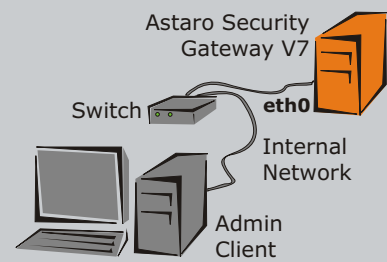


ASG - Minimum Hardware Requirements:

- ▶ Pentium II 500 MHz or compatible CPU
- ▶ 256 MB RAM
- ▶ 10 GB IDE or SCSI hard disk drive
- ▶ Bootable CD-ROM drive

Client - Hard-/Software Requirements:

- ▶ 1 GHz and 512 MB RAM
- ▶ Browser: Firefox recommended (<http://www.getfirefox.com/>) or Microsoft Internet Explorer 6 or 7
- ▶ WebAdmin is running at port 4444

1. Install the Software

Install the Astaro Security Gateway V7 Software on a separate host. The installation will completely erase all data on the hard disk including all programs and the operating system.

After the security system has rebooted (a process which, depending on hardware, can take up to five minutes), **ping** the IP address of the **eth0** interface to ensure it is reachable.

2. Start your Browser and open WebAdmin

Before you can access the **WebAdmin** interface, you will need to configure the *Admin Client* with the *LAN connection properties*. This properties can later be changed to the IP addresses used in the local network.

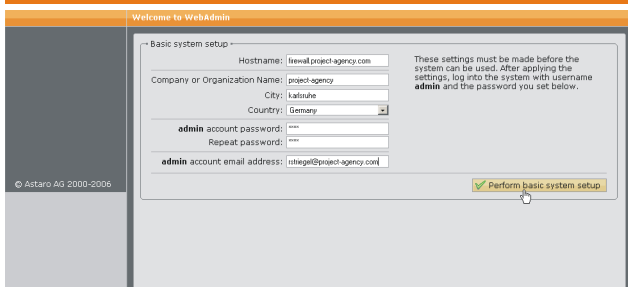
The filing position of the menu for these settings depends on the operating system of the client. Example: With Microsoft Windows XP the menu can be found under *Start/System Control/Network connections*.

**LAN connection properties:**

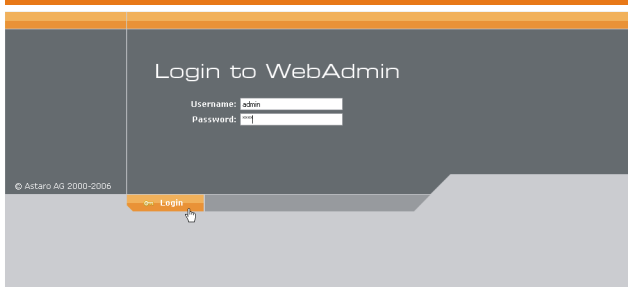
- IP Address:** Any address in the range 192.168.2.1 through 192.168.2.254 (192.168.2.100 excepted)
- Netmask:** Enter 255.255.255.0
- Standard Gateway:** Enter the IP address of the appliance's internal network card (eth0): 192.168.2.100
- DNS Server:** Enable this option and enter the IP address of the internal network card (eth0): 192.168.2.100

Admin Client

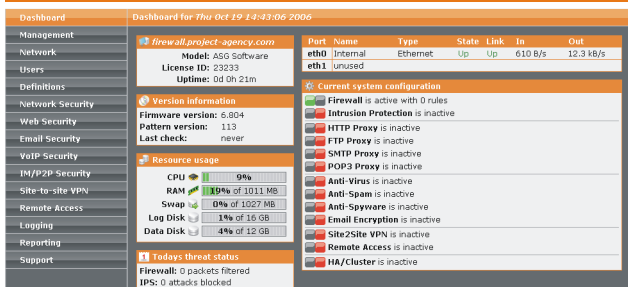
Once your browser is correctly configured, start it and enter the management address of the security system (the internal IP address configured for eth0) as follows:
https://IP Address:4444 (e.g., <https://192.168.2.100:4444>).

3. Enter the Administrator Contact and set the System Passwords

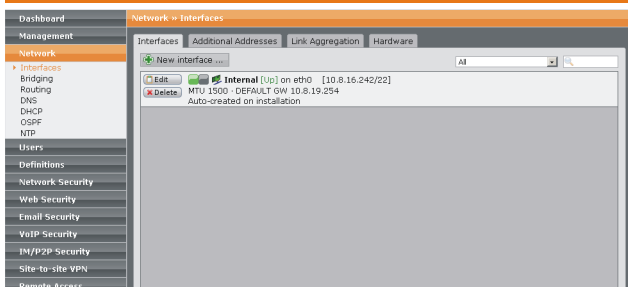
In the **Basic System Setup** window, enter the Administrator Contact and the passwords for the Astaro Security Gateway.

4. Log in to WebAdmin

Username: admin
Password: Password of the WebAdmin user

>> The Dashboard opens

The Dashboard graphically displays a snapshot of the current operating status of the firewall device.

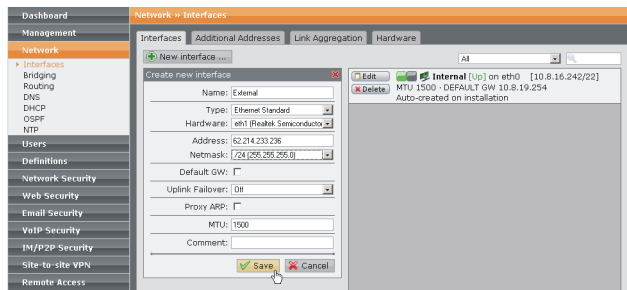
5. Configure the Internal Network (LAN) Interface (eth0)

In the **Network/Interfaces** directory, open the **Interfaces** tab and check the settings for **eth0 network card**.

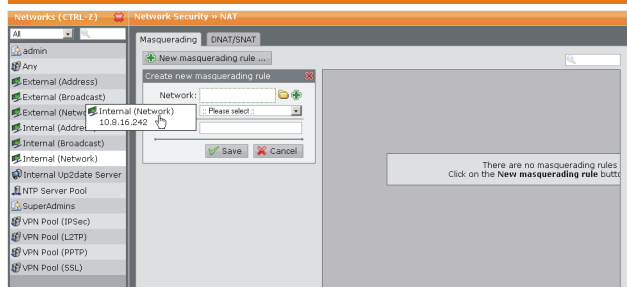
The settings for this network card are based on the information entered during the software installation.

6. Configure the Internal Network

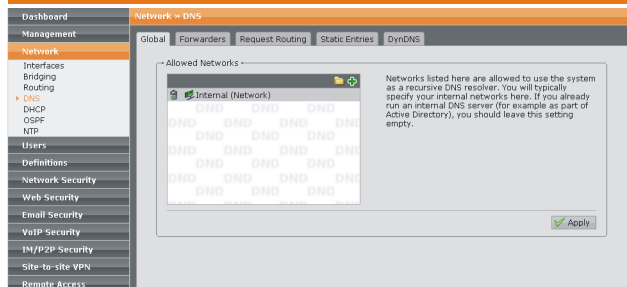
In the **Definitions** directory, open the **Networks** menu and check the settings for the internal network. Three logical networks were defined during installation based on your settings for the **internal network card (eth0)**.

7. Configure the External Interface (eth1)

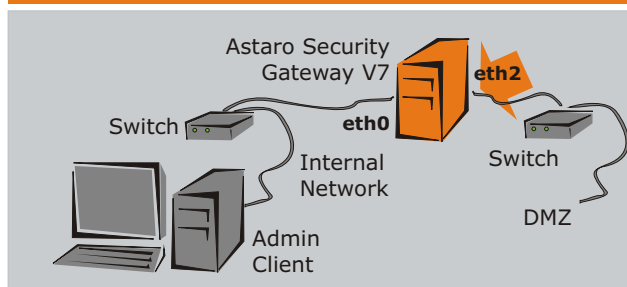
In the **Network** directory, open the **Interfaces** menu and configure the interface to be used to connect to the Internet. The choice of interface and the required configuration depend on what kind of connection to the Internet you will be using.

8. Define Masquerading Rules

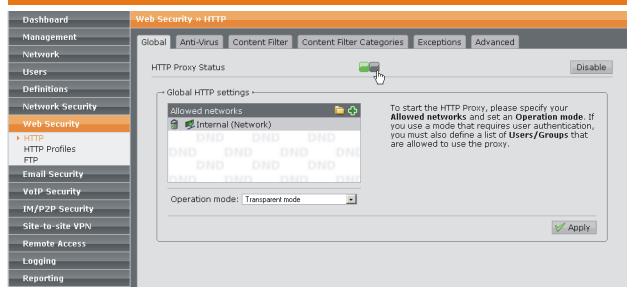
In the **Network Security/NAT** directory, open the **Masquerading** tab and configure the relevant rule. You need this setting, if you wish to use private IP addresses for your internal network and you wish to connect directly (without proxies) to the Internet.

9. Configure the DNS Proxy

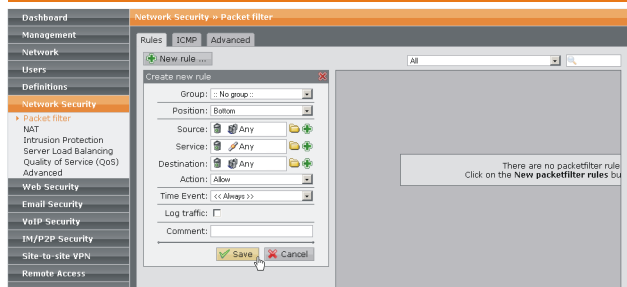
In the **Network/DNS** directory, open the **Global** tab and specify the internal networks to use the security system as a DNS resolver.

10. Connect other Networks

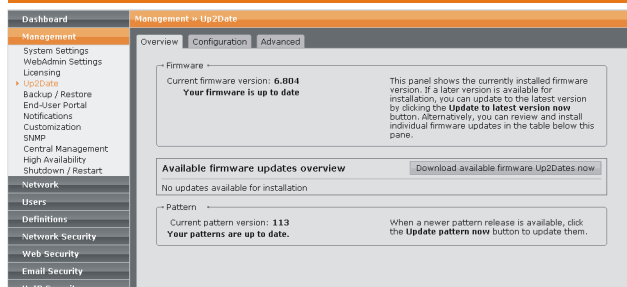
If you wish to connect other internal networks (e.g., DMZ) to the security system, attach their cables now.

11. Configure the HTTP Proxy

In the **Web Security** directory, open the **HTTP** menu and enable the proxy. In Transparent mode it isn't necessary to configure the browsers to allow the clients in the internal network to access the Internet by using the HTTP proxy.

12. Configure the Packet Filter

In the **Network Security/ Packet Filter** directory, open the **Rules** tab and establish the packet filtering rules. By default, all packets are filtered until you explicitly enable certain services.

13. Install System and Virus Scanner Updates

By default, the Firmware and Pattern Up2Dates will be downloaded automatically from the Up2Date server. To keep the system safe, please install a new Firmware Up2Date shortly after the download. Now, the initial configuration is complete.