoming connections"
- Click **Next**
- **Do not** select anything for "Devices for Incoming Connections", just click **Next**
- Choose "Allow virtual private connections"

You should end up with a New Connection Wizard box showing Incoming VPN Connection as seen in *Figure 8.33* on the next page.

Figure 8.33: Incoming VPN Connection



New Connection Wizard

Incoming Virtual Private Network (VPN) Connection

Another computer can connect to yours through a VPN connection

Virtual private connections to your computer through the Internet are possible only if your computer has a known name or IP address on the Internet.

If you allow VPN connections, the system will modify the Windows Firewall settings to allow your computer to send and receive VPN packets.

Do you want to allow virtual private connections to this computer?

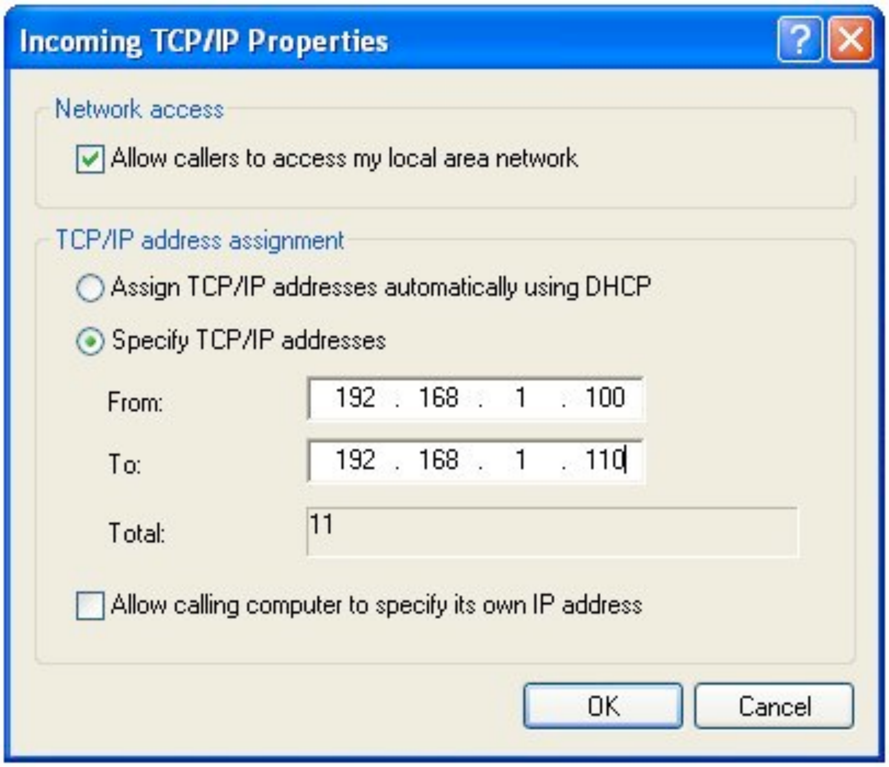
● Allow virtual private connections

○ Do not allow virtual private connections

- Click **Next**
- Select the user(s) you wish to be able to access this VPN remotely. In our instance, we would want to select vpnuser. One you select a user, click **Next.**
- On the next dialog, select **Internet Protocol (TCP/IP)** and click on **Properties**
- If you wish the remote machine to have access to the entire network, then click **Allow callers to access my local network**
- Under `TCP/IP address assignment`, you can select `Assign TCP/IP addresses automatically using DHCP` or you can specify an actual range. In our case I will specify an actual range.
- Make sure `Allow calling computer to specify its own IP address` is unchecked.

You should end up with a Incoming ICP/IP Properties display box as *Figure 8.34* shows on the next page.

Figure 8.34: Incoming ICP/IP Properties



Incoming TCP/IP Properties

Network access

☑ Allow callers to access my local area network

TCP/IP address assignment

○ Assign TCP/IP addresses automatically using DHCP

● Specify TCP/IP addresses

From: 192 . 168 . 1 . 100

To: 192 . 168 . 1 . 110

Total: 11

□ Allow calling computer to specify its own IP address

- Click **OK**
- Click **Next**
- Click **Finish**

You have now created the incoming connection for your VPN. Next we will need to configure the client to connect to this VPN Endpoint.

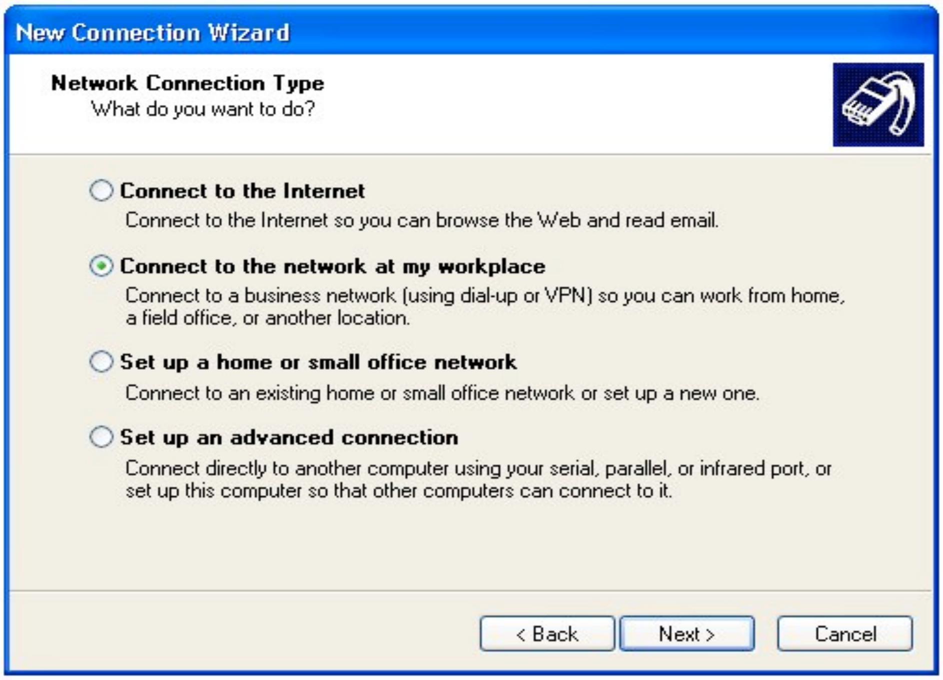
Connecting from the Windows client

Log into the client machine that will be connecting to the school or office VPN.

- Click on **Start Menu** -> **Control Panel** -> **Network Connections**
- Click on `Create a new connection` from the right hand menu
- Click **Next**
- Select `Connect to the network at my workplace`

You should end up with a New Connection Wizard box as *Figure 8.35* shows below.

Figure 8.35: Network Connection-Network at Workplace



New Connection Wizard

Network Connection Type
What do you want to do?

○ **Connect to the Internet**
Connect to the Internet so you can browse the Web and read email.

● **Connect to the network at my workplace**
Connect to a business network (using dial-up or VPN) so you can work from home, a field office, or another location.

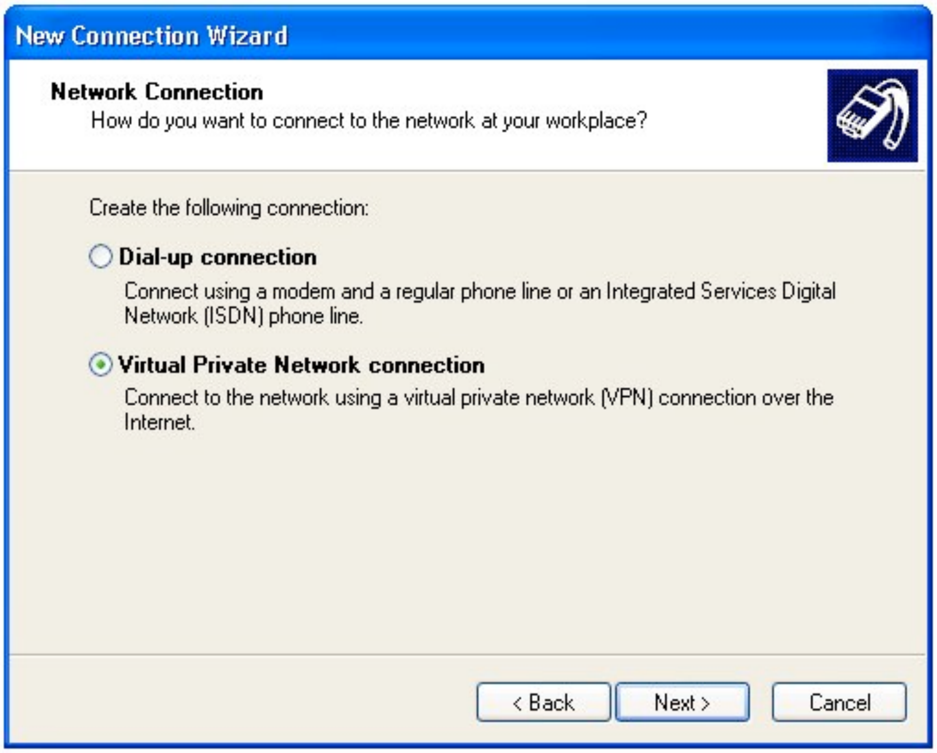
○ **Set up a home or small office network**
Connect to an existing home or small office network or set up a new one.

○ **Set up an advanced connection**
Connect directly to another computer using your serial, parallel, or infrared port, or set up this computer so that other computers can connect to it.

- Click **Next**
- Select `Virtual Private Network Connection`

You should end up with *Figure 8.36* as seen below.

Figure 8.36: Network Connection-Virtual Private Network Connection



New Connection Wizard

Network Connection

How do you want to connect to the network at your workplace?

Create the following connection:

○ **Dial-up connection**

Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

● **Virtual Private Network connection**

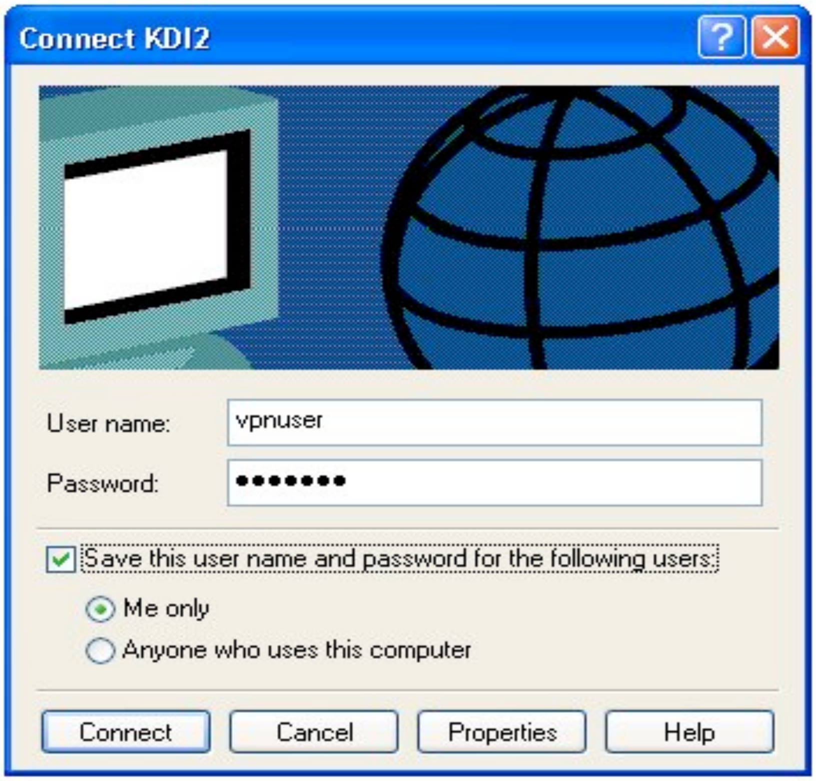
Connect to the network using a virtual private network (VPN) connection over the Internet.

- Click **Next**
- Enter a name for the connection, this can be anything descriptive.
- Click **Next**
- Select `Do not dial the initial connection`, unless you are on dial up
- Next enter the Host Name or IP address of the remote network, this will be the RED address of the NetSentron (or if you have set up a Host Name, the host name of the NetSentron)
- Click **Finish**
- Next a dialog will pop up asking for a User Name and Password as well as a connect button, etc.
- Enter the user you created on the remote machine and the password
- Click on `Save this user name and password for the following`

users

- Click **Connect**
  You should end up with *Figure 8.37* shown below.

Figure 8.37: Connection Window



Connect KDI2

User name: vpnuser

Password: ●●●●●●●

☑ Save this user name and password for the following users:

● Me only

○ Anyone who uses this computer

At this point you should be connected to the LAN at the remote site, unless you have an error.

You should be able to access all of the resources on the company or school LAN that you are connecting to. As there is no WINS server or DNS, you may need to access resources by IP address.

Chapter 9 OpenVPN

OpenVPN is an SSL VPN that allows you to connect to your network from remote locations. It has clients for Windows and Mac, as well as other platforms such as Linux, Android and iPhone. On the NetSentron, we support Windows 32/64 bit and Mac clients (OSX 10.4 through 10.7).

The OpenVPN security model is based on SSL, the industry standard for secure communications via the internet. OpenVPN implements OSI layer 2 or 3 secure network extension using the SSL/TLS protocol, supports flexible client authentication methods based on certificates. OpenVPN is not a web application proxy and does not operate through a web browser.

OpenVPN is designed with simplicity in mind, it is easy to configure and deploy on client machines. No complex left and right settings like IPSec VPN's. No expensive clients to purchase, OpenVPN has a free client for most platforms.

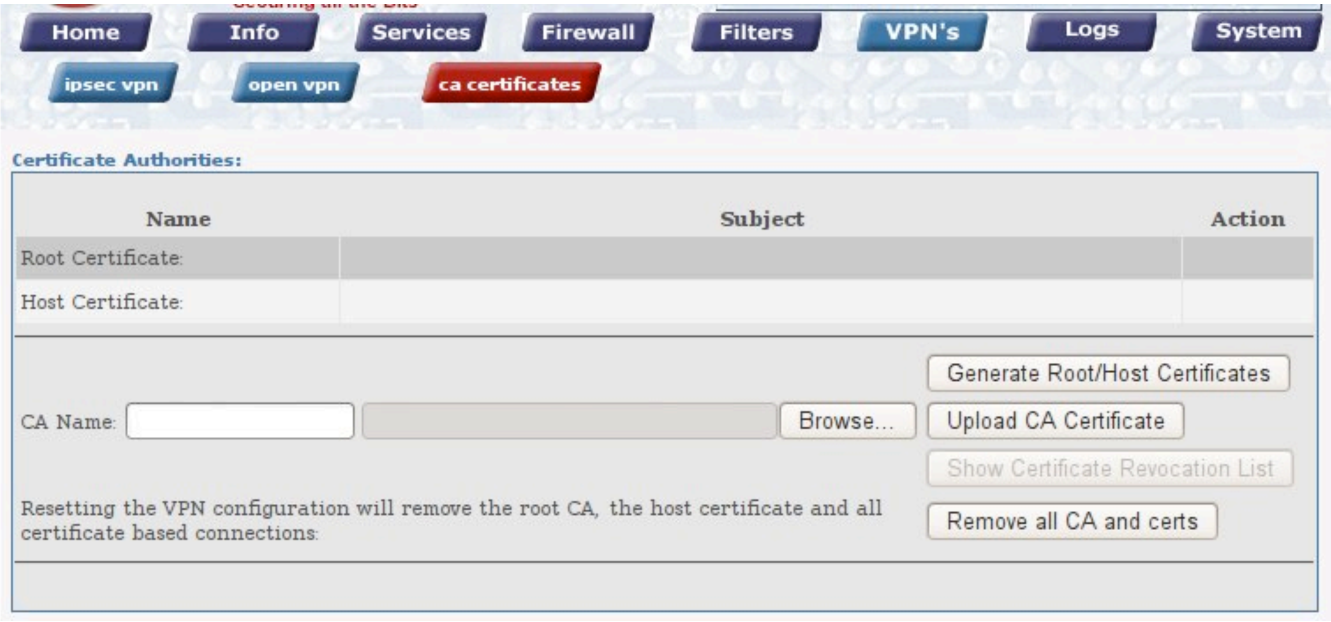
OpenVPN Requirements

In order to use OpenVPN on the NetSentron, you must have created a Root/Host Certificate on the ca certificates page.

Generating the Root/Host Certificate

This is simple to do, in the NetSentron GUI: go to VPN's and the click on `ca certificates`. If you have not previously created the Root/Host Certificate for your NetSentron, this page will be blank, as shown in *Figure 9.1* on the next page.

Figure 9.1: Root/Host Certificate Display



Certificate Authorities:

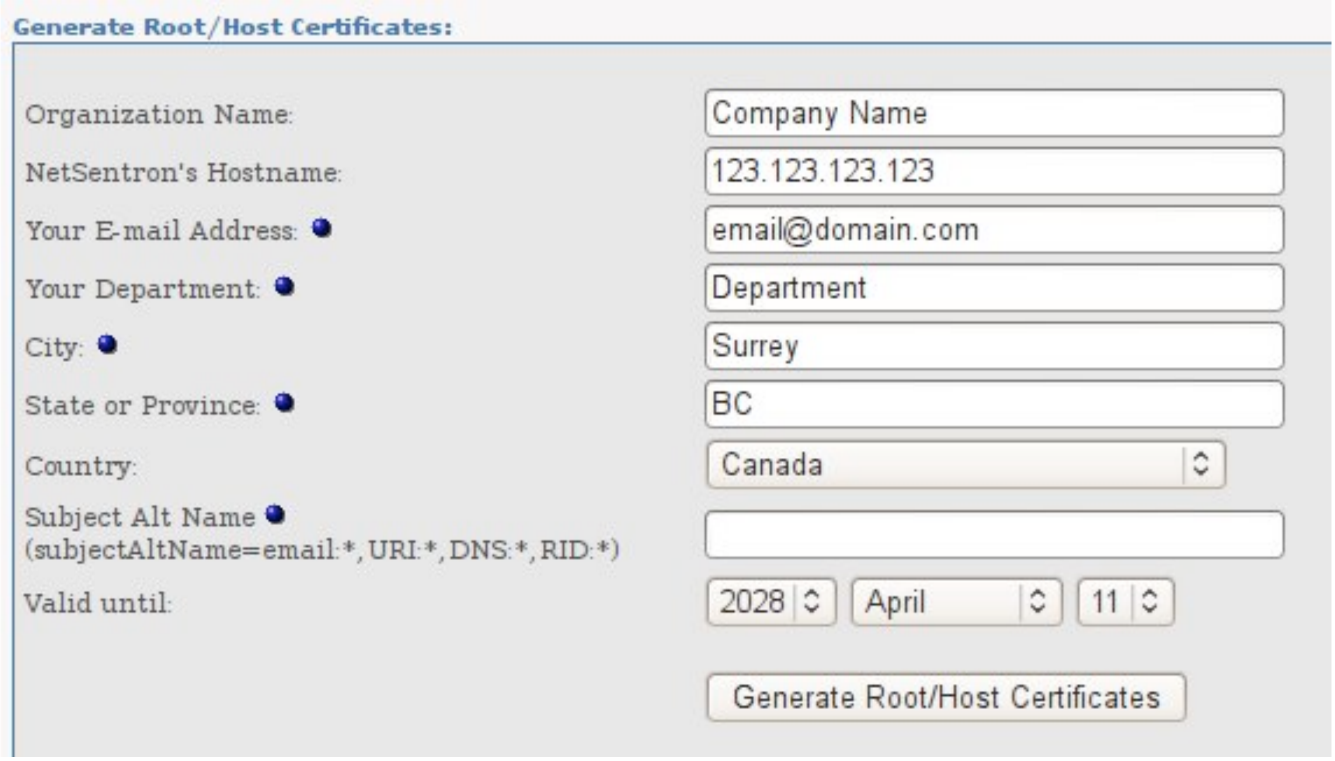
Name	Subject	Action
Root Certificate:		
Host Certificate:		

CA Name:

Resetting the VPN configuration will remove the root CA, the host certificate and all certificate based connections:

Click on the `Generate Root/Host Certificates` and fill in the information on the form that appears. It should look as *Figure 9.2* shows below.

Figure 9.2:Generate Root/Host Certificate Display



Generate Root/Host Certificates:

Organization Name:	Company Name
NetSentron's Hostname:	123.123.123.123
Your E-mail Address: ●	email@domain.com
Your Department: ●	Department
City: ●	Surrey
State or Province: ●	BC
Country:	Canada
Subject Alt Name ● (subjectAltName=email:*,URI:*,DNS:*,RID:*)	
Valid until:	2028 April 11

Anything with a blue dot is optional to fill in. Filling in all fields makes the certificate unique, however.

The following is an explanation of each field:

Organization Name: put the name of your company in here

NetSentron's Hostname: this should automatically be filled with the IP address of your

NetSentron or the Hostname of your NetSentron. If not, then enter the RED IP address in here. This must be an IP address or fully qualified domain name.

Your E-mail Address (optional): put an email address associated with your company in here. This is optional.

Your Department (optional): You can put your detpartment here or leave blank.

City (optional): Enter your city here or leave blank

State or Province: (optional) Put your state or province in this box or leave blank.

Country: Select your country from the list.

Subject Alt Name (optional): The subject alternative name extension allows additional identities to be bound to the subject of the certificate. Defined options include an Internet electronic mail address, a DNS name, an IP address, and a uniform resource identifier (URI).

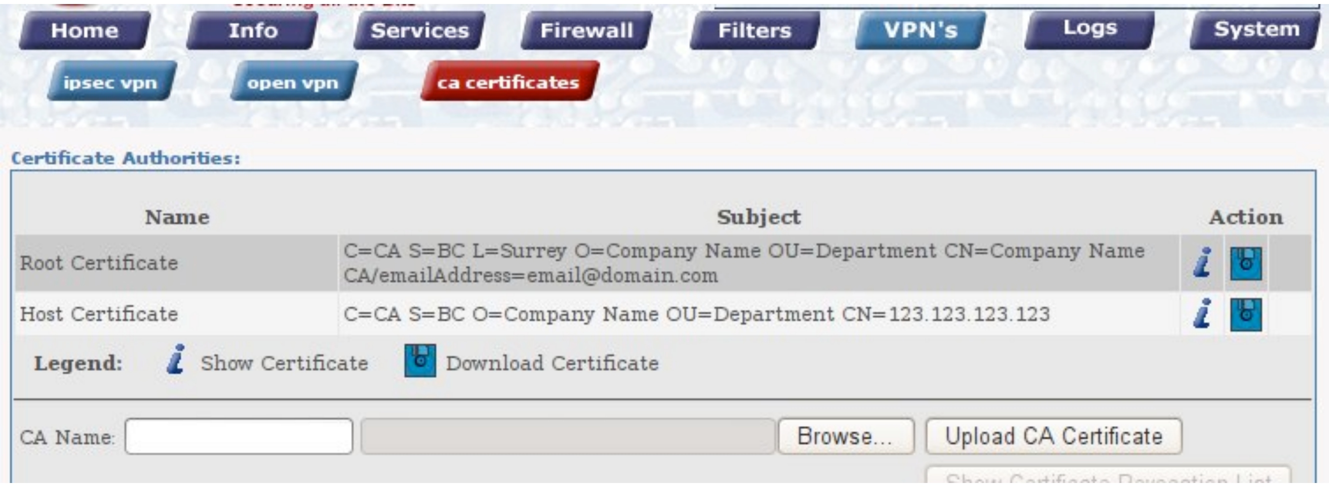
The SubjectAltName extension is defined in RFC 3280, section 4.2.1.7.

Valid until: Select when you want the certificate to expire. Longer is better for this one, as you don't want to have to regenerate all of your VPN certificates when this expires.

Once you have filled in the information, click on the `Generate Root/Host Certificates`.

You should end up with a screen looking like Figure 9.3 seen below.

Figure 9.3: Root/ Host Certificates



Certificate Authorities:

Name	Subject	Action
Root Certificate	C=CA S=BC L=Surrey O=Company Name OU=Department CN=Company Name CA/emailAddress=email@domain.com	i 💾
Host Certificate	C=CA S=BC O=Company Name OU=Department CN=123.123.123.123	i 💾

Legend: i Show Certificate 💾 Download Certificate

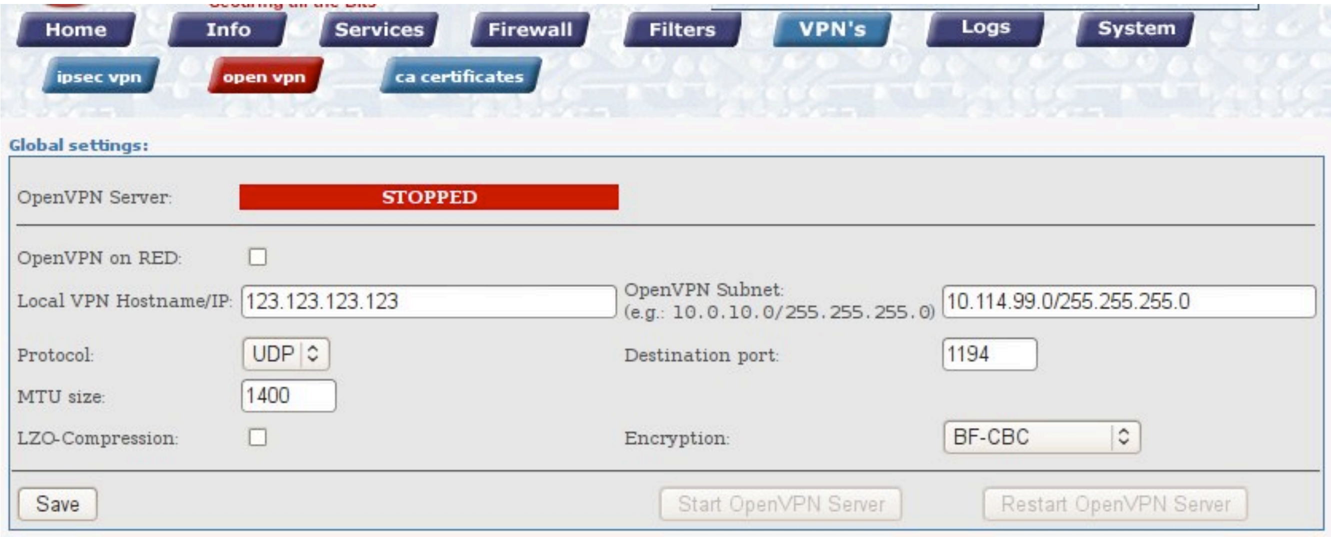
CA Name:

You have now completed the generation of the Root/Host Certificates and are ready to configure the OpenVPN.

Configuring OpenVPN

Click on the open vpn button in the menu buttons across the top of the page, you will see a page that looks like *Figure 9.4* as seen below.

Figure 9.4: Open VPN Display



Global settings:

OpenVPN Server:	STOPPED		
OpenVPN on RED:	□		
Local VPN Hostname/IP:	123.123.123.123	OpenVPN Subnet: (e.g.: 10.0.10.0/255.255.255.0)	10.114.99.0/255.255.255.0
Protocol:	UDP	Destination port:	1194
MTU size:	1400		
LZO-Compression:	□	Encryption:	BF-CBC

The first thing we want to do is check the box next to `OpenVPN` on RED and click `Save`. At that point, the Start and Restart buttons will be enabled. There is nothing other than the checkbox that you will need to adjust on this page, but if you wish to, you can make changes.

The following is an explanation of each field:

Local VPN Hostname/IP: This is the RED (public) IP Address of the NetSentron or the fully qualified domain name. It is how machines on the outside will find the NetSentron.

NOTE

If your RED address is dynamic, then you put your dynamic DNS domain name in here.

OpenVPN Subnet: This is the virtual subnet that OpenVPN will create on both sides of the VPN. Make sure that this ip address range does not conflict with any ranges on NetSentron on GREEN, BLUE or ORANGE Also, none of the clients can be from this range as well.

Protocol: OpenVPN works best when running on UDP for a protocol, but if for some reason, you cannot use UDP, you can change to TCP. However, performance of the VPN will be severely affected when running on TCP.

Destination Port: This is the port that OpenVPN uses to allow remote computers to connect to the NetSentron. You can change it to any port, as long as it is not used for something else. 1194 is the official IANA port number assignment for OpenVPN.

MTU size: The MTU (Maximum Transmission Units) is the maximum datagram size in bytes that can be sent unfragmented over a particular network path.

LZO Compression: This enables the NetSentron to compress the packets, but, this comes at a price, more processor power is required to do this. This is best left unchecked.

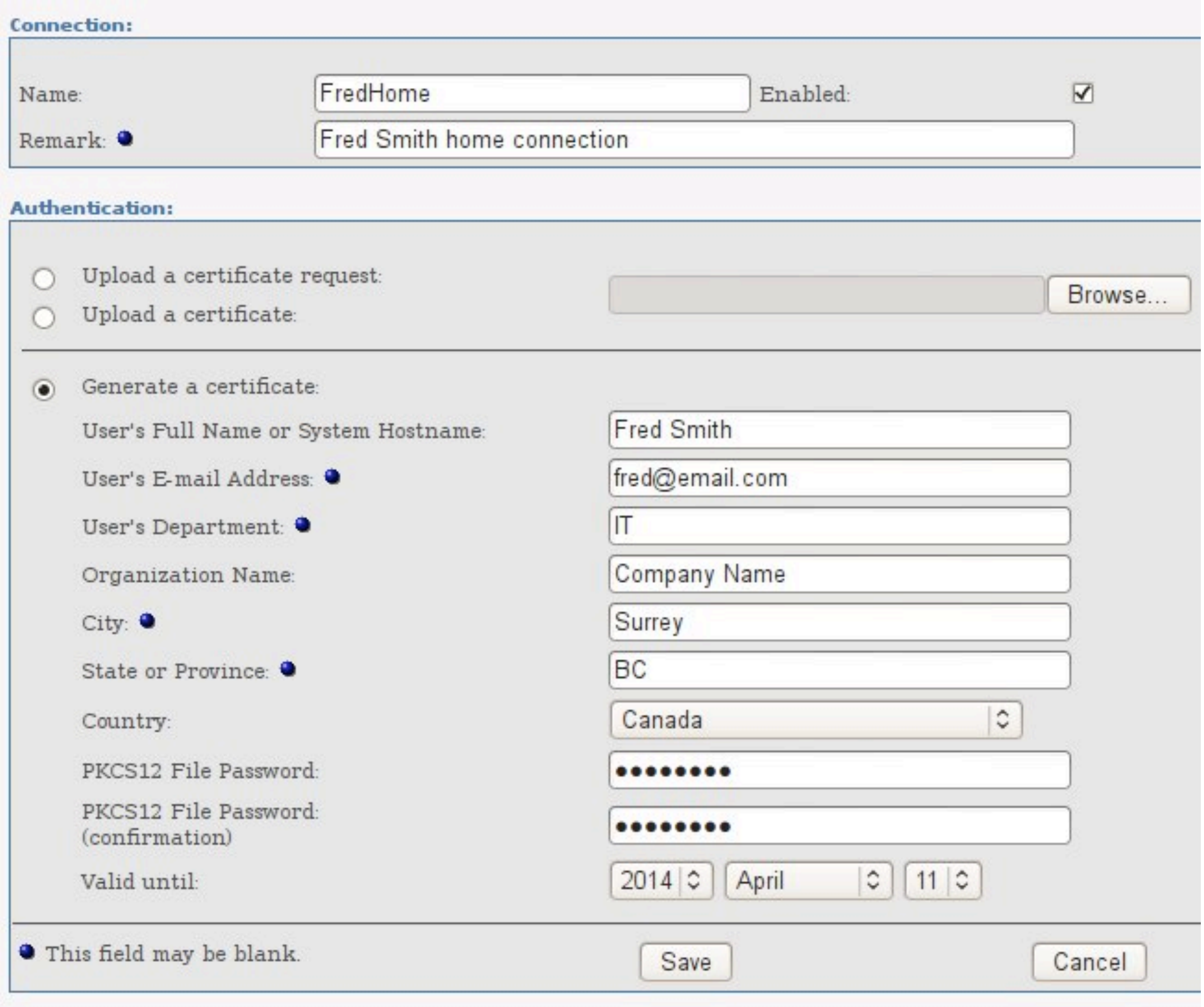
Encryption: OpenVPN can use many different types of algorithms to encrypt packets. The default BF-CBC will be adequate for most installations, it is fast and very secure.

Creating Connections

Next you will want to create a connection for each client that you would like to connect to your LAN. In the Connection status and control area, click on the Add button.

You will end up on a screen that looks like *Figure 9.5* on the next page.

Figure 9.5: Connection Display



Connection:

Name:	FredHome	Enabled:	☑
Remark: ●	Fred Smith home connection		

Authentication:

○ Upload a certificate request:

○ Upload a certificate:

● Generate a certificate:

User's Full Name or System Hostname:	Fred Smith
User's E-mail Address: ●	fred@email.com
User's Department: ●	IT
Organization Name:	Company Name
City: ●	Surrey
State or Province: ●	BC
Country:	Canada
PKCS12 File Password:	••••••••
PKCS12 File Password: (confirmation)	••••••••
Valid until:	2014 April 11

● This field may be blank.

You will need to fill in the fields that are not marked with a blue dot, which are optional. Like the Root/Host Certificate, the more you fill in, however, the more unique the certificate will be.

The following is an explanation of each field:

Name: This is the name for the connection so you can remember it. Generally, a good idea is to put the end users name and location such as FredHome.

NOTE
The name cannot have any spaces in it, it can only contain letters and numbers

Remark (optional): This field is for describing the connection and is optional.

User's Full Name or System Hostname: Here you can enter the full name of the remote user or their system hostname.

User's Email Address (optional): The remote users email address.

User's Department (optional): The department the remote user works in.

Organization Name: Your company name goes here.

City (optional): Enter the city

State or Province (optional): Enter the State or Province

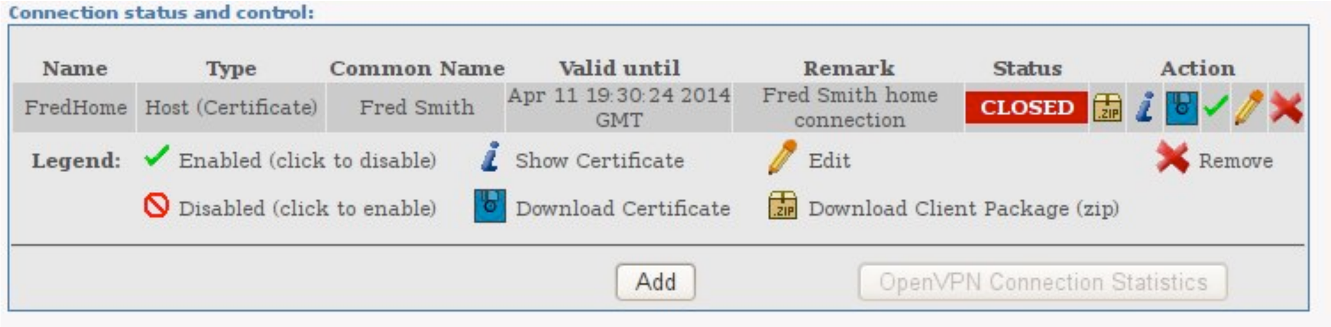
Country: Select your country from the list

PKCS12 File Password: This adds a password to the certificate for the tunnel. It is required and when the client tries to connect via the VPN, they will be required to enter the password. Make sure you write down the password. If a password is forgotten, a new connection will have to be made and the old one deleted.

Valid until: This defaults to 2028, but I would recommend selecting a year from now. You do not want certificates to last longer than that for security reasons. Don't forget, anyone who has the certificate and the password will have full access to your network. You can delete a connection at any time, which renders the certificate useless.

Click on `Save` when you have entered the required information. You will now have an entry in the Connection status and control section that looks like *Figure 9.6* shown below.

Figure 9.6:Connection Status and Control Display



Connection status and control:

Name	Type	Common Name	Valid until	Remark	Status	Action
FredHome	Host (Certificate)	Fred Smith	Apr 11 19:30:24 2014 GMT	Fred Smith home connection	CLOSED	ZIP i ⬇ ✓ ✎ ✗

Legend: ✓ Enabled (click to disable) i Show Certificate ✎ Edit ✗ Remove

⃠ Disabled (click to enable) ⬇ Download Certificate ZIP Download Client Package (zip)

The next step is to download the certificate and configuration for the tunnel. Click on the little ZIP icon in the line for the connection you created. This will allow you to save a file to your hard drive. It should have a title of *ConnectionName-To-NetSentron.zip* where *ConnectionName* is the name you gave the VPN connection.

This zip file will be copied to the remote machine, the one that is running the OpenVPN client. We will cover VPN clients in the next section.

If you need to make connections for other users, then repeat the steps above.

Starting and Stopping OpenVPN

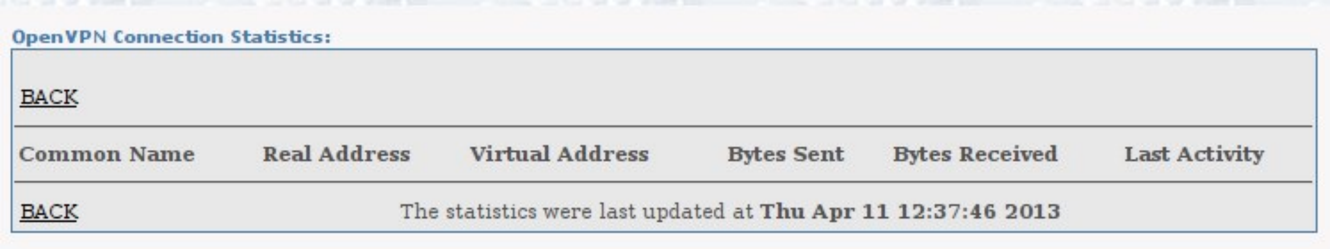
When you are ready to have clients connect, click on the `Start OpenVPN Server` button and the top of the page should show OpenVPN Server: RUNNING with RUNNING highlighted in green. If it is still RED and showing STOPPED, then there is a configuration error. Go through the steps again to make sure you didn't make a typo.

Once the OpenVPN server is running, remote clients may now connect to your LAN.

You might also notice now, that in the Connection status and control area of the page (where all the connections are listed), the OpenVPN Connection Statistics is now enabled. You can click on that button to view active connections and how much data was sent back and forth.

The screen looks like this *Figure 9.7* as seen below.

Figure 9.7: Open VPN Connection Statistics Display



OpenVPN Connection Statistics:

BACK

Common Name	Real Address	Virtual Address	Bytes Sent	Bytes Received	Last Activity

BACK The statistics were last updated at **Thu Apr 11 12:37:46 2013**

To turn off, or disable, OpenVPN, click on the `Stop OpenVPN Server` button. Then, uncheck `OpenVPN` on RED and click Save. This will fully disable the OpenVPN server. If you only stop the server, on the next reboot of the NetSentron, the OpenVPN server will start again.

OpenVPN Clients

Included on the NetSentron are some OpenVPN clients, they are found on the Info->ip utils page. If you have a Windows machine or a Mac, you can download the appropriate client and then install it on the remote machine that is going to use the vpn tunnel.

Installation of the clients is straight forward and no real explanation is required.

Configuring Windows OpenVPN Clients

1. On a Windows machine, you need to copy the contents of the zip file we created on the NetSentron to the configuration directory. The configuration directory is located at: ***C:\Program Files\OpenVPN\config\***

2. Open up the zip file we created earlier and copy the contents of that file to the config directory. The files in the zip should be *ConnectionName.p12* and *ConnectionName-TO-NetSentron.ovpn* where *ConnectionName* is the name you set for the tunnel. If you open the zip file in Windows Explorer and open up the config directory in another Windows Explorer, you can simply drag and drop the two files into the config directory.

3. Next, double click the `OpenVPN GUI` icon to start the OpenVPN client. Not much will happen on your desktop, but a new icon will appear in the lower right hand side. It will be two little computers together with a world between them. The screens on the computers will be RED, indicating no connection.

4. Next, right click on the icon and choose `Connect`.

5. A dialog will come up and it will start outputting information and then a second dialog will come up and ask you to enter a password.

6. Remember that password we told you to write down earlier? It is now time to enter that password (and every time you wish to connect to the LAN).
7. Enter the password and the first dialog should continue to output information. If everything goes as planned, the dialog should disappear and the icon for OpenVPN should go from RED to YELLOW and finally GREEN when connected. If the dialog does not go away and seems to be repeating itself, click on the Disconnect button, then go back to the icon in the bottom toolbar and right click and hit `Connect`.

8. It may take a couple of tries to get the connection up, but eventually the icon in the toolbar will show Green screens. Once you have the Green screens, you cannot access the resources of your LAN.

NOTE
Just like the IPSec VPN, you have to connect to servers and services using IP addresses.

9. When you are done with the VPN, right click the `OpenVPN` icon in the

toolbar and select Disconnect. The icon will now go to Red screens.

10. Right click the `OpenVPN` icon again and select Exit, to completely disable OpenVPN

Configuring Mac OpenVPN clients

NOTE: The Mac client at the time of this writing only works on Macs with OSX 10.4 to 10.7

1. The Mac client is called Tunnelblick. To configure the client, make sure you have the zip file contents ready to go.

2. A dialog box will ask for an administrator username/password to secure Tunnelblick. Type the administrator credentials and click OK.

3. Click the `Create` and open configuration folder button.

4. A Finder window will open with the configuration folder.

5. Open up the zip file we created earlier and copy the contents of that file to the configuration folder. The files in the zip should be *ConnectionName.p12* and *ConnectionName-TO-NetSentron.ovpn* where *ConnectionName* is the name you set for the tunnel.

6. Rename the configuration directory to the name of the connection you want and add the extension .tblk

7. Close Tunnelblick

8. Double click on the renamed folder and it should install the certificate and the configuration file for OpenVPN.

9. Start Tunnelblick

10. A dialog box will appear asking if you wish to check for updates to Tunnelblick automatically. Click Check Automatically or Don't Check, as you prefer;

11. A dialog box will appear asking for an administrator username/password to secure the configuration file. Type administrator credentials and click OK;

12. A dialog box will appear asking for the VPN password. Type the VPN password and click "OK" . You may save them in the Keychain by putting a check in the check box.

    You should now be connected to your LAN.

13. Verify by pinging across to a machine on the LAN.

Configuring Android OpenVPN clients

1. Use an SD Card, FTP, or other method to copy the contents of the zip file we created on the NetSentron to the Android device you intend to VPN from.

2. Download the "OpenVPN Connect" app from the Google Play store..

3. Open the "OpenVPN Connect" app, and tap "menu," then tap "import."

4. Tap "Import Profile from SD card. Navigate to the location on your device's storage you saved the files in step 1.

5. You will be returned to the homes screen of the home screen of the "OpenVPN Connect" app. Click the button that says "connect." A message should appear prompting you to select a client certificate. Tap "select certificate."

6. Tap the "Install" button to install a new certificate. Navigate to the location on your device's storage you saved the contents of the zip file in step 1. Select the .p12 file.

7. On the certificate page, tap "Allow."

8. The "OpenVPN Connect" app should now display the status of the VPN connection.

NOTE: for more information regarding issues or advanced setup with "OpenVPN Connect" see https://docs.openvpn.net/docs/openvpn-connect/openvpn-connect-android-faq.html

Configuring iOS OpenVPN clients

1. Download the "OpenVPN Connect" app from the App Store..

2. Email the contents of the zip file we created on the NetSentron to the iOS device.

3. Open the Mail app and find the email containing the two files. Tap the .p12 file.

4. In the "Install Profile" page, tap "install. Tap "Install now," and key in the password for the profile. Tap "Done."

5. Navigate back to the Mail app and find the email containing the two files. Tap the .ovvpn file, and tap "Open in OpenVPN."

6. The "OpenVPN Connect" app will appear. Tap the green plus sign to open the profile.

7. Tap "None selected" next to the title "Certificate." Select the

certificate, then tap the "OpenVPN" button in the top left to return to the previous screen.

8. Finally, tap the slider to "connect."

NOTE: for more information regarding issues or advanced setup with "OpenVPN Connect" see https://docs.openvpn.net/docs/openvpn-connect/openvpn-connect-ios-faq.html

Chapter 10 Logs

The Logs section on the NetSentron Interface gives the administrator the ability to view all the NetSentron logs. By default, when you click on the Logs button you will be given the Summary Logs Page. Clicking on the remaining buttons gives the administrator access to viewing Settings, Web Access, Firewall, IDS and other logs.

Viewing Summary Logs

From the Summary Logs page you can view the Kernel/Firewall logs, the Local and Remote Login logs and Disk Usage Logs. From this page you have the option of choosing which date you want to view the logs for.

1. From the Administration Interface, click on the button. The Summary Logs page appears. *See* ***Error! Reference source not found.**.* The displayed logs are from the previous day.

2. Use the drop down menus to select the month and day of the specific logs you want to view and then click the Update button. The logs for the date selected are listed.

Exporting Summary Logs

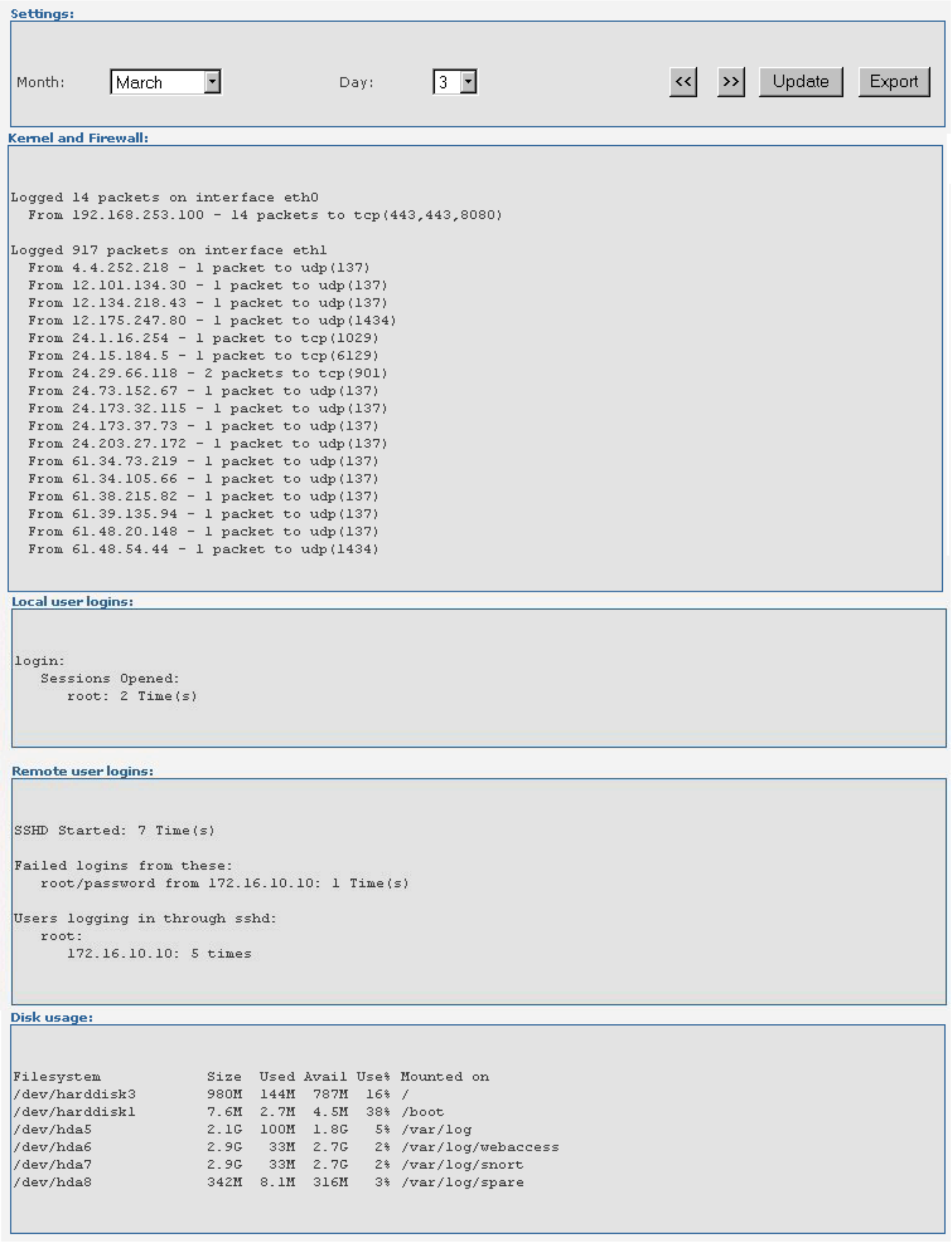
The export option to allow you to download the summary logs from your NetSentron to your local machine.

1. From the Administration Interface, click on the Logs button. The Summary Logs page appears. *See Figure 10.1: Summary Logs* on the next page.
2. Use the drop down menus to select the month and day of the specific logs you want to Export and then click the Update button. The logs for the date selected are listed.
3. Next, click on the Export button. A `File Download` dialog box

appears.

4. To save the log, click on the Save button. The `Save As` dialog box appears. Using the drop down menu, select a location where you want to save your logs. Click the Save button to confirm. The logs have now been saved separate from the NetSentron Server.

Figure 10.1: Summary Logs



Settings:

Month: March

Day: 3

Kernel and Firewall:

```
Logged 14 packets on interface eth0
  From 192.168.253.100 - 14 packets to tcp(443,443,8080)

Logged 917 packets on interface eth1
  From 4.4.252.218 - 1 packet to udp(137)
  From 12.101.134.30 - 1 packet to udp(137)
  From 12.134.218.43 - 1 packet to udp(137)
  From 12.175.247.80 - 1 packet to udp(1434)
  From 24.1.16.254 - 1 packet to tcp(1029)
  From 24.15.184.5 - 1 packet to tcp(6129)
  From 24.29.66.118 - 2 packets to tcp(901)
  From 24.73.152.67 - 1 packet to udp(137)
  From 24.173.32.115 - 1 packet to udp(137)
  From 24.173.37.73 - 1 packet to udp(137)
  From 24.203.27.172 - 1 packet to udp(137)
  From 61.34.73.219 - 1 packet to udp(137)
  From 61.34.105.66 - 1 packet to udp(137)
  From 61.38.215.82 - 1 packet to udp(137)
  From 61.39.135.94 - 1 packet to udp(137)
  From 61.48.20.148 - 1 packet to udp(137)
  From 61.48.54.44 - 1 packet to udp(1434)
```

Local user logins:

```
login:
   Sessions Opened:
      root: 2 Time(s)
```

Remote user logins:

```
SSHD Started: 7 Time(s)

Failed logins from these:
   root/password from 172.16.10.10: 1 Time(s)

Users logging in through sshd:
   root:
      172.16.10.10: 5 times
```

Disk usage:

```
Filesystem            Size  Used Avail Use% Mounted on
/dev/harddisk3        980M  144M  787M  16% /
/dev/harddisk1        7.6M  2.7M  4.5M  38% /boot
/dev/hda5             2.1G  100M  1.8G   5% /var/log
/dev/hda6             2.9G   33M  2.7G   2% /var/log/webaccess
/dev/hda7             2.9G   33M  2.7G   2% /var/log/snort
/dev/hda8             342M  8.1M  316M   3% /var/log/spare
```

Log Settings

The Log Settings administration page allows the administrator to make changes to how the summary log is viewed, select how long to keep log summary and how to enable remote logging.

1. From the Administration Interface, click on the Logs button.

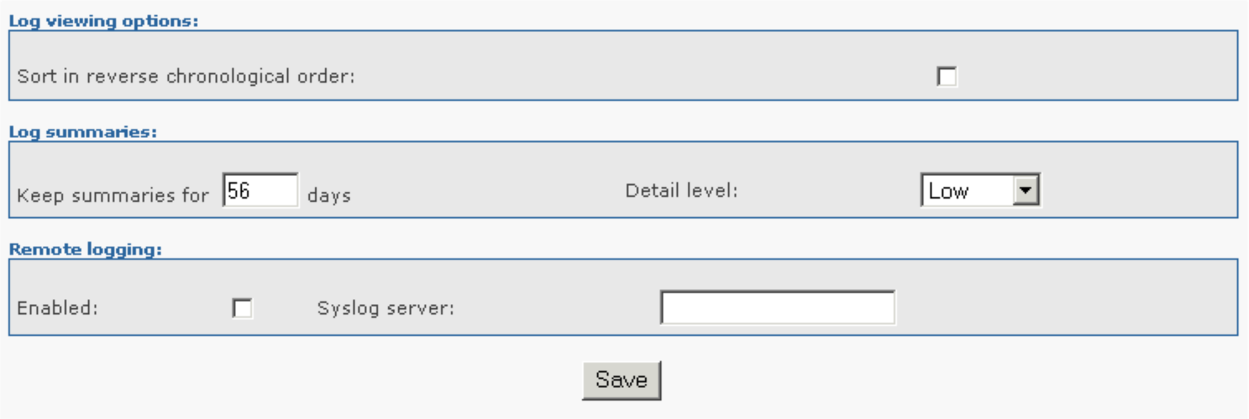
The Summary Logs page appears.

To make changes to the log settings, click on the settings button. The Log Settings page appears. *See Figure 10.2: Log Settings, below*. The Log Settings page has been divided into 3 panels. The following is a description of the panels provided on this page.

Log viewing options	Checking the box provided allows you to view the summary log in reverse chronological order.
Log summaries	Key in the amount of days you would like the log summaries saved for. In this display you can also select the Detail level from the drop down box. The higher the level the more detail will be listed on the summary logs. **Note**: The detail level is defaulted at low.
Remote logging	Allows the administrator to select an IP address of a remote server and allow the logs to be sent to that machine. Key in the IP address of the remote server and then select the enabled box.

2. Click the Save button to confirm the changes. To view your logs go to the Logs Summary page.

Figure 10.2: Log Settings



Log viewing options:

Sort in reverse chronological order: ☐

Log summaries:

Keep summaries for 56 days Detail level: Low

Remote logging:

Enabled: ☐ Syslog server:

Viewing the Web Access Logs

The Web Access Page gives you the ability to view the usage log on the web server. This program will examine the log files created by the content filtering software.

Different search criteria can be specified. The search criteria are cumulative (added together). For example, specifying a date range and an IP address will only show entries that match BOTH criteria. If you want to see all log entries, do not specify any criteria.

Presently, no sorting is done on the results. This is to ensure a very fast search, use a small amount of memory, and "feed" the browser periodically with information so a timeout does not occur.

1. From the Administration Interface, click on the Logs button. New sets of buttons appear.
2. Click on the web access button. The Web Access Page appears. *See Figure 10.3: Web Access Logs* on page 277 .The following is a description of each of the search criteria.

Enter Date Range Select the range of dates to match. If dates are used, **both** a start and end date must be selected. Failure to select any part of a start or end date will result in no date range being used. The dates will match greater than or equal to start date - less than or equal to end date.

Enter IP address Enter an IPv4 address to match. Example: 10.0.0.1

Enter A Username Enter a username to match. Proxy auth must be enabled in the Proxy page for this to work. If usernames are not shown when matching without any criteria, then proxy auth is most likely not enabled. Refer to the appropriate instructions on how to do this.

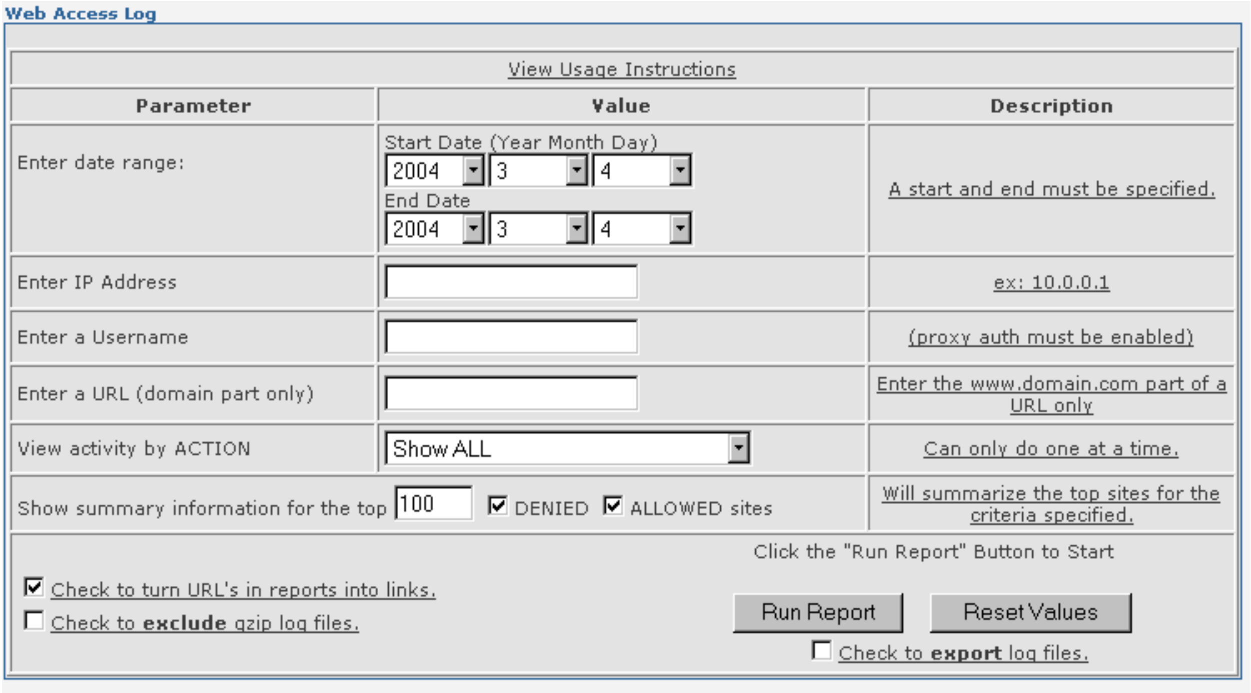
Enter a URL (domain art only) Enter the www.domain.com part of a URL only. Do not enter http:// or any other part of the url. Exact match only.

View Activity by ACTION	Enter an action to match. Use the drop-down list to select the ACTION to match. The ACTIONs are the special case requests logged by the content filter. To see ALL matches for DENIED and EXCEPTION, select "ALL DENIED" or "ALL EXCEPTIONS". Only one ACTION can be viewed at a time and it shows the most restrictive. For example, if "Banned Site" is selected, then only DENIED requests that were DENIED because of a site being in a banned site list will be shown. No other DENIED requests will be shown.
Show Summary Information for the top	Selecting these options will show a summary report for the number of sites entered. The top 1 to 999 sites may be selected. Note: the higher the number, the longer the report will take to process. Once the summary screen appears, you may "investigate" why a site was denied/allowed and who/what machine was visiting the site. Simply click on the "Trace" link under the "Investigate" column and the results will be shown. Caution: If you select to filter for only DENIED and check to show a summary for allowed, there will not be any results. This is correct. If you don't see the results you expected, go back and check the criteria that were entered.
URLs to links	Checking this box will allow you to click the URL links in the report.
Exclude gzip log files	Checking this box will cause the report generator to skip archived files. Only the current weeks log file will be used for the report. At the end of each week, the current log file is compressed using gzip and a new log file is created.
Export log files	Checking this box will cause the report to be exported to your PC in a tab delimited format that can be imported into MS Access or MS Excel. The first line of the file is the field names. The delimiting character is a tab

3. Once you have selected your search criteria, click on the

button.

Figure 10.3: Web Access Logs



Web Access Log

View Usage Instructions

Parameter	Value	Description
Enter date range:	Start Date (Year Month Day) 2004 ▾ 3 ▾ 4 ▾ End Date 2004 ▾ 3 ▾ 4 ▾	A start and end must be specified.
Enter IP Address		ex: 10.0.0.1
Enter a Username		(proxy auth must be enabled)
Enter a URL (domain part only)		Enter the www.domain.com part of a URL only
View activity by ACTION	Show ALL ▾	Can only do one at a time.
Show summary information for the top	100 ☑ DENIED ☑ ALLOWED sites	Will summarize the top sites for the criteria specified.

☑ Check to turn URL's in reports into links.

☐ Check to **exclude** gzip log files.

Click the "Run Report" Button to Start

Run Report | Reset Values

☐ Check to **export** log files.

Viewing Firewall Logs

The Firewall Logs Page on the NetSentron Interface allows you to view the logs of all unauthorized machines trying to gain access to your network.

In this section there are the Source and Destination IP addresses and ports, as well as the protocol involved.

NOTE

Not all denied packets are hostile attempts by hackers to gain access to your network. Connections to the ident/auth port (113) and Net Bios port (137) are common occurrences and can be safely ignored. However, you should pay attention to any attempted connections to destination ports 5445 and 222.

1. From the Administration Interface, click on the Logs button. New sets of buttons appear.
2. Click on the firewall button. The Firewall Logs Page appears. *See*

Figure 10.4: Firewall Logs on page 279.

3. Just like your standard log viewer, you can select which logs you wish to view by clicking on date. You can select the dates by clicking on the drop boxes next to month and day. When entering the page you are defaulted with the current date. Once you have selected a date, click on the Update button. All the firewall logs for the chosen date are listed*.*

Blocking IP Addresses from Firewall Logs Page

The Firewall Logs page also give the administration a quick way to block IP address directly from the Firewall Logs page.

1. From the Firewall Logs page you will see a list of IP addresses. This is a list of the hack attempts. Click the Mark box on the same line of the IP address want to block. You may select more than one IP address at a time to block.
2. Click on the Block Address button. The page refreshes. The IP addresses have been added to the blocked IP address list.

NOTE

You will still see the blocked IP address listed on the Firewall Logs page.

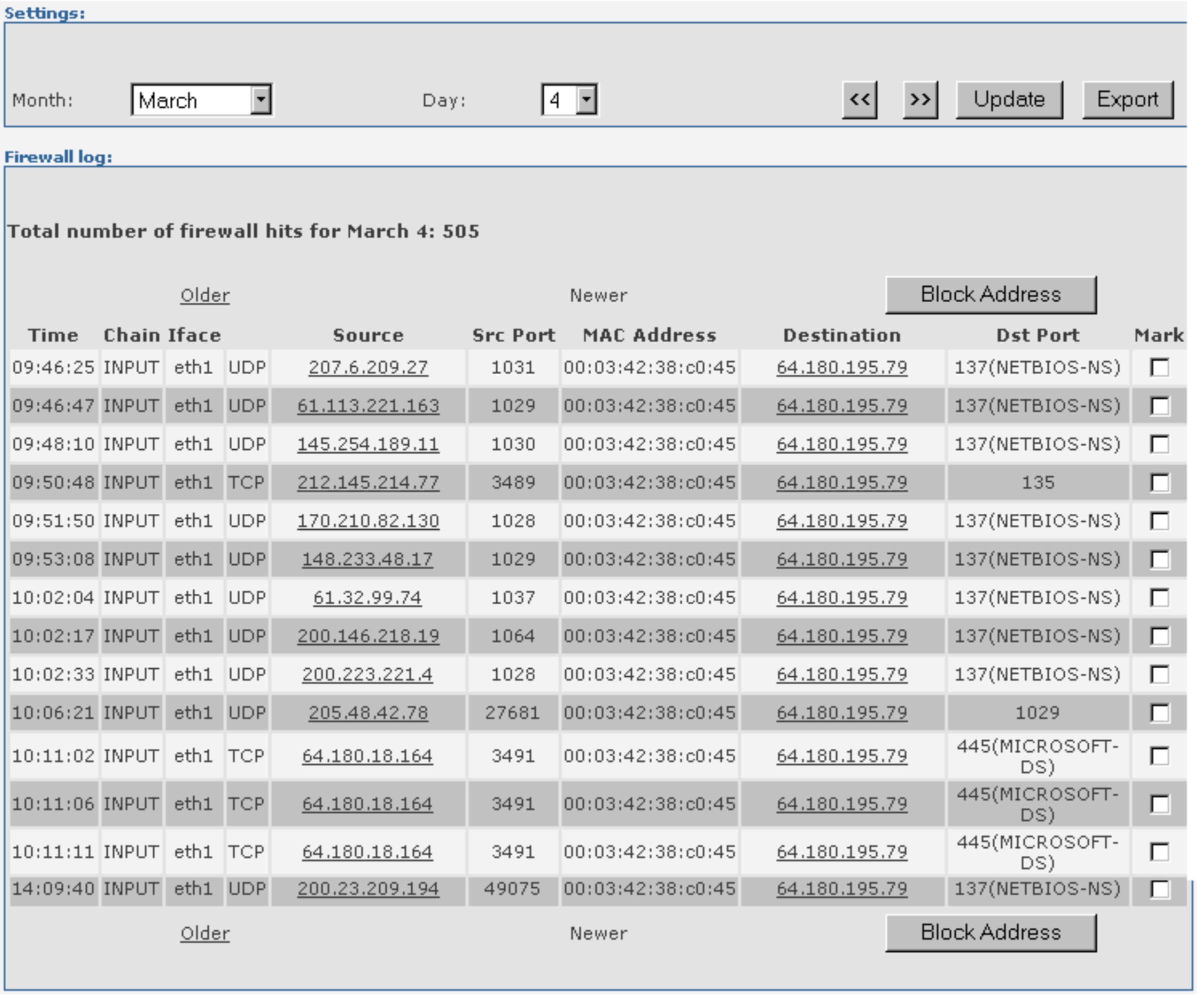
3. To confirm if the IP address have been blocked, click on the Firewall and then the ip block button. The IP addresses you blocked should be listed on this page. You can also edit and remove the IP address from this page. For instructions on editing a blocked IP see the section on *Editing a Blocked IP, above*. For instruction on removing a Blocked IP see the section on *Removing a Blocked IP, above*.

Exporting Firewall Logs

If desired, you may use the export option to download firewall logs file from your NetSentron to your local machine.

1. From the Administration Interface, click on the Logs button. The Firewall Logs page appears. *See Figure 10.4: Firewall Logs, below.*
2. Use the drop down menus to select the month and day of the specific logs you want to Export and then click the Update button. The logs for the date selected are listed.
3. Next, click on the Export button. A File Download dialog box appears.
4. To save the log, click on the Save button. The Save As dialog box appears.
5. Using the drop down menu, select a location where you want to save your logs. Click the Save button to confirm. The logs have now been saved separate from the NetSentron Server.

Figure 10.4: Firewall Logs



Month: March

Day: 4

Total number of firewall hits for March 4: 505

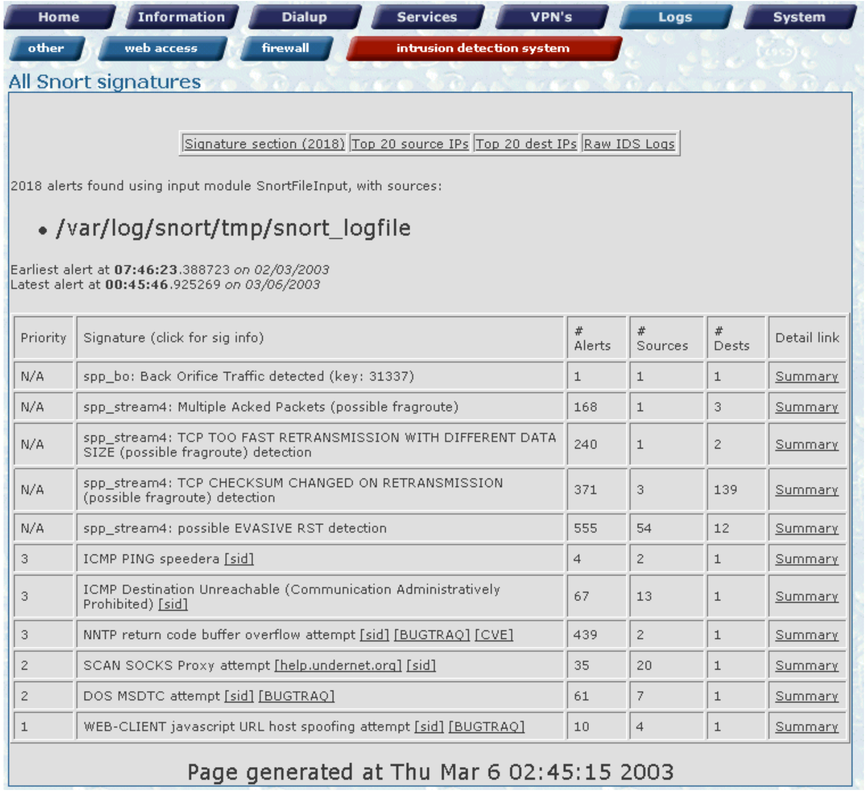
Time	Chain	Iface		Source	Src Port	MAC Address	Destination	Dst Port	Mark
09:46:25	INPUT	eth1	UDP	207.6.209.27	1031	00:03:42:38:c0:45	64.180.195.79	137(NETBIOS-NS)	☐
09:46:47	INPUT	eth1	UDP	61.113.221.163	1029	00:03:42:38:c0:45	64.180.195.79	137(NETBIOS-NS)	☐
09:48:10	INPUT	eth1	UDP	145.254.189.11	1030	00:03:42:38:c0:45	64.180.195.79	137(NETBIOS-NS)	☐
09:50:48	INPUT	eth1	TCP	212.145.214.77	3489	00:03:42:38:c0:45	64.180.195.79	135	☐
09:51:50	INPUT	eth1	UDP	170.210.82.130	1028	00:03:42:38:c0:45	64.180.195.79	137(NETBIOS-NS)	☐
09:53:08	INPUT	eth1	UDP	148.233.48.17	1029	00:03:42:38:c0:45	64.180.195.79	137(NETBIOS-NS)	☐
10:02:04	INPUT	eth1	UDP	61.32.99.74	1037	00:03:42:38:c0:45	64.180.195.79	137(NETBIOS-NS)	☐
10:02:17	INPUT	eth1	UDP	200.146.218.19	1064	00:03:42:38:c0:45	64.180.195.79	137(NETBIOS-NS)	☐
10:02:33	INPUT	eth1	UDP	200.223.221.4	1028	00:03:42:38:c0:45	64.180.195.79	137(NETBIOS-NS)	☐
10:06:21	INPUT	eth1	UDP	205.48.42.78	27681	00:03:42:38:c0:45	64.180.195.79	1029	☐
10:11:02	INPUT	eth1	TCP	64.180.18.164	3491	00:03:42:38:c0:45	64.180.195.79	445(MICROSOFT-DS)	☐
10:11:06	INPUT	eth1	TCP	64.180.18.164	3491	00:03:42:38:c0:45	64.180.195.79	445(MICROSOFT-DS)	☐
10:11:11	INPUT	eth1	TCP	64.180.18.164	3491	00:03:42:38:c0:45	64.180.195.79	445(MICROSOFT-DS)	☐
14:09:40	INPUT	eth1	UDP	200.23.209.194	49075	00:03:42:38:c0:45	64.180.195.79	137(NETBIOS-NS)	☐

Viewing Intrusion Detection System Logs

Just like your Firewall logs, the Intrusion Detection System (IDS) logs allow you to view logs of attempted attacks on your network. Unlike your Firewall logs, the IDS logs give you more detailed information on the type of attack detected. By default you are given the logs for the current date.

1. Start from the Administration Interface, click on the Logs button. New sets of buttons appear.
2. Click on the intrusion detection system button. The IDS Logs Page appears. For a detailed summary of the recorded alert click on the **Summary** link located in the last column of each alert. *See Figure 10.5: IDS Logs below*.

Figure 10.5: IDS Logs



All Snort signatures

Signature section (2018) | Top 20 source IPs | Top 20 dest IPs | Raw IDS Logs

2018 alerts found using input module SnortFileInput, with sources:

- /var/log/snort/tmp/snort_logfile

Earliest alert at **07:46:23**.388723 *on 02/03/2003*
Latest alert at **00:45:46**.925269 *on 03/06/2003*

Priority	Signature (click for sig info)	# Alerts	# Sources	# Dests	Detail link
N/A	spp_bo: Back Orifice Traffic detected (key: 31337)	1	1	1	Summary
N/A	spp_stream4: Multiple Acked Packets (possible fragroute)	168	1	3	Summary
N/A	spp_stream4: TCP TOO FAST RETRANSMISSION WITH DIFFERENT DATA SIZE (possible fragroute) detection	240	1	2	Summary
N/A	spp_stream4: TCP CHECKSUM CHANGED ON RETRANSMISSION (possible fragroute) detection	371	3	139	Summary
N/A	spp_stream4: possible EVASIVE RST detection	555	54	12	Summary
3	ICMP PING speedera [sid]	4	2	1	Summary
3	ICMP Destination Unreachable (Communication Administratively Prohibited) [sid]	67	13	1	Summary
3	NNTP return code buffer overflow attempt [sid] [BUGTRAQ] [CVE]	439	2	1	Summary
2	SCAN SOCKS Proxy attempt [help.undernet.org] [sid]	35	20	1	Summary
2	DOS MSDTC attempt [sid] [BUGTRAQ]	61	7	1	Summary
1	WEB-CLIENT javascript URL host spoofing attempt [sid] [BUGTRAQ]	10	4	1	Summary

Page generated at Thu Mar 6 02:45:15 2003

Viewing System Logs

The Systems Logs Administration Page gives you the ability to view the following system logs; general NetSentron log (default), PPP logs, ISDN logs, DHCP server logs, SSH logs, Login/Logout logs, Kernel logs, IPSec logs, and Update transcript logs. *See Figure 10.6: Log Systems Page,* on the next page.

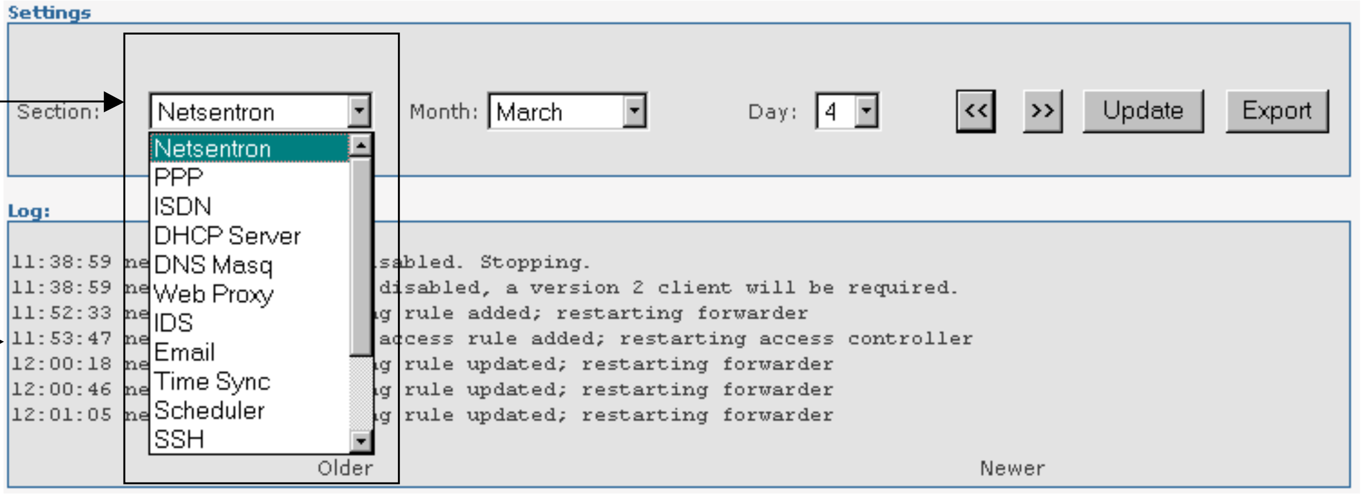
1. From the Administration Interface, click on the Logs button. New sets of buttons appear.
2. Click on the other button. The System Logs page appears. *See Figure*
3. Locate the system log you want to view by clicking on the drop down box. From the list, click on your selection.
4. Next, you can use the month and day drop down menu to select the date of the system log you want to view.
5. Next, click on the Update button. All the log details for your selection are listed in the Logs section. If there is more than one page of log details, you can click the Older and Newer links at the bottom of the section.

NOTE

If there are any errors during the request, they will be listed below in the Error messages section, in red.

Figure 10.6: Log Systems Page

Section dropdown box



Section: Netsentron Month: March Day: 4

```
11:38:59 ne                          sabled. Stopping.
11:38:59 ne                          disabled, a version 2 client will be required.
11:52:33 ne                         g rule added; restarting forwarder
11:53:47 ne                          access rule added; restarting access controller
12:00:18 ne                         g rule updated; restarting forwarder
12:00:46 ne                         g rule updated; restarting forwarder
12:01:05 ne                         g rule updated; restarting forwarder
```

Logs panel

Exporting System Logs

If desired, you may use the export option to download system logs file from your NetSentron to your local machine.

1. From the Administration Interface, click on the Logs button. The Firewall Logs page appears. *See Figure 10.4: Firewall Logs*, on page 279.
2. Use the drop down menus to select the month and day of the specific logs you want to Export and then click the Update button. The logs for the date selected are listed.
3. Next, click on the Export button. A File Download dialog box appears.
4. To save the log, click on the Save button. The Save As dialog box appears.
5. Using the drop down menu, select a location where you want to save your logs. Click the Save button to confirm. The logs have now been saved separate from the NetSentron Server.

Chapter 11 Systems

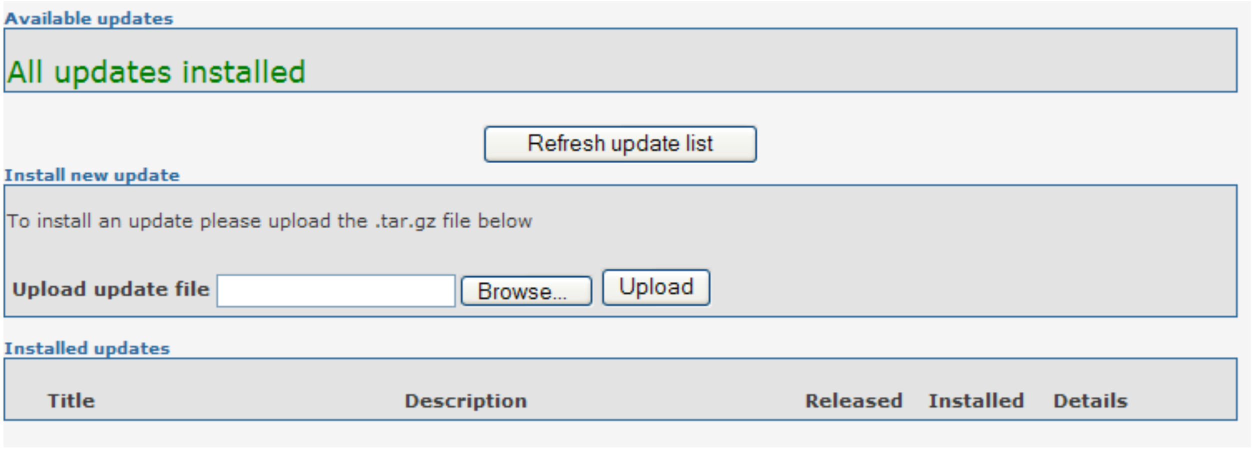
The Systems section of your NetSentron interface gives you the ability to setup and configure your NetSentron settings, as well as do updates and backups. By default, when you click on the System button you will be given the Updates page. Clicking on the remaining buttons gives you all other system administration pages.

Updating the NetSentron

The `Updates` page allows you to upload any new patches for the NetSentron. You are usually alerted of any updates on the Home page of the NetSentron Interface.

1. Start from the Administration Interface, click on the System button. New sets of buttons appear.
2. Click the updates button. The `Updates Administration` Page of the NetSentron Interface appears. See *Figure 11.1: Updates Administration Page*, below. This page is divided into three panels. The first panel displays the updates that have been installed. The second panel displays the available updates. The third panel is used to install the update.

Figure 11.1: Updates Administration Page



Available updates

All updates installed

Install new update

To install an update please upload the .tar.gz file below

Upload update file

Installed updates

Title	Description	Released	Installed	Details

3. Click the Refresh update list located at the bottom of the `Updates` page.
4. All the latest updates should be in the `Available Updates` section. Click on the update link.
5. Save the file to your local hard drive. Make note of where you saved it.
6. Click on the Browse... button located in the `Install New Update` section. Locate the patch you saved and click on it.
7. Click the **Open** button. The patch you selected is in the `Upload update` file.
8. Click the **Upload** button. The patch has been installed. **NOTE**: You should see a log in the `Installed Updates` section, showing that the patch has been installed. In some cases it might be necessary to do a reboot. For instructions on how to reboot the NetSentron go to *Rebooting/Shutting Down the NetSentron*.

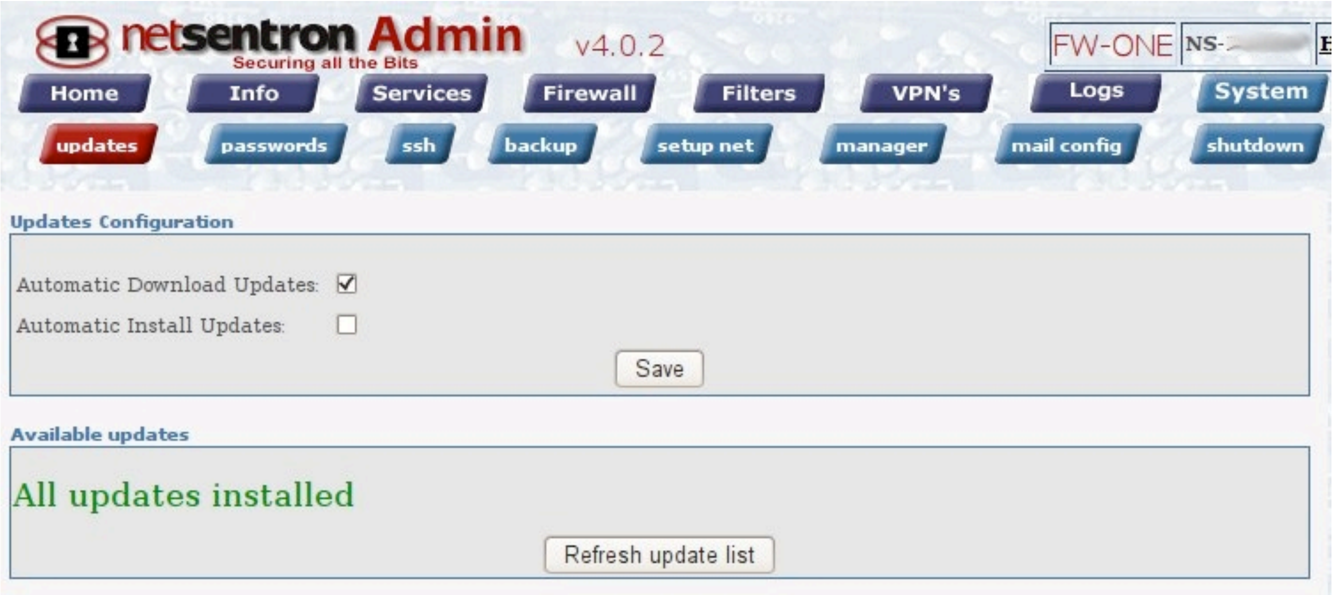
Automatic Updates and Installation

As of version 4.0.1, we have added the ability for the NetSentron to grab updates; inform you of their presence and optionally automatically install them.

If you wish to be emailed notices of updates that are ready to be installed, or updates that have been installed, insure that you configure your NetSentron to connect to an SMTP server, instructions for that are located in Chaper 11 – Mail Configuration.

To enable automatic downloading of updates on your NetSentron, go to System → `Updates`. You will notice a box at the top of the page labeled `Updates Configuration`. Within that box are two options, `Automatic Download Updates` and `Automatic Install Updates` as *Figure 11.2* shows below.

Figure 11.2: Updates Configuration Display



Updates Configuration

Automatic Download Updates: ☑

Automatic Install Updates: □

Available updates

All updates installed

To have the NetSentron automatically download an update when one becomes available, enable the check box next to `Automatic Download Updates` and click Save.

To have the NetSentron automatically install the downloaded updates, make sure that Automatic Install Updates is also checked.

If you only have Automatic Download Updates checked, then the NetSentron will download an update as one becomes available and if you have set up Mail Config, then it will send you an email telling you that there is an update waiting to be installed. When you come back to the Updates page, you will see the update listed and a small icon next to it to install the update. Click on that icon and it will install the update.

If you have both checkboxes enabled, then the NetSentron will download updates as they become available and install them. Then, if Mail Config has been set up, it will email you with the results of the update.

SSH

The SSH (Secured Shell) session on your NetSentron allows the user SSH access without having a SSH client installed on your system. This is a remote access tool used to configure definite aspects on the NetSentron Security Server, which cannot be conducted through the GUI Interface alone. Only root and setup users are allowed to log into an SSH session

1. From the Administration Interface, click the System **button**. New sets of buttons appear.

2. Next, click the ssh button**.** The `Remote Access` display appears. Before you can make any changes you will have to activate the SSH session. To do this, ensure every box is checked.

⚠ It is highly recommended that you disable the SSH access once you are done with your changes. To do this, uncheck all the boxes on the Remote access display and then click the Save button.

3. Once you have selected each box, click on the Save button. The SSH session has now been activated. The SSH Session appears.

4. Next, press the **Enter** button on your keyboard. A login prompt will appear with the name setup.

NOTE

If you want to login as root, use the backspace button on your keyboard, remove the name setup and key in root.

5. Key in your setup password. If you are logging in as root, key in the root password. If logging is a setup, key in the setup password.

NOTE

If you are accessing SSH for the first time, key in the default password, ***setup***. Press the **Enter** button on your keyboard. The Section Menu appears.

NOTE

You are unable to use your mouse in this display. Use the ↑ and ↓ arrows to move between selections. Use the **Tab** button on your keyboard to move between OK and Quit. Use the **Space** or **Enter** buttons on your keyboard to make a selection.

Backup

The Backup Page is used to back up all the NetSentron configuration files. Once you have configured all the settings on your NetSentron it would be wise to do a back-up in case your systems need a fresh install.

Creating a Backup

Backing up to your Desktop

1. Start from the Administration Interface, click on the System button. New sets of buttons appear.
2. Click the backup button. The `Backup Page` of the NetSentron Interface appears. See *Figure 11.3* on the next page.
3. Click on the Create button. The set you created will be listed in the Backup Sets field, above.

> **NOTE**
>
> The set will include the date and time.

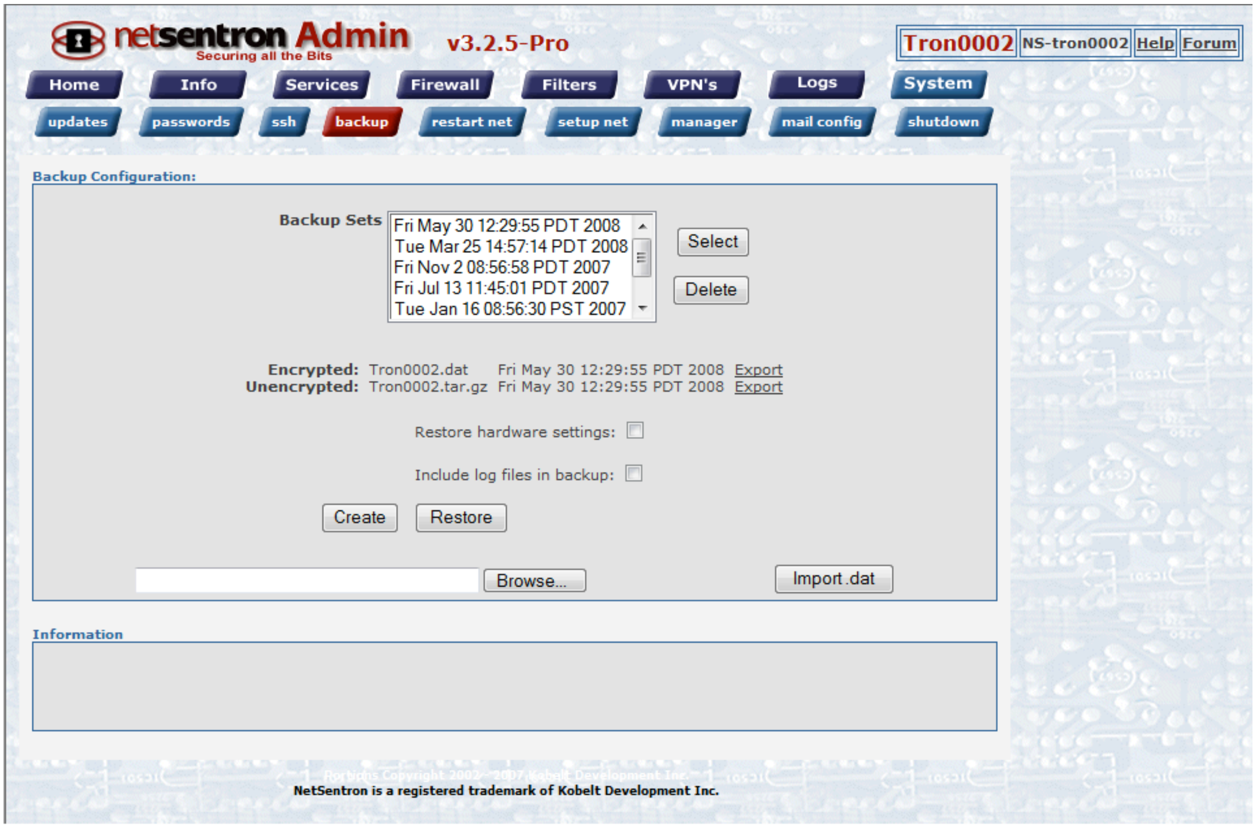
4. Highlight the set you want to backup by clicking on it, and then click the Select button.

> **NOTE**
>
> The set you selected is listed below twice. One set is encrypted, which is used for restoring all the settings created on the NetSentron. This file will be saved as a .dat. The other set is unencrypted, which would be used in the event that there is a complete failure. This file will be saved as a .tar.gz. It is recommended this file be put somewhere safe, as all passwords to the NetSentron are included. It is also recommended that in the event of a complete failure that you should contact a KDI Technician or a NetSentron Partner to help with a complete restoration.

5. Next click on the ***export*** link associated with the set you want to back up. The `File Download` dialog box will appear.

6. Select where you want to save the file and then click the Save button.

Figure 11.3: Backup Administration Page



Backup Configuration:

Backup Sets
- Fri May 30 12:29:55 PDT 2008
- Tue Mar 25 14:57:14 PDT 2008
- Fri Nov 2 08:56:58 PDT 2007
- Fri Jul 13 11:45:01 PDT 2007
- Tue Jan 16 08:56:30 PST 2007

Select

Delete

Encrypted: Tron0002.dat Fri May 30 12:29:55 PDT 2008 Export
Unencrypted: Tron0002.tar.gz Fri May 30 12:29:55 PDT 2008 Export

Restore hardware settings: □

Include log files in backup: □

Create Restore

Browse... Import .dat

Information

Rorbitns Copyright 2002 - 2007 Kobelt Development Inc.
NetSentron is a registered trademark of Kobelt Development Inc.

Restoring a Backup

1. Start from the Administration Interface, click on the System button. New sets of buttons appear.

2. Click the backup button. The `Backup Page` of the NetSentron

Interface appears. See *Figure 11.3.*

3. Use the Browse... button to locate the file you want to backup (the file would have been saved as a .dat). In the event that this is a restore to a clean installation of the NetSentron Software, then select the file with tar.gz (unencrypted).

4. Once the file has been selected, click on the Import .dat button. In the event that this is a restore to a clean installation of the NetSentron Software, the button will contain **Import .tar.gz**

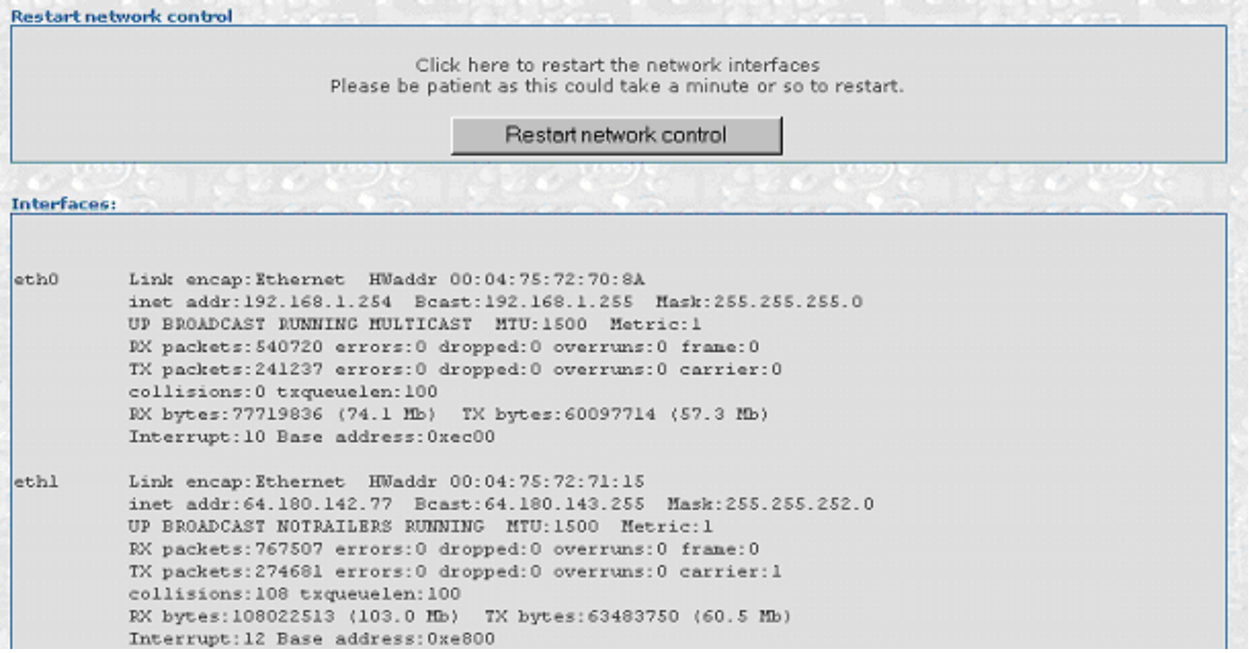
5. Finally click on the **RESTORE** button to restore the uploaded back up file.

Restart Net

The Restart Net page is used whenever you need to restart your network interfaces. This function is similar to a release/renew in windows. Also, from this page you can view the interface details.

1. Start from the Administration Interface, click on the System button. New sets of buttons appear.
2. Click on the restart net button. The Restart Network Control page appears. See *Figure* .
3. Next, click on the Restart network control button to restart the network interfaces.

Figure 11.4: Restart Net Page



Click here to restart the network interfaces
Please be patient as this could take a minute or so to restart.

```
eth0      Link encap:Ethernet  HWaddr 00:04:75:72:70:8A
          inet addr:192.168.1.254  Bcast:192.168.1.255  Mask:255.255.255.0
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:540720 errors:0 dropped:0 overruns:0 frame:0
          TX packets:241237 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:77719836 (74.1 Mb)  TX bytes:60097714 (57.3 Mb)
          Interrupt:10 Base address:0xec00

eth1      Link encap:Ethernet  HWaddr 00:04:75:72:71:15
          inet addr:64.180.142.77  Bcast:64.180.143.255  Mask:255.255.252.0
          UP BROADCAST NOTRAILERS RUNNING  MTU:1500  Metric:1
          RX packets:767507 errors:0 dropped:0 overruns:0 frame:0
          TX packets:274681 errors:0 dropped:0 overruns:0 carrier:1
          collisions:108 txqueuelen:100
          RX bytes:108022513 (103.0 Mb)  TX bytes:63483750 (60.5 Mb)
          Interrupt:12 Base address:0xe800
```

Manager

Unlike the administrator who has full access to the GUI, the Manager may be allowed to manage the NetSentron, but with limited access. The Manager Administration page allows the administrator the ability to select which areas of the NetSentron Administration pages the manager would have access to. Basically you check off the pages that you want the manager to have access to. Note, there is only one manager account available.

Selecting Manager Settings

1. Start from the Administration Interface, click on the System button. New sets of buttons appear.

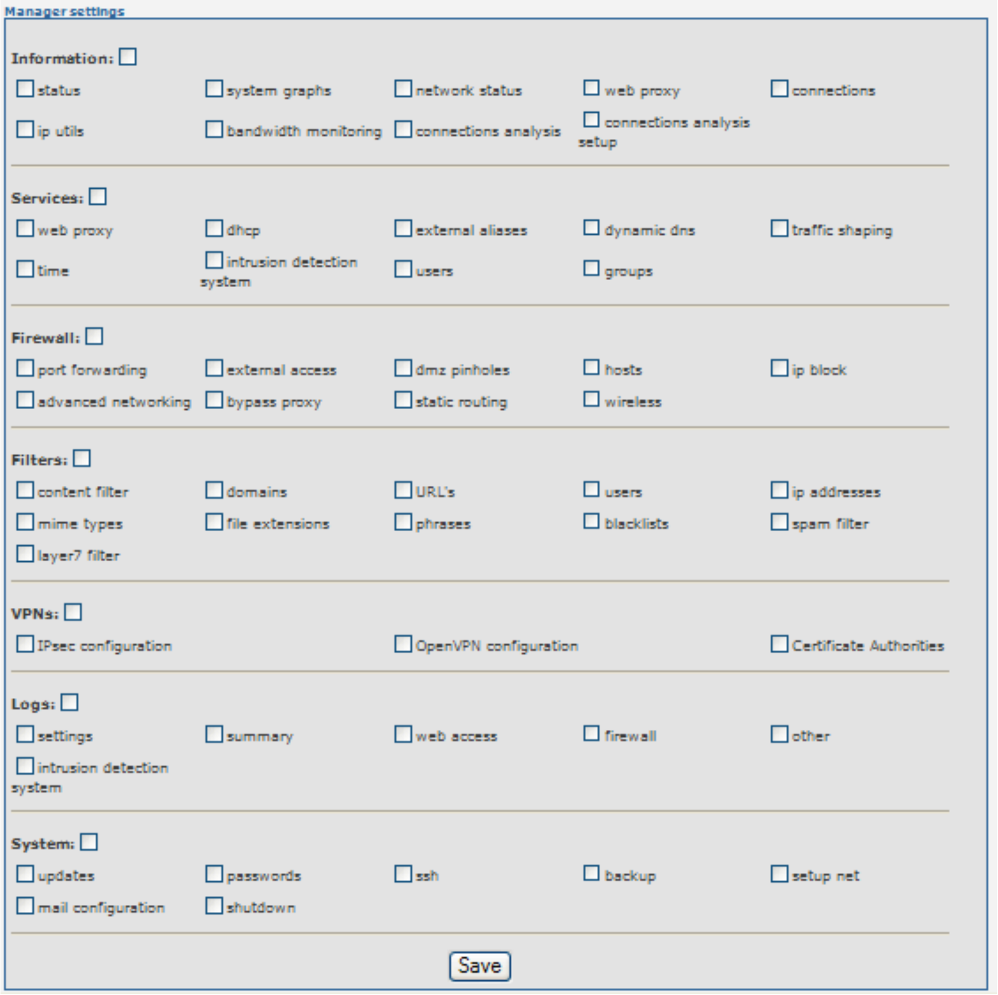
2. Click on the manager button. The `Manager Settings Administration` page is displayed. *See Figure 11.5: Manager Settings Administration Page on the next page.*

3. By selecting the corresponding box, you are allowing the manager access to those areas of the NetSentron Interface.

NOTE
You need to check the title as well. For example if you select web proxy you will also need to select the box next to the title Information.

4. Once you have selected which areas you want the manager to have access to, click the Save button.

Figure 11.5: Manager Settings Administration Page



Manager settings

Information: □

□ status □ system graphs □ network status □ web proxy □ connections

□ ip utils □ bandwidth monitoring □ connections analysis □ connections analysis setup

Services: □

□ web proxy □ dhcp □ external aliases □ dynamic dns □ traffic shaping

□ time □ intrusion detection system □ users □ groups

Firewall: □

□ port forwarding □ external access □ dmz pinholes □ hosts □ ip block

□ advanced networking □ bypass proxy □ static routing □ wireless

Filters: □

□ content filter □ domains □ URL's □ users □ ip addresses

□ mime types □ file extensions □ phrases □ blacklists □ spam filter

□ layer7 filter

VPNs: □

□ IPsec configuration □ OpenVPN configuration □ Certificate Authorities

Logs: □

□ settings □ summary □ web access □ firewall □ other

□ intrusion detection system

System: □

□ updates □ passwords □ ssh □ backup □ setup net

□ mail configuration □ shutdown

Mail Configuration

Mail configuration allows one to tell the NetSentron about an SMTP server on your LAN or on the Internet that can be used to send important emails from the NetSentron.

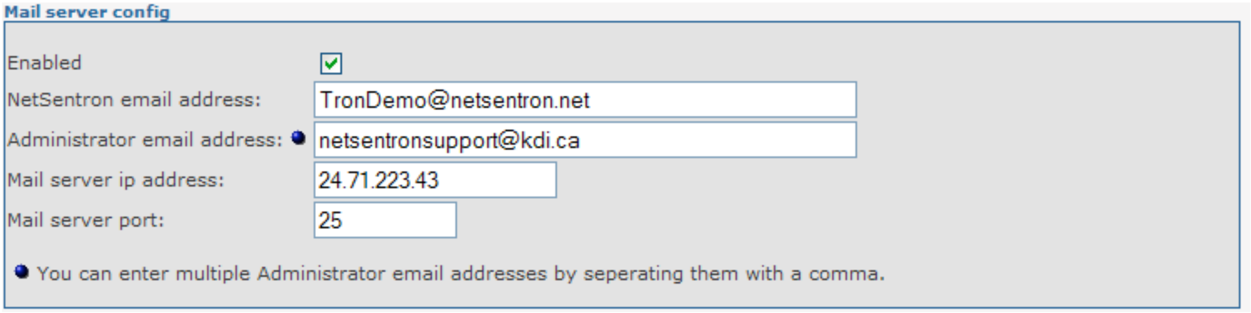
Currently if this section is configured, when an end user is denied access to a web page, a dialogue will pop up allowing the end user to enter a message that will be sent to the administrator.

Also if UPS Monitoring is enabled, emails about the status of the UPS will be sent to the administrator.

The following are instructions on how to do a mail configuration.

1. Start from the Administration Interface, click on the System button. New sets of buttons appear.
2. Click on the mail config button. The `Mail Server Config Administration` page is displayed.

Figure 11.6: Mail Server Config Administration Page



Mail server config

Enabled	☑
NetSentron email address:	TronDemo@netsentron.net
Administrator email address: ●	netsentronsupport@kdi.ca
Mail server ip address:	24.71.223.43
Mail server port:	25

● You can enter multiple Administrator email addresses by seperating them with a comma.

3. To enable, check the `enabled` box.
4. Next, key in the NetSentron email address, the Administrator email address and Mail server ip address.

> **NOTE**
>
> When keying in the NetSentron email address, make sure that it is associated with the network you are on.

5. To confirm, click on the Save button.

Rebooting/Shutting Down the NetSentron

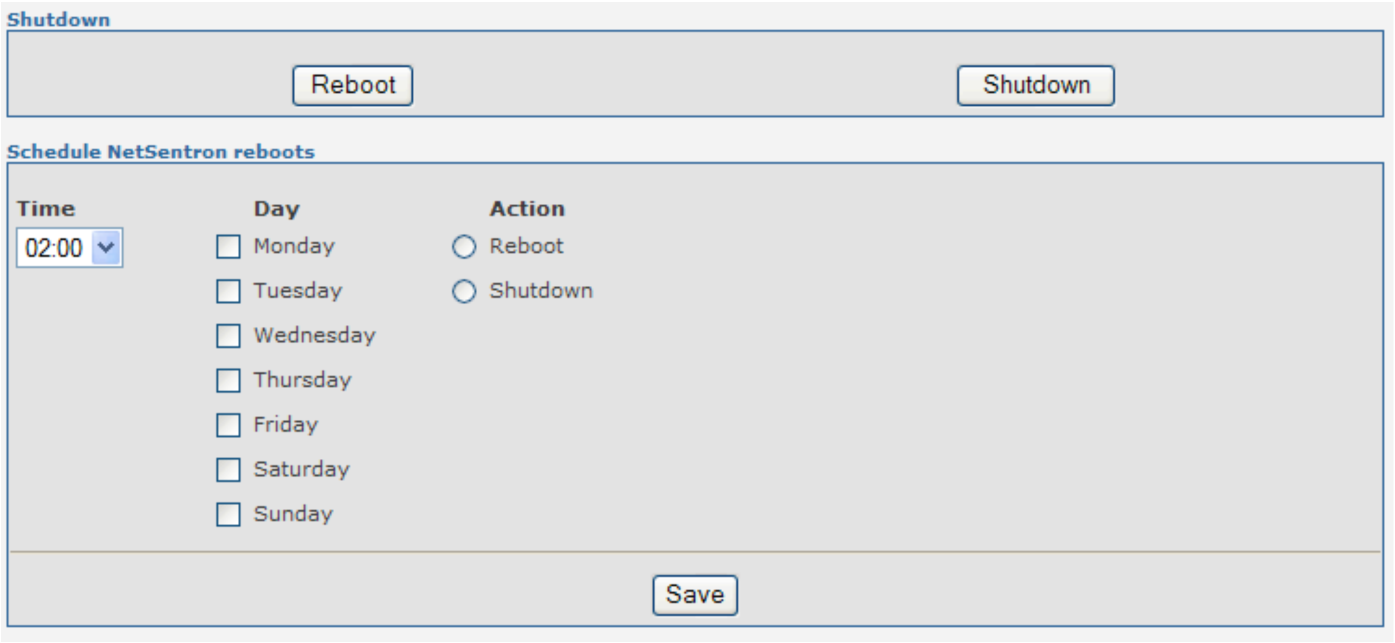
The Shutdown gives the administrator the ability to shutdown and/or reboot the NetSentron server.

3. From the NetSentron Interface, click the System button. The Shutdown page appears. See *Figure 11.7: Shutdown Page*, below.

4. To reboot the NetSentron, simply click the Reboot button located at the bottom of the display.

5. To completely shut down the NetSentron click the Shutdown button. Please be advised that once you click either buttons you will lose the NetSentron GUI Interface.

Figure 11.7: Shutdown Page



Shutdown

Reboot   Shutdown

Schedule NetSentron reboots

Time	Day	Action
02:00	□ Monday	○ Reboot
	□ Tuesday	○ Shutdown
	□ Wednesday	
	□ Thursday	
	□ Friday	
	□ Saturday	
	□ Sunday	

Save

Index

GPL Source used in NetSentron

Red Hat Linux

The underlying operating system - http://www.redhat.com/

apcupsd

Apcupsd a daemon for controlling APC UPSes - http://www2.apcupsd.com/

apache

httpd web server - http://www.apache.org/

busybox

Common UNIX utilities - http://www.busybox.net/

dhcp

DHCP client, server and relay agent - http://www.isc.org/products/DHCP

dansguardian

True content filtering (KDI has a solutions provider license) - http://www.dansguardian.org/

dnsmasq

DNS (domain name) service utility - http://thekelleys.org.uk/

ez-ipupdate

Utility for updating your host name for the any of the dynamic DNS services - http://www.gusnet.cx/proj/ez-ipupdate

fileutils

Basic file manipulation utilities for the GNU operating system - http://www.gnu.org/software/fileutils/

freeswan

Virtual Private Network support - http://www.freeswan.org/

gd

GD graphics library - http://www.boutell.com/gd/

ipac

IP accounting package - http://www.daneben.de/ipac.html

iptables

IPv4 firewalling code - http://www.netfilter.org/

isdn4linux

ISDN kernel modules - http://www.isdn4linux.de/

joe

Joe's own editor - http://sourceforge.net/projects/joe-editor

lct

Linux Console Tools - http://lct.sourceforge.net/

logwatch

Logwatch - http://www.logwatch.org/

less

Text viewer - http://www.greenwoodsoftware.com/

lilo

LInux LOader - Werner Almesberger and John Coffman ncurses

Library to provide window functionality for text-based terminals - http://www.gnu.org/software/ncurses/

ntp

Network Time Protocol utilities - http://www.eecis.udel.edu/~ntp/

openssl

Secure sockets layer toolkit - http://www.openssl.org/

p3scan

Transparent proxy-server for POP3-Clients - http://p3scan.sourceforge.net/

perl

Web programming language - http://www.perl.org/

samba

Windows Network protocol emulation - http://www.samba.org/

sendEmail

A Tool for Sending SMTP Email from a Console - http://caspian.dotconf.net/menu/Software/SendEmail/

shellutils

Basic shell-manipulation utilities of the GNU operating system - http://www.gnu.org/software/shellutils/

snort

Intrusion Detection System - http://www.snort.org/

snortsnarf

Intrusion Detection System Analyzer - http://www.silicondefense.com/

spamassassin

SpamAssassin(tm) is a mail filter to identify spam - http://www.spamassassin.org/

squid

Web proxy cache - http://www.squid-cache.org

squid-graph

Graphical proxy server traffic analysis tool - http://www.squid-graph.dhs.org/

squid log analyzer

Squid Log Analyzer - http://www.aplawrence.com/Unix/squidlog.html

textutils

Basic text-manipulation utilities for the GNU operating system - http://www.gnu.org/software/textutils/

uClibc

A C library for developing embedded Linux systems - http://www.uclibc.org/

Other Contributions

Jose L. Catubigan Jr.

Comment Fields in Port Forwarding - Jose L. Catubigan Jr.

Adam Kennedy - Adam Kennedy

Content Filter GUI - http://sourceforge.net/projects/dgwebminmodule/

Jimmy Myrick - Jimmy Myrick

Content Filter Log Analyzer - http://www.tiger.org/technology/dg/

IPCop

The NetSentron is based on the IPCop GPL firewall project. KDI has donated much time and code to the IPCop Project, including the Port Forwarding page for iptables.

Smoothwall

IPCop is based on the Smoothwall GPL version, v0.9.9. Smoothwall was developed by:

Founder and Project Manager - Richard Morrell (dick@dickmorrell.com)

Development Team Leader and Author - Lawrence Manning (lawrence@smoothwall.org)

Licenses

Zlib Licence - Copyright (C) 1995-2003

Jean-loup Gailly and Mark Adler

BSD License - Copyright (c) 1989, 1993

The Regents of the University of California.

All rights reserved.

SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Apache License

Version 2.0, January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

   "License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

   "Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

   "Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

   "You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

   "Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

   "Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

   "Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

   "Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

   "Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

   "Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License. Subject to the terms and conditions of this License, each

Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License. Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution. You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

(a) You must give any other recipients of the Work or Derivative Works a copy of this License; and

(b) You must cause any modified files to carry prominent notices stating that You changed the files; and

(c) You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and

(d) If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions. Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks. This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty. Unless required by applicable law or agreed to in writing, Licensor

provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability. In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability. While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

APPENDIX: How to apply the Apache License to your work.

To apply the Apache License to your work, attach the following boilerplate notice, with the fields enclosed by brackets "[]” replaced with your own identifying information. (Don't include the brackets!) The text should be enclosed in the appropriate comment syntax for the file format. We also recommend that a file or class name and description of purpose be included on the same "printed page" as the copyright notice for easier identification within third-party archives.

Copyright [yyyy] [name of copyright owner]

Licensed under the Apache License, Version 2.0 (the "License"); you may not use this file except in compliance with the License. You may obtain a copy of the License at

http://www.apache.org/licenses/LICENSE-2.0

Unless required by applicable law or agreed to in writing, software distributed under the License is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it. For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a freeprogram will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

GNU GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long

as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSEDOR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK ASTO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

GNU LESSER GENERAL PUBLIC LICENSE

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public Licenses are intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the library or if you modify it.

For example, if you distribute copies of the library, whether gratis or for a fee, you must give the recipients all the rights that we gave you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Finally, software patents pose a constant threat to the existence of any free program. We wish to make sure that a company cannot effectively restrict the users of a free program by obtaining a restrictive license from a patent holder. Therefore, we insist that any patent license obtained for a version of the library must be consistent with the full freedom of use specified in this license.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a" work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

GNU LESSER GENERAL PUBLIC LICENSE

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy inappropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not.

Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution.

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by

third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software, which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE

LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public

License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU

Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail. You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

<signature of Ty Coon>, 1 April 1990

Ty Coon, President of Vice

That's all there is to it!

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software, which everyone can redistribute, and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the program's name and a brief idea of what it does.>

Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of

MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'.

This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program
`Gnomovision' (which makes passes at compilers) written by James Hacker.

<signature of Ty Coon>, 1 April 1989
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.