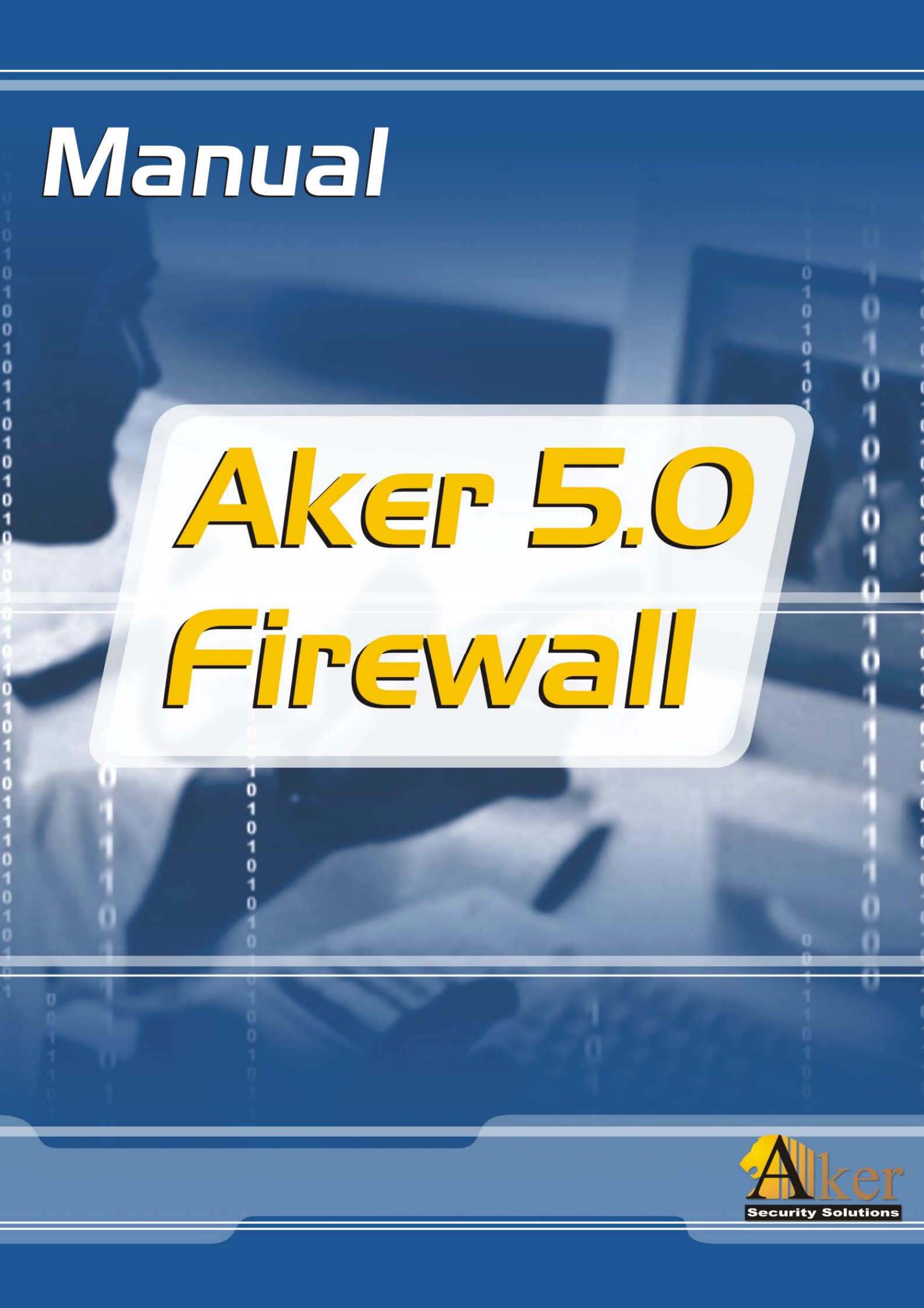
Manual

Aker 5.0 Firewall



Aker
Security Solutions

Aker Firewall

Version 5.0 Configuration Manual

- Introduction **– pág. 05**
- 1-0 Installing Aker Firewall **– pág. 07**
  - 1-1 Hardware and software requirements **– pág. 07**
  - 1-2 Installing the firewall **– pág. 10**
  - 1-3 Installing the remote interface on Windows platforms **– pág. 20**
- 2-0 Using the remote interface **– pág. 22**
  - 2-1 Starting the remote interface **– pág. 24**
  - 2-2 Finishing the remote management **– pág. 29**
  - 2-3 Configuring the interface parameters **– pág. 30**
  - 2-4 Changing your user's password **– pág. 31**
  - 2-5 Viewing session information **– pág. 32**
- 3-0 Managing firewall users **– pág. 33**
  - 3-1 Using the graphic user interface **– pág. 33**
  - 3-2 Using the command line interface **– pág. 37**
- 4-0 Configuring the system parameters **– pág. 41**
  - 4-1 Using the graphic user interface **– pág. 41**
  - 4-2 Using the command line interface **– pág. 49**
- 5-0 Registering entities **– pág. 51**
  - 5-1 Planning the installation **– pág. 51**
  - 5-2 Registering entities using the graphic user interface **– pág. 54**
  - 5-3 Using the command line interface**– pág. 75**
  - 5-4 Using the Entities Wizard**– pág. 79**
- 6-0 The Stateful Filter **– pág. 85**
  - 6-1 Planning the installation **– pág. 85**
  - 6-2 Editing a list of rules using the graphic user interface **– pág. 90**
  - 6-3 Working with filtering policies **– pág. 95**
  - 6-4 Using the command line interface **– pág. 99**
  - 6-5 Using the rules wizard **– pág. 102**
- 7-0 Configuring the Network Address Translation **– pág. 109**
  - 7-1 Planning the installation **– pág. 109**
  - 7-2 Using the graphic user interface **– pág. 117**
  - 7-3 Using the command line interface **– pág. 129**
  - 7-4 Using the NAT Configuration Wizard **– pág. 132**
- 8-0 Creating secure channels **– pág. 137**
  - 8-1 Planning the installation **– pág. 137**
  - 8-2 Aker-CDP certificates **– pág. 148**
  - 8-3 IPSEC certificates **– pág. 151**
  - 8-4 Configuring Firewall-Firewall channels **– pág. 154**
  - 8-5 Using the command line interface **– pág. 162**
- 9-0 Configuring Client-Firewall secure channels **– pág. 169**
  - 9-1 Planning the installation **– pág. 169**
  - 9-2 Configuring the firewall using the graphic user interface **– pág. 171**
  - 9-3 Configuring the firewall using the command line interface **– pág. 175**
  - 9-4 Installing Aker encryption client **– pág. 178**

    - 9-5 Configuring the encryption client **– pág. 180**
- 10-0 Integration of the firewall modules **– pág. 187**
    - 10-1 The flow of packets in the Aker Firewall **– pág. 187**
    - 10-2 Integration of the filter and the network address translation **– pág. 190**
    - 10-3 Integration of the filter with the network address translation and the encryption **– pág. 191**
- 11-0 Configuring the security **– pág. 192**
    - 11-1 Protection against SYN Flood **– pág. 192**
    - 11-2 Configuring SYN Flood protection through the GUI **– pág. 194**
    - 11-3 Flood protection **– pág. 196**
    - 11-4 Configuring Flood protection through the GUI **– pág. 197**
    - 11-5 Anti-Spoofing protection **– pág. 199**
    - 11-6 Configuring Anti-Spoofing protection from the GUI **– pág. 201**
    - 11-7 Intrusion detection system (IDS) **– pág. 203**
    - 11-8 Configuring support for intrusion detection agent **– pág. 204**
    - 11-9 Installing IDS agents plugin on Windows NT **– pág. 206**
    - 11-10 Using the command line interface - Syn Flood **– pág. 212**
    - 11-11 Using the command line interface - Flood protection **– pág. 214**
    - 11-12 Using the command line interface - Anti-Spoofing **– pág. 215**
    - 11-13 Using the command line interface - IDS **– pág. 216**
- 12-0 Configuring the system actions **– pág. 218**
    - 12-1 Using the graphic user interface **– pág. 218**
    - 12-2 Using the command line interface **– pág. 223**
- 13-0 Viewing the system log **– pág. 227**
    - 13-1 Using the graphic user interface **– pág. 228**
    - 13-2 Format and meaning of the fields of the log registers **– pág. 237**
    - 13-3 Using the command line interface **– pág. 241**
- 14-0 Viewing system events **– pág. 243**
    - 14-1 Using the graphic user interface **– pág. 244**
    - 14-2 Format and meaning of the fields of events messages **– pág. 250**
    - 14-3 Using the command line interface **– pág. 251**
- 15-0 Viewing statistics **– pág. 253**
    - 15-1 Using the graphic user interface **– pág. 254**
    - 15-2 Using the command line interface **– pág. 259**
- 16-0 Viewing and removing connections **– pág. 261**
    - 16-1 Using the graphic user interface **– pág. 261**
    - 16-2 Using the command line interface **– pág. 266**
- 17-0 Working with proxies **– pág. 268**
    - 17-1 Planning the installation **– pág. 268**
    - 17-2 Installing the authentication agent on Unix platforms **– pág.273**
    - 17-3 Installing the authentication agent on Windows NT **– pág. 276**
- 18-0 Configuring the authentication parameters **– pág. 281**
    - 18-1 Using the graphic user interface **– pág. 281**
    - 18-2 Using the command line interface **– pág. 288**
- 19-0 User access profiles **– pág. 290**
    - 19-1 Planning the installation **– pág. 290**
    - 19-2 Creating access profiles **– pág. 291**
    - 19-3 Assigning access profiles to users **– pág. 300**
- 20-0 Aker authentication client **– pág. 304**

    - 20-1 Planning the installation **– pág. 304**
    - 20-2 Installing Aker authentication client **– pág. 305**
    - 20-3 Configuring the authentication client **– pág. 307**
    - 20-4 Viewing and removing users logged in the firewall **– pág. 314**
    - 20-5 Using the command line interface **– pág. 317**
- 21-0 Configuring the SMTP proxy **– pág. 318**
    - 21-1 Configuring the parameters of a SMTP context **– pág. 320**
- 22-0 Configuring the Telnet proxy **– pág. 335**
    - 22-1 Configuring the parameters of a Telnet context **– pág. 336**
- 23-0 Configuring the FTP proxy **– pág. 339**
    - 23-1 Configuring the parameters of a FTP context **– pág. 340**
- 24-0 Configuring the POP3 proxy **– pág. 342**
    - 24-1 Configuring the parameters of a POP3 context **– pág. 343**
- 25-0 Configuring the WWW proxy **– pág. 347**
    - 25-1 Planning the installation **– pág. 347**
    - 25-2 Editing the parameters of the WWW proxy **– pág. 350**
- 26-0 Configuring the SOCKS proxy **– pág. 358**
    - 26-1 Planning the installation **– pág. 358**
    - 26-2 Editing the parameters of the SOCKS proxy **– pág. 359**
- 27-0 Using the GUI tools **– pág. 361**
    - 27-1 Activation keys **– pág. 361**
    - 27-2 Saving configurations **– pág. 363**
    - 27-3 Restoring configurations **– pág. 365**
    - 27-4 Reverse DNS **– pág. 367**
    - 27-5 Date and Time **– pág. 369**
    - 27-6 Filtering rules simulation **– pág. 371**
    - 27-7 Reports **– pág. 374**
    - 27-8 Patches and Updates **– pág. 376**
    - 27-9 TCP/IP configuration **– pág. 378**
    - 27-10 Rebooting the firewall **– pág. 382**
    - 27-11 Entity search **– pág. 383**
    - 27-12 Alarm window **– pág. 385**
    - 27-13 Using the command line interface for TCP/IP configuration **– pág. 387**
    - 27-14 Using the command line interface for activation keys **– pág. 393**
- 28-0 Configuring the Firewall in cluster **– pág. 395**
    - 28-1 Planning the installation **– pág. 395**
    - 28-2 Using the command line interface **– pág. 397**
- 29-0 System files and backups **– pág. 400**
    - 29-1 System files **– pág. 400**
    - 29-2 Firewall Backup **– pág. 405**
- 30-0 Aker Firewall Box **– pág. 407**
- Appendix A - System Messages **– pág. 410**
    - Firewall log messages **– pág. 410**
    - Firewall event messages **– pág. 416**
- Appendix B - Questions and answers **– pág. 437**
- Appendix C - Copyrights and Disclaimers **– pág. 440**
- Appendix D - What's new in version 5.0 **– pág. 445**

Introduction

This is the User's Manual of Aker Firewall version 5.0. In the following chapters you will learn how to configure this powerful network protection tool. This introduction will help you to use this manual efficiently.

Manual's arrangement

This manual consists of several chapters. Each chapter shows one aspect of the configuration of the product and all information relevant information to it.

Every chapter starts with a theoretical introduction followed by the specific aspects of the Aker Firewall configuration. Some of the chapters also contain practical examples (hypothetical situations, but very close to the reality) of the use of the service to be configured, which makes the understanding of the various configurations easier.

We recommend you to read this manual thoroughly at least once, in the given order. Afterwards, if necessary, it can be used as reference. In order to make the use of this manual as reference easier, the chapters are divided in sections which can be accessed through the main index. This way, the desired information can be easily found).

Sometimes the symbol  will be shown and followed by a sentence written in red. This means that the sentence is an important remark and must be fully understood before further reading.

Command Line Interface vs. Graphic User Interface

Aker Firewall has two different configuration interfaces: a remote graphic user interface and a local command line interface.

- Graphic user interface

  The graphic user interface is called remote because it is possible to remotely administrate an Aker Firewall located anywhere in the world, via local network or via the Internet. This administration is done through a secure channel between the interface and the Firewall, with strong authentication and encryption algorithms, in order to make it totally secure.

  The graphic user interface is available for Windows 95™, Windows 98™, Windows NT™ and Windows 2000™, Windows XP™, Linux and FreeBSD platforms.

- Command line interface

The command line interface runs only on the host where the Firewall is installed. Its basic purpose is to make the automation of the Aker Firewall's tasks possible (through the creation of scripts).

Almost all the variables configured through the graphic user interface can also be configured through the command line interface. The only exception to this rule is the proxies configuration that cannot be done through the command line interface.

As the two interfaces work with the same variables, their functionality, values and comments are valid for both the graphic and the command line interface. Therefore, the sections that refer to the command line interface usually will be short and limited to its functionality.

 The simultaneous use of many graphic user interfaces for the same firewall is not allowed. The use of a command line interface when a remote interface is being used is not allowed either.

System Copyrights

1-0 Installing Aker Firewall

This chapter shows all the steps and requirements necessary to install Aker Firewall.

1-1 Hardware and software requirements

Firewall

Aker Firewall 5.0 runs on Linux (Red Hat 7.3 and Conectiva 9) and FreeBSD versions 4.7 and 4.9 operating systems on Intel or compatible platforms. Due to the fact that both Linux and FreeBSD systems are royalty free, they are distributed with the installation media of Aker Firewall. This way, all the software necessary to run the firewall is already included in it. It is not necessary to buy any other extra software.

In relation to the hardware, the following list is mandatory (all components of the hardware must be supported by FreeBSD or by Linux, in one of the supported versions):

- Pentium or compatible computer 200 Mhz or superior

If a high transfer rate link is used or if you want to use encryption in a relatively high speed link, you may need a faster computer.

- 128 Mbytes of RAM

If it's intended to use a large number of proxy-based services, 256 Mbytes or even more will probably be necessary.

- 4 Gbytes of disk space

A larger disk may be necessary if the system log is intended to be stored for a long period of time.

- CD-ROM reader, monitor, mouse and keyboard

These are necessary only during the installation, however, they are highly recommended in all cases.

- Network Adapter(s)

There is no maximum number for network adapters that can be installed in the Firewall. The only limit is imposed by hardware. If a large number of network interfaces is required, adapters with more than one port can be used.

It is important to emphasize that all the hardware devices must be supported by FreeBSD or Linux. Before getting any devices, it is necessary to verify that one of these operating systems, in the versions supported by Aker Firewall, accepts such device.

For further information about the Linux or FreeBSD operating systems or to check if a device is supported by them or not, we suggest that you contact one of the following addresses:

- WWW

  - http://www.freebsd.org (FreeBSD)
  http://www.linux.org (Linux)
  http://www.kernel.org (Linux)
  http://www.redhat.com (Linux)

- E-Mail

questions@freebsd.org (FreeBSD discussion list)

Aker Security Solutions does not take any responsibility for any configuration, operation, compatibility or information problems related to the Linux or FreeBSD operating systems.

Graphic User Interface

The graphic user interface of Aker Firewall runs on Windows 95 or superior, Linux Red Hat 7.3, 8 and 9 and Conectiva 8 and 9; FreeBSD versions 4.7 and 4.9, on Intel or compatible platforms.

In relation to the hardware, the following list is mandatory (all components of the hardware must be supported by the operating system which the interface will be installed on, in one of the product supported versions):

- Pentium II or compatible computer 450 Mhz or superior
- 128 Mbytes of RAM
- 4 Gbytes of disc space
- Monitor
- Mouse
- Keyboard
- Network adapter

Remote log server

The graphic user interface of Aker Firewall runs on Windows 95 or superior, Linux Red Hat 7.3, 8 and 9 and Conectiva 8 and 9; FreeBSD versions 4.7 and 4.9, on Intel or compatible platforms.

In relation to the hardware, the following list is mandatory (all components of the hardware must be supported by the operating system which the interface will be installed on, in one of the product supported versions):

- Pentium III or compatible computer 1 Ghz or superior
- Storage system with speed equal or superior to an Ultra-ATA 66

- 64 Mbytes of RAM (128 Mbytes is highly recommended)
- 40 Gbytes of disc space
- Monitor
- Mouse
- Keyboard
- Network adapter

1-2 Installing the firewall

Aker Firewall can be sold in appliances. This way, the product is already installed and previously configured. If you choose to buy only the software, however, you have to install the firewall in the chosen machine. This will be explained in this section.

In order to install the Aker Firewall, the Linux or FreeBSD operating systems must be installed first. The installation of both are simple, however, we recommend that it's done by a person who has basic Unix operating system knowledge. The FreeBSD and Linux installation procedures are on their CD-ROMs. If there are any problems, we suggest that you contact any one of the addresses mentioned above for more information.

After FreeBSD or Linux is installed, in order to install Aker Firewall, you need to mount the installation CD-ROM in the target machine or copy the contents from the installation directory on the CD-ROM to any temporary directory in the machine you want to install the product. It is possible to copy it via FTP or NFS, in case you do not have a CD-ROM reader in the machine the product will be installed.

After mounting the CD-ROM or copying the files to any directory, you need to run the following command:

#*/installation_directory*/en/aker/*platform*/fwinst

The *installation_directory* is the directory where the installation files are stored and *platform* is the platform where the firewall will be installed on. For instance, if the CD-ROM was mounted in the directory `/cdrom` and the installation would be done on FreeBSD, the command to be typed would be: `/cdrom/en/aker/freebsd/fwinst`

The symbol # stands for the shell prompt while you are logged as root. Do not type it as part of the command.

Installing the Firewall in FreeBSD operating system

The **fwinst** program is responsible for the installation and configuration of the system to run Aker Firewall. When it is run, the following screen will be shown:

```
                Aker Firewall v5 - Installation Program

This program installs the Aker Firewall 5 and the command line
interface.

The installation can be made from a precompiled kernel supplied with
the
the firewall, it's possible to compile a specific kernel for this
machine or
to use the kernel currently installed (provided version 5 or superior
has been previously installed). The precompiled kernel has support for
3 ISA
network adapters and an unlimited number of PCI adapters. For more
information
```

```
on which cards are supported, which are their I/O and IRQ
configurations and
how to change these values, please refer to the product documentation.

If you want to compile a specific kernel, before running this program
it's
necessary to create a kernel configuration file called FIREWALL. This
file must
be located in the /usr/src/sys/i386/conf directory.

Do you want to proceed with the firewall installation (Y/N) ?
```

If the kernel configuration file named FIREWALL has already been created or the precompiled or currente kernels will be used, you should answer **Y** and then **Enter** to continue with the installation. If you want to compile a new kernel and this file has not been created, you must type **N** and create it, before continuing.

In case of compilation of a new kernel, there is a file named `FIREWALL`, in the installation directory, which can be used as base to generate the customized file, just by copying it to the `/usr/src/sys/i386/conf` directory and removing or adding the desired components. For more information about this file, consult the FreeBSD documentation.

 If Aker Firewall installation was performed using the pre-compiled kernel, it will be configured to support up to 10 (ten) VLANs, through 802.1q protocol. VLANs configuration can be done later using the graphic user interface. For more information refer to section TCP/IP configuration .

When you answer Yes to this question, the program will show the Aker Firewall license agreement . In order to proceed with the installation, it is necessary to accept the terms and conditions specified in the license. If they are accepted, the program will continue the installation showing the following screen:

```
                Aker Firewall v5 - Installation Program

Starting the installation:

Do you want to use the (P)recompiled kernel, (C)ompile a new one or
use the
(K)ernel currently installed for the firewall installation ? (P/C/K)
```

If you want to use the precompiled kernel, just type **P** followed by **Enter**. If you want to use the current kernel, type **K**. Otherwise, type **C**.

 The use of precompiled kernel is recomended, specially if nobody has previous experience with FreeBSD. The only need to compile a new kernel is to to generate a more optimized version of it.

 It's only possible to use the current kernel if Aker Firewall 5.0 has been installed previously. Otherwise, one of the other two options must be choosen.

Independently of the chosen option, the program will start the installation. It will show the progress through a serie of self-explained messages.

 You must be aware of the fact that the installation program replaces the file **`/etc/rc`**. If changes have been made to this file, it is necessary to perform them again after the installation.

After copying the files, the installation program will ask for information required to perform the system-dependent configuration. First, it will ask for the product activation key. No firewall module will work without this key.

The following screen will be displayed:

```
                Aker Firewall v5 - Installation Program

System configuration completed. It's now necessary to activate the
installed copy by typing the activation key that came with the product.

The activation key, the company name and the IP address of the external
interface must be typed exactly as they appear in the document
provided
by the Aker Security Solutions or its authorized dealer.

Press enter to continue
```

After pressing enter, the program will show a screen asking to type the information contained in the document provided by Aker Security Solutions or by its authorized sales representative. All fields must be typed exactly as they appear in the document.

 The key must be typed with the hyphens '-' that appear in the original document. In the company name, capital and small letters are considered different and must be typed exactly how they are in the original document.

The screen below demonstrates an example of data entry:

```
                    Aker Firewall version 5
                Activation key configuration module
```

```
Company name: Aker Security Solutions
External interface IP address: 10.0.0.1
Activation key: 2DBDC612-FA4519AA-BBCD0FF1-129768D3-89BCA59C
```

If the key is valid, the program will proceed with the installation. If the key or the name of the company contains typing errors, the program will ask you to type them again.

The IP address typed must have been previously assigned to an interface of the system, otherwise, the program will not go on with the installation.

If the key is accepted, the installation will go on. At this point, the installation program will search for configuration files of version 4.50 of Aker Firewall. If any of these files are found, the following screen will be shown:

```
                Aker Firewall v5 - Installation Program

Updating configuration files of the version 4.50 of Aker Firewall...

Updating messages and parameters... OK
Updating entities... OK
Updating filtering rules... OK
Updating secure channels configuration... OK
Updating network address translation... OK
Updating SMTP contexts... OK
Updating access profiles... OK
Updating authentication parameters
Updating HTTP parameters... OK
Updating SYN Flood protection... OK
Updating client encryption... OK

Update complete. The version 4.50 configuration files were removed
from the
system.

Press enter to continue
```

The files updating is done automatically and the existing configuration will be kept unaltered. After it is performed, the original files will be removed from the system and the following screen will be displayed:

```
                Firewall Aker v5 - Installation program

Creating standard services and rules... OK

Would you like to allow ICMP ping packets for diagnosis purposes?
```

If this question is answered negatively, the firewall will be installed with a deny-all policy, that is, all network traffic will be blocked, except for the traffic used for the remote administration. After this question is answered, another screen will be shown:

```
                Firewall Aker v5 - Installation Program

It's necessary to define the name of the Firewall external interface.
The IP addresses originated from this interface will not be counted in
the
maximum number of licenses.

The external interface must be set to one of the following values:

fxp0
fxp1
de0

Enter the external interface:
```

The external interface configuration is used only for firewall license control purposes. It must be informed the name of the firewall interface that will be connected to the Internet.

 The specification of the external interface does not have any security implication. Absolutely no access control is performed based on this interface.

```
                Aker Firewall v5 - Installation Program

System activation completed. Now let's configure some Aker Firewall
parameters.

I can automatically create an administrator capable of managing
remotely
the firewall. This administrator will have full administrative rights
and
new users can be registered by him later.

If you don't create an administrator, you won't be able to manage the
firewall using the remote graphic user interface. The only way to
manage
it will be through the command line interface.

Do you want to create the administrator (Y/N) ?
```

In order to manage the firewall from the graphic user interface, it is necessary to register an administrator, answering **Y** to this question.

It is possible to register other administrators afterwards through the local management interface. For further details refer to the chapter Managing firewall users.

If you choose to add a new administrator, a screen asking for the data of administrator to be registered will be shown. An example of such screen is shown below (be aware that the administrator's password will not be displayed):

```
                    Aker Firewall version 5
                Remote users administration module
                        User creation

Enter the login          : administrator
Enter the complete name : Aker Firewall administrator
Enter the password       :
Confirm the password     :



                      Create user ? (Y/N)
```

After adding or not the administrator, and if you chose to compile a new kernel, the installation program will show the a screen informing that it will start compiling a new kernel for the firewall, based on the kernel configuration file called **/usr/src/sys/i386/conf/FIREWALL.**

```
              Aker Firewall v5 - Installation Program

I will now compile a new kernel to install Aker Firewall on this
host. This compilation takes between 5 and 40 minutes, depending on
your configuration and the speed of this machine.

Press enter to continue
```

When you press enter, the program will start compiling the new kernel. After compiling and installing this new kernel, the program will ask you to restart the machine to activate the Aker Firewall. When the machine is restarted, the firewall will automatically start its operation.

Installing the Firewall on Linux operating system

The **fwinst** program is responsible for the installation and configuration of the system to run Aker Firewall. When it is run, the following screen will be shown:

```
                Aker Firewall v5 - Installation Program

This program installs the Aker Firewall 5 and the command line
interface.

Aker Firewall 5 can be installed in the kernel distributed with Red
Hat
Linux 7.3 or Conectiva 8 and 9. Because of that, it's not necessary to
recompile the kernel.

Do you want to proceed with the firewall installation (Y/N) ?
```

When you answer Yes to this question, the program will show the Aker Firewall license agreement . In order to proceed with the installation, it is necessary to accept the terms and conditions specified in the license. If they are accepted, the program will continue the installation, showing its progress through a serie of self-explained messages.

After copying the files, the installation program will ask for information required to perform the system-dependent configuration. First, it will ask for the product activation key. No firewall module will work without this key.

The following screen will be displayed:

```
                Aker Firewall v5 - Installation Program

System configuration completed. It's now necessary to activate the
installed copy by typing the activation key that came with the product.

The activation key, the company name and the IP address of the external
interface must be typed exactly as they appear in the document
provided
by the Aker Security Solutions or its authorized dealer.

Press enter to continue
```

After pressing enter, the program will show a screen asking to type the information contained in the document provided by Aker Security Solutions or by its authorized sales representative. All fields must be typed exactly as they appear in the document.

The key must be typed with the hyphens '-' that appear in the original document. In the company name, capital and small letters are considered different and must be typed exactly how they are in the original document.

The screen below demonstrates an example of data entry:

```
                    Aker Firewall version 5
                Activation key configuration module

Company name: Aker Security Solutions
External interface IP address: 10.0.0.1
Activation key: 2DBDC612-FA4519AA-BBCD0FF1-129768D3-89BCA59C
```

If the key is valid, the program will proceed with the installation. If the key or the name of the company contains typing errors, the program will ask you to type them again.

The IP address typed must have been previously assigned to an interface of the system, otherwise, the program will not go on with the installation.

If the key is accepted, the installation will go on. At this point, the installation program will search for configuration files of the version 4.5 of Aker Firewall. If any of these files are found, the following screen will be shown:

```
              Aker Firewall v5 - Installation Program

Updating configuration files of the version 4.50 of Aker Firewall...

Updating messages and parameters... OK
Updating entities... OK
Updating filtering rules... OK
Updating secure channels configuration... OK
Updating network address translation... OK
Updating SMTP contexts... OK
Updating access profiles... OK
Updating authentication parameters... OK
Updating HTTP parameters... OK
Updating SYN Flood protection... OK
Updating client encryption... OK

Update complete. The version 4.50 configuration files were removed
from the
system.

Press enter to continue
```

The files updating is done automatically and the existing configuration will be kept unaltered. After it is performed, the original files will be removed from the system and the following screen will be displayed:

```
                Firewall Aker v5 - Installation program

Creating standard services and rules... OK

Would you like to allow ICMP ping packets for diagnosis purposes?
```

If this question is answered negatively, the firewall will be installed with a deny-all policy, that is, all network traffic will be blocked, except for the traffic used for the remote administration. After this question is answered, another screen will be shown:

```
                Firewall Aker v5 - Installation Program

It's necessary to define the name of the Firewall external interface.
The IP addresses originated from this interface will not be counted in
the
maximum number of licenses.

The external interface must be set to one of the following values:

eth0
eth1
eth2

Enter the external interface:
```

The external interface configuration is used only for firewall license control purposes. It must be informed the name of the firewall interface that will be connected to the Internet.


The specification of the external interface does not have any security implication. Absolutely no access control is performed based on this interface.

```
                Aker Firewall v5 - Installation Program

System activation completed. Now let's configure some Aker Firewall
parameters.

I can automatically create an administrator capable of managing
remotely
```

```
the firewall. This administrator will have full administrative rights
and
new users can be registered by him later.

If you don't create an administrator, you won't be able to manage the
firewall using the remote graphic user interface. The only way to
manage
it will be through the command line interface.

Do you want to create the administrator (Y/N) ?
```

In order to manage the firewall from the graphic user interface, it is necessary to register an administrator, answering **Y** to this question.

It is possible to register other administrators afterwards through the local management interface. For further details refer to the chapter Managing firewall users.

If you choose to add a new administrator, a screen asking for the data of administrator to be registered will be shown. An example of such screen is shown below (be aware that the administrator's password will not be displayed):

```
                    Aker Firewall version 5
                Remote users administration module
                        User creation

Enter the login         : administrator
Enter the complete name : Aker Firewall administrator
Enter the password      :
Confirm the password    :



                      Create user ? (Y/N)
```

After adding or not the administrador, a message indicating the installation is complete and asking you to restart the machine to activate Aker Firewal will be shown. When the machine is restarted, the firewall will automatically start its operation.

1-3 Installing the remote interface

On Windows Platforms

In order to install the remote interface on the Windows 95, 98, Me, NT, 2000 or XP platforms, you must insert the CD-ROM in the drive and follow the instructions that will appear in the screen.

If the autorun option is disabled, then it is necessary to take the following steps:

1. Click on the **Start** menu
2. Select the option **Run**
3. When you are asked about which program to run, type ***D:\en\firewall\gui\install.*** (If the CD-ROM reader is accessed through a letter different from **D**, substitute this letter with the correct one in the previous command).

The remote interface installation screen will be displayed. To proceed, follow the instructions presented on the screen.

When the installation is completed, a group called **Aker** will be created in the **Start** menu. Select the option **Firewall 5.0 GUI** inside this group in order to start the remote interface.

On Linux platforms

To install the remote interface on Linux platforms, it is necessary that QT library packages are previously installed.

The graphic user interface for Linux platforms is distributed in RPM packages. To install it, proceed as follows:

1. Insert the CD-ROM in the drive and mount it using the command **`mount /mnt/cdrom`**
2. Run the command: **`rpm -ivh /mnt/cdrom/en/firewall/gui/fwgui-br-linux-5.0_1.rpm`**
3. When the prompt returns the interface will be installed.

 The name of the package to be installed may change according to the version of Linux where the interface will be installed on. Check the contents of **`/mnt/cdrom/en/firewall/gui/`** directory in order to take a look on all package names and select the most adequate.

On FreeBSD platforms

To install the remote interface on FreeBSD platforms, it is necessary that QT library packages are previously installed.

The graphic user interface for FreeBSD platforms is distributed in tbz packages. To install it, proceed as follows:

1. Insert the CD-ROM in the drive and mount it using the command **`mount /cdrom`**
2. Run the command: **`pkg_add /cdrom/en/firewall/gui/fwgui-br-freebsd49-5.0_1.rpm`**
3. When the prompt returns the interface will be installed.

 The name of the package to be installed may change according to the version of FreeBSD where the interface will be installed on. Check the contents of **`/cdrom/en/firewall/gui/`** directory in order to take a look on all package names and select the most adequate.

2-0 Using the Remote Interface

This chapter shows how the Aker Firewall remote graphic user interface works.

What is the Aker Firewall remote management ?

Aker Firewall can be entirely configured and managed remotely from any host that has an operating system compatible with one of the remote interface versions, has the TCP/IP protocol and can access the host where the firewall is running. This allows a high level of flexibility and management facility. Moreover, it makes it possible for an administrator to monitor and configure many firewalls from his workstation.

Besides, the remote management allows resource saving, because it is not necessary for the host running the firewall to have a monitor and other devices.

How does Aker Firewal remote management work ?

To allow the remote management, there is a process running in the firewall host that is responsible for receiving the connections, validating users and performing the tasks requested by these users. When a user starts a remote management session, the graphic user interface connects to the remote management module and keeps the connection open until the user finishes the session.

All communication between the remote interface and the firewall is done in a secure channel, where encryption and authentication are used. For each session, different encryption and authentication keys are generated. Besides, additional security measures are used to prevent other kinds of attacks such as the packet repetition.

There are some important remarks about the remote management that should be made:

1. For the remote interface to be able to connect to the firewall, it is necessary to add a rule allowing **TCP** access to the port **1020**, from the host where it is running. Information about how to do this is in the chapter called The Stateful Filter.
2. It's only possible to open one administration connection at a certain time. If there is an interface already connected, subsequent connections requests will be refused and the remote interfaces will inform that there is already an active administration session established.
3. Each user that will operate the remote interface must be registered in the system. The installation program can automatically create an administrator with powers to register the other administrators. If this administrator has been deleted or its password lost, it is necessary to use the local command line interface module to create a new administrator. More details can be found in the chapter called Managing Firewall Users.

How to use the Windows interface

The interface is simple to use, however, it might be useful to know that:

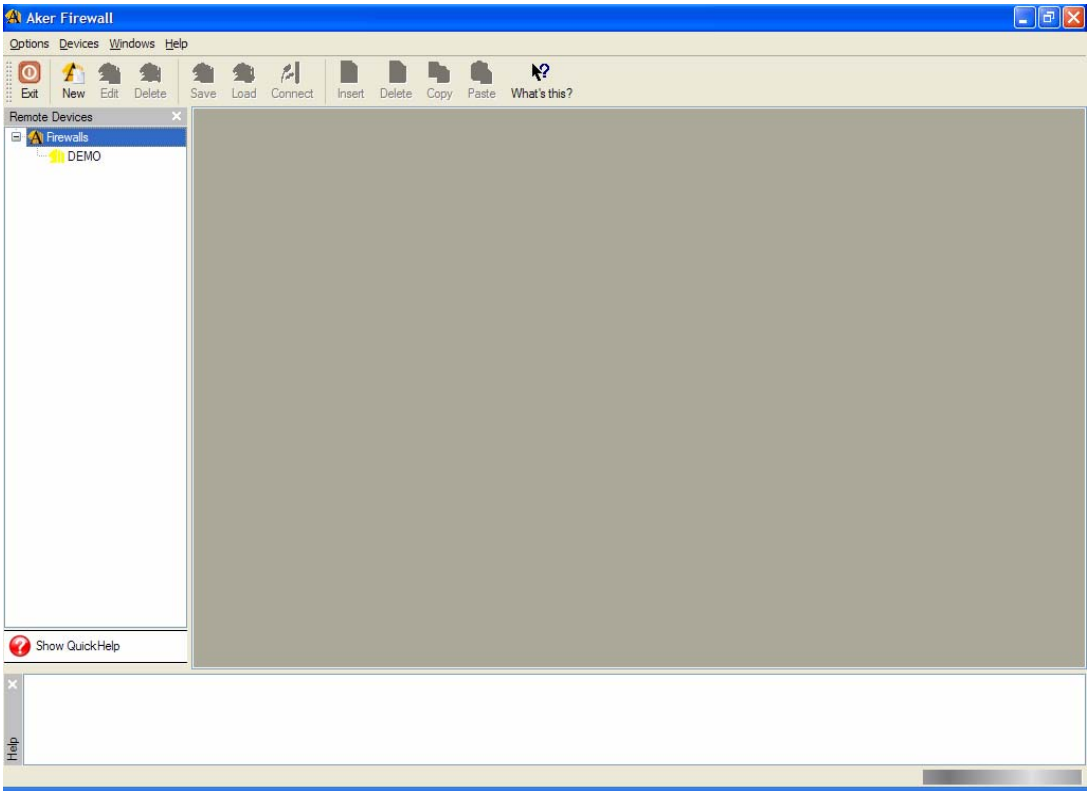
The left and right buttons of the mouse have different functions in the interface. The left button is used to select entries in a list and to click buttons. The right button shows the pop-up menu for certain lists. Most of the options that appear on the pop-up menu are also available in the toolbar at the top of the windows.

2-1 Starting the remote interface

To start the graphic user interface you must take the following steps:

- On Windows boxes, click on the **Start** menu, select **Aker** group, inside this group, select **Firewall 5.0 GUI** group and then click on the **Aker Firewall 5.0** icon.
- On FreeBSD or Linux, run the command '`fwgui`' from the shell prompt or click on the icon created on the desktop (KDE only).

The following window will be shown:



The window displayed above is the Aker Firewall main window. All the configuration options are accessed from it. It consists of 4 menus, described briefly below:

- **Options**

The *Options* menu contains all configuration related to the layout of the graphic user interface. When it is selected, the following options will be shown (when a firewall is selected, a fifth menu is displayed, with options specific for the selected firewall):

- Buttons labels: if this option is enabled, the action corresponding to each button will be shown beneath the icon. If it is disabled, only the icon will be displayed.

- Tooltips for entities: when this option is enabled a small box with the description of each entity will be displayed when the mouse is scrolled over its icon, like the picture below:

- Quickhelp: this option activates the automatic contextual help for each window.

- Show icons on push buttons: this option, if enabled, causes the interface to display icons on push buttons of all windows.

- Exit: closes the application.

- **Windows**

  This menu has the options for the configuration of open windows and system toolbar.

  - Toolbars: this option selects if the toolbar in the superior part of the main window will be displayed or not.

  - Windows: this option selects if the standard windows, *help*, *firewalls* and *entities* will be displayed or not.

  - Tile: if this option is chosen, the right open windows of the graphic user interface will be resized in order to keep all visible.

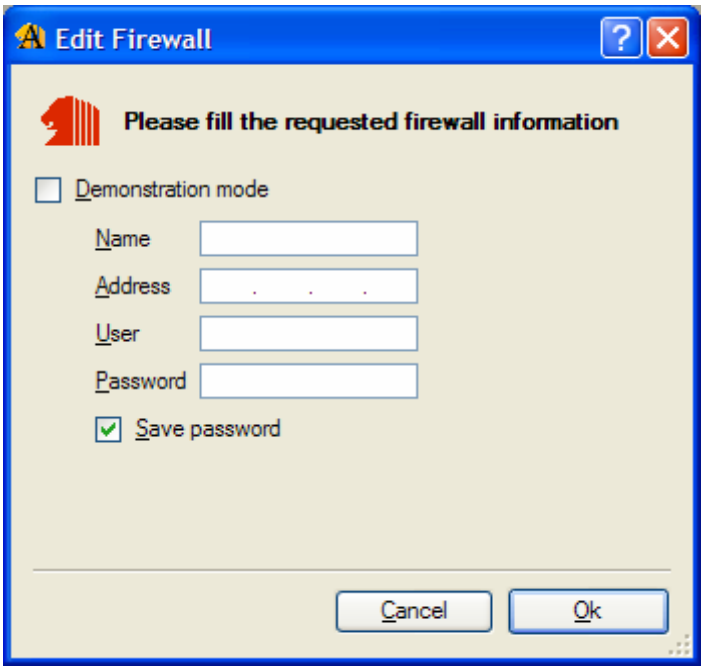
  - Cascade: if this option is chosen, the right open windows of the graphic user interface will be positioned in a cascade form, one over the other.

Initially, not all options in the menus are enabled, for they are work only one a connection is established. To access all options, it is necessary to establish a remote management session with the firewall you want to administrate. Therefore, you must follow these steps:

- Create the firewall, selecting *Firewalls* menu and *New Firewall* option (take a look in the Creating Firewalls section down below)
- Select the firewall which you want to connect to
- Click on the *Connect* option

Registering Firewalls

In this section it will be shown how to register one (or more) firewalls. When the option *New Firewall* is selected, inside the *Firewalls* menu or when the icon "*New Firewall*"  on the toolbar is clicked, the following window will be displayed:



- **Demonstration mode**: if this option is checked, a demo firewall with the default configuration will be created. No real connection will be performed when you try to connect to this firewall and it is possible to create many different demo firewalls, each one with a distinct configuration;

- **Name**: this field is used to define a name by which the firewall will be referred by the interface;

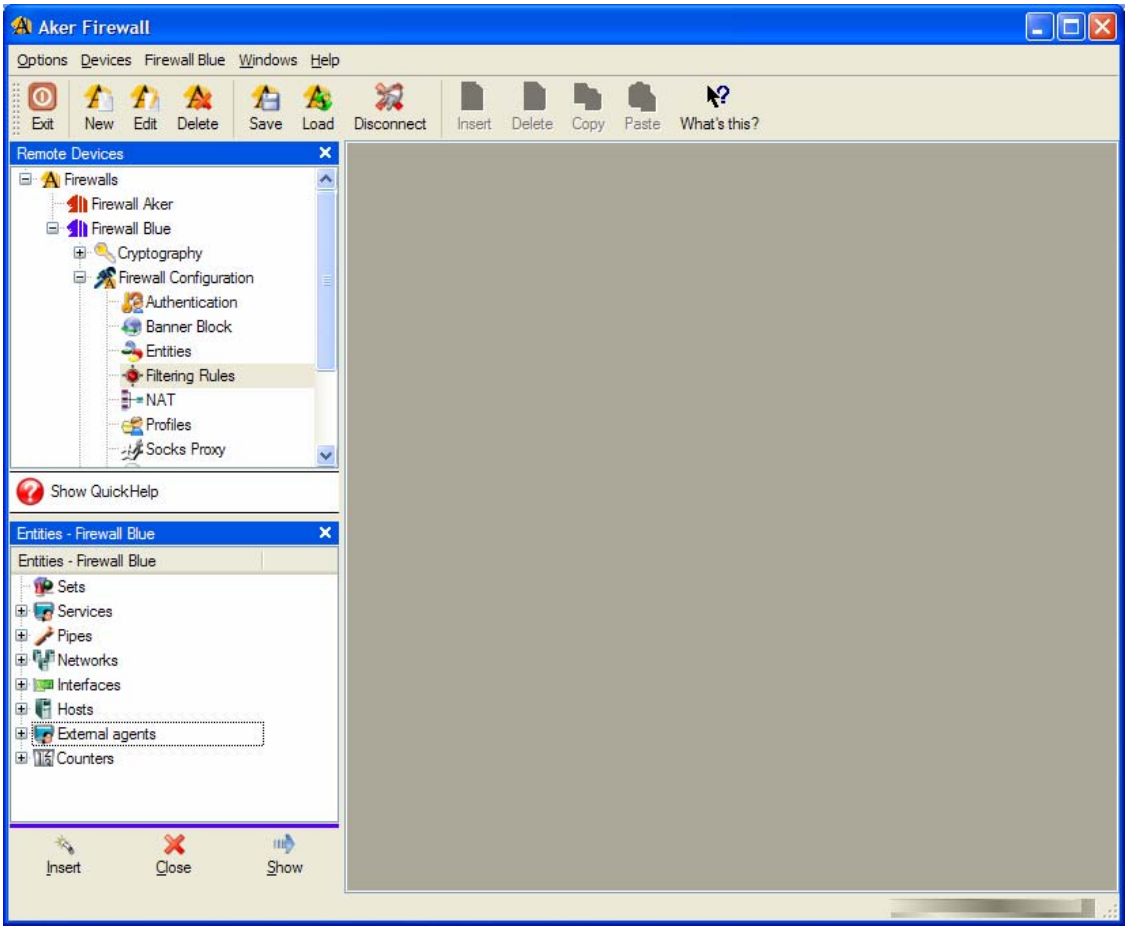
- **Address**: this field specifies the IP address used to connect to the firewall;

- **User**: the user that will manage the firewall. This field is useful because no longer will be necessary to specify the user when it is necessary to connect to the firewall.

- **Password**: the user's password. If the *Save password* option is checked, it won't be necessary to type in the password every time a connection is made. If this option is not set, this field will be disabled.

After all information is supplied, it is enough to click on **Ok** and the firewall will be registered. If the firewall creation is not desired, just click on **Cancel**.

When the firewall is registered, it is possible to double click on the firewall icon, at the left side of the window, or click once to select it and then on the *Connect* button  to cause the interface to connect to the chosen firewall, as in the picture below:



If it is not possible to establish the management session, a window showing the error will be displayed. In this case, there are many possible messages. Below is a list of the most common error messages:

- Aker is being administrated by another interface

Aker Firewall allows only one management session at a time. If this message is shown, it means that there is either another remote interface connected or a local management module being used.

- Network error or connection closed by the server

This is a general error and may have many causes. The most common reason is a typing mistake of the login or the password. If the user's login is not registered or his password is wrong, the server will close the connection. Make sure that your login and password are entered correctly. In case the error remains, follow these steps:

1. Check if the user who is trying to connect is registered in the system and his password is correct (to do so, use the local users management module. Take a look at the chapter Managing firewall users).
2. Check if the network is working correctly. It is possible to do this in many ways, one of them is by using the **ping** command. (Do not forget to add to the firewall a rule allowing the echo request and echo reply ICMP services from the host being tested to the firewall, in case you use the ping. To learn how to do this,

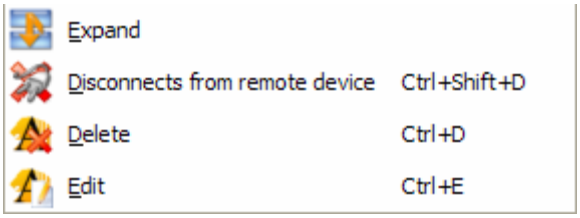
refer to the chapter The Stateful Filter). If it does not work, then the network has connectivity problems and they must be solved before you try the remote management. If it works, go to step number 3.

3. See if there is a filtering rule allowing access from the host you want to establish the management session to the firewall, on the Aker service (TCP, port 1020). In case it does not exist, create this rule (to learn how to do this, refer to chapter The Stateful Filter).

2-2 Finishing the remote management

There are three ways of finishing the remote management of Aker Firewall:

- Finishing the session, by right clicking in the connected firewall and selecting the *Disconnect from Firewall* option;



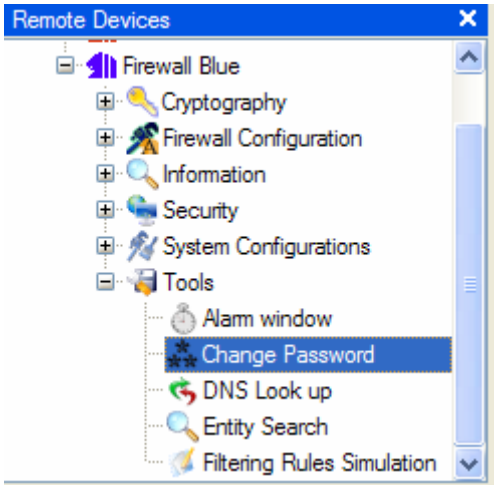
- Clicking once on the firewall and selecting the *Disconnect* button on the toolbar;

- Closing the interface. In this case all firewall connections will be closed.

In case you want to close the window, just click on the *Exit* button  on the main window toolbar or click on the "x" on the right superior corner of the main window.

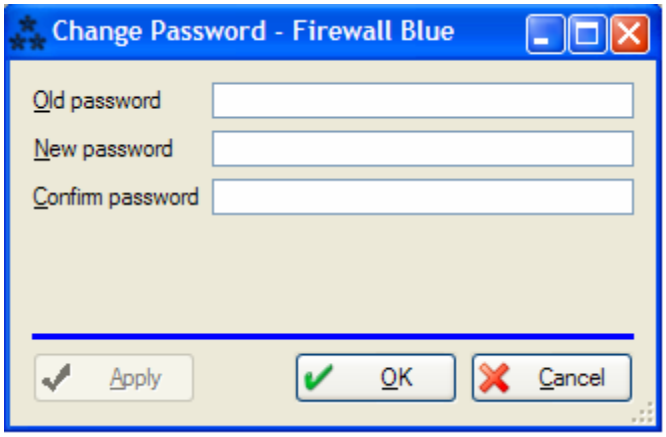
2-3 Changing your user's password

Any Aker Firewall user can change his password every time it is necessary. In order to do it, a management session must be established first (as shown in the section Starting the remote interface) and then the following steps should be taken:



- Select the firewall to be configured
- Click on *Tools*
- Double click on *Change Password.*

The following window will be shown:

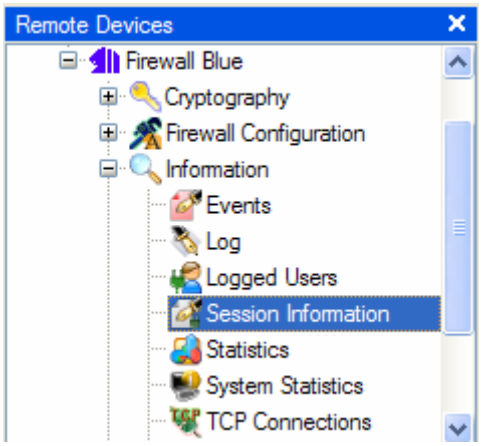


You must type the old password in the **Old Password** field and the new password in the **New Password** and in the **Confirm Password** fields (the passwords will be displayed on the screen as asterisks "*").

After filling in the fields, you must press the **OK** button to change the password or the **Cancel** button in case you do not want to change it.

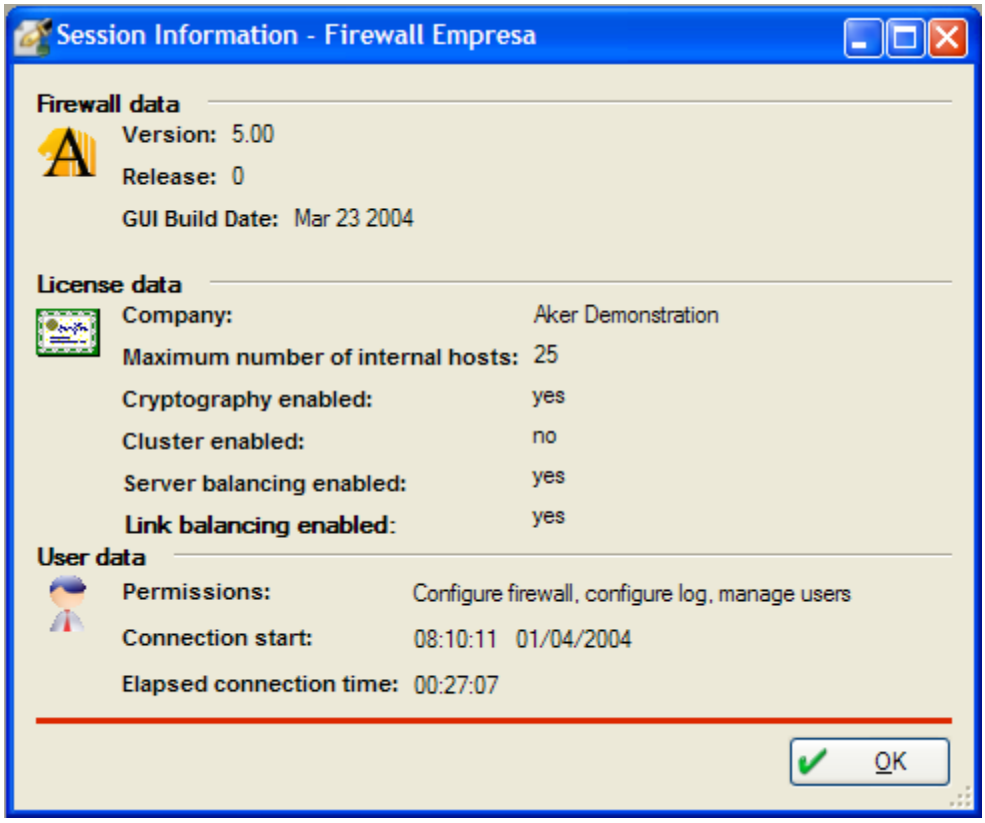
2-4 Viewing session information

It is possible to view information about the active management session at any time. For this purpose, there is a window that shows useful information such as: login name, full name and the permissions of the user who is managing the firewall, the version and the release of the Aker Firewall that is being managed. The connection time and how long it has been active are also shown. To open this window, take the following steps:



- Select the firewall to be configured
- Click on *Information*
- Double click on *Session Information.*

The following window will be shown:

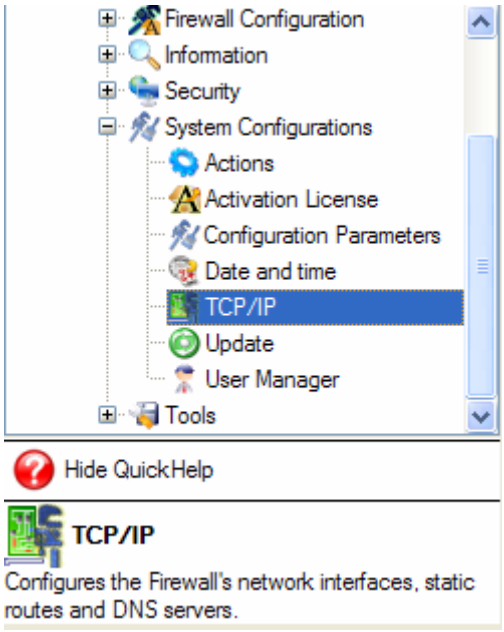


2-5 Using the online help and the QuickHelp

Aker Firewall has a very complete online help. It is shown in a window at the lower part of the main window. It is possible to select whether or not this help window will be shown by clicking on the *Windows* menu, then *Windows* sub-menu and *Help* option.

The online help consists of the contents of this manual showed in a case sensitive way related to the active configuration window, that is, the relevant part of the manual to the active window will be displayed.

The QuickHelp consists of a brief explanation about each of the configuration menus. This explanation is shown in a small window below the menus, as demonstrated in the following picture:



It is possible to show or hide the QuickHelp just by clicking on its icon.

3-0 Managing Firewall users

This chapter shows how to create users who will manage Aker Firewall remotely.

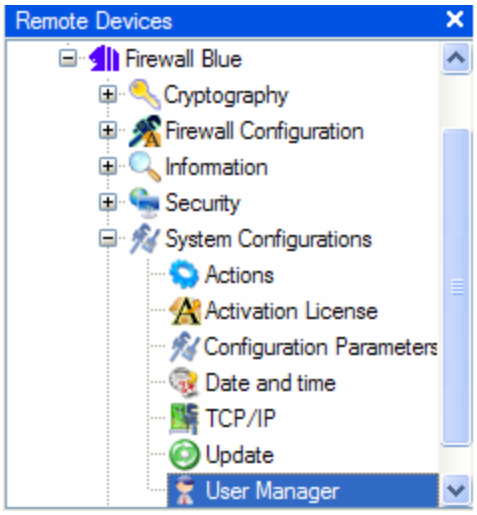
What are Aker Firewall users?

In order to manage Aker Firewall remotely, a user needs to be recognized and validated by the system. This validation is done by passwords and, in order to make it possible, each one of the administrators must have been previously registered with a login and a password.

Furthermore, Aker Firewall allows the existence of many distinct administrators, each one responsible for a certain administrative task. Besides making the management easier, this allows higher levels of control and security.

3-1 Using the graphic user interface

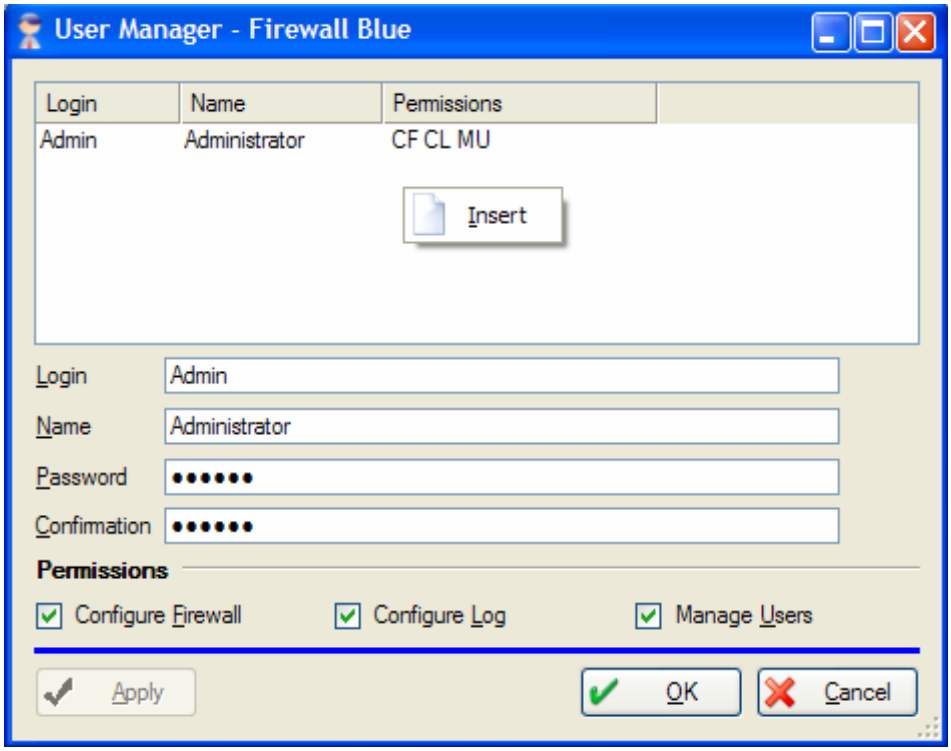
To access the users management window in the remote interface, follow these steps:



- Click on *System configurations* menu in the window of the firewall you want to manage
- Select the *User Manager* option

This option is enabled only if the user who has the management session established in the remote interface has the authority to manage users. This will be presented in details in the next section.

The users management window



This window consists of a list of all registered firewall users. Each user's login, full name and permissions are displayed. The number of currently registered users is shown at the bottom of the window.

- The **OK** button closes the users management window and saves all changes.
- The **Apply** button saves the modifications done on a user and keeps the window open.
- The **Cancel** button closes down the users management window and discards all the changes done.
- When a user is selected, his complete properties are shown in the fields below the list.

To change the users' properties, you must proceed as follows:

1. Select the user to be modified by clicking on his name with the left mouse button. His properties will be displayed in the fields below the list of users.
2. Change the value of the properties and click on the **Apply** or **OK** button.

To add a new user to the list, go on as follows:

1. Click with the right mouse button anywhere in the reserved area to show the list and select the **Insert** button on the pop-up menu or click on the icon that represents the insertion in the toolbar.
2. Fill in the fields of the user to be registered and click on the **Apply** or **OK** button.

To remove a user from the list, you must follow these steps:

1. Select the user to be removed by clicking on his name with the left mouse button and click on the icon  that represents the removal on the toolbar.
   or
2. Click with the right mouse button on the user name to be removed and select the **Remove** option in the pop-up menu.

Meaning of the user's attributes

- **Login**

It is the user identification for the firewall. It is not possible to have two users with the same login. This login will be requested from the firewall administrator when he establishes a remote management session.

The login must consist of 1 to 14 characters and is not case sensitive.

- **Name**

This field contains the full name of the user. It is merely informative, not being used for any validation.

This name must be a string with length of 0 to 40 characters.

- **Password**

This field will be used together with the login field to identify an user to Aker Firewall. When you type the password, asterisks "*" will be shown on the screen instead of letters.

The maximum password field length is 14 characters. Its minimum length is configurable in the interface parameters window (for more information refer to the section Configuring the interface parameters). **The password field is case sensitive.**

 It is extremely important to use long passwords, as close as possible to the limit of 14 characters. Besides, a combination of small letters, capital letters, numbers and other special characters in the passwords should always be used (special characters are those found on the computer keyboard and that are neither numbers nor letters: "$", "&", "]", etc). **Do not ever use words in any language or only numbers as a password.**

- **Confirmation**

This field is used to confirm the password typed in the previous field.

- **Permissions**

This field defines what a user can do in Aker Firewall. It consists of three options that can be marked independently.

The aim of these permissions is to allow the creation of a decentralized administration of the firewall. It is possible, for instance, in a company that has many departments and many firewalls, to let an administrator be responsible for the configuration of each one of the firewalls and a central one with the task of supervising the administration. This supervisor would be the only person capable of clearing and changing the configuration of the log and events of the firewall. This way, even though each department has administrative autonomy, it is possible to have a central control of what and when was changed by each administrator.

 If a user does not have any permissions, then he will only be able to view the firewall configuration and compact the log and events files.

- **Configure the Firewall**

If this permission is marked, the user will be able to administrate the firewall, which means he will be allowed to change the configuration of entities, filtering rules, network address translation, secure channels, proxies and configuration parameters not related to the log.

- **Configure the Log**

If this option is marked, the user will have the power to change the parameters related to the log (for example, the log lifetime), change the configuration of the actions window (both the messages and the parameters) and erasing the log and events permanently.

- **Manage Users**

If this option is marked, the user will have access to the users management window, which allows him to add, edit and remove other users.

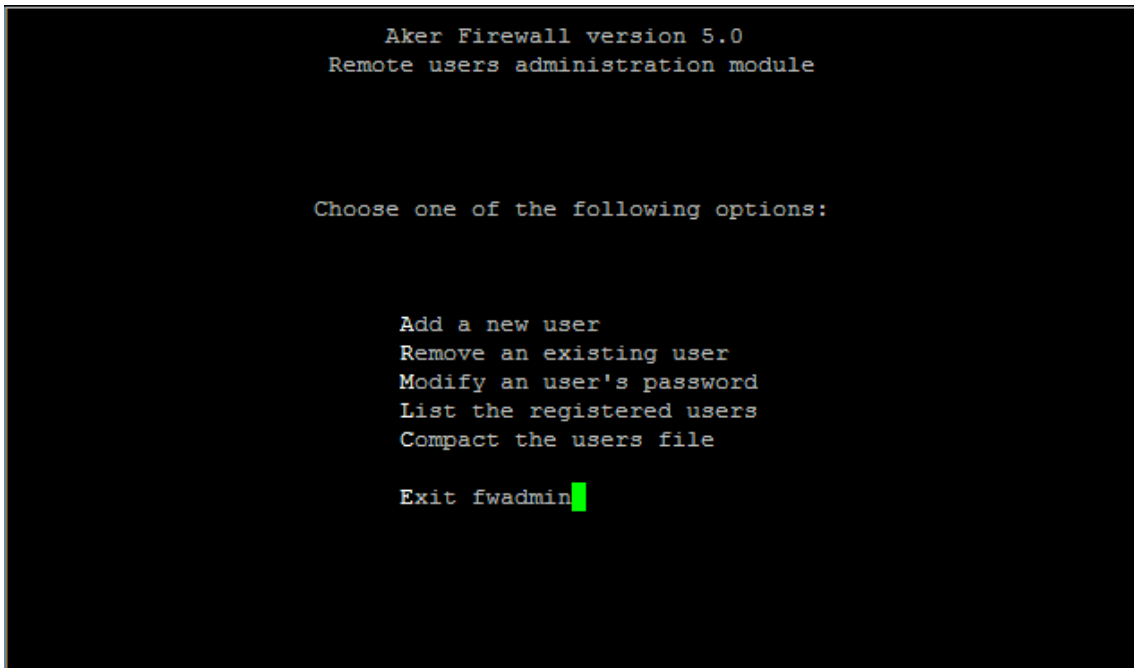
 A user that has this authority can only create, edit or remove users with the same or lower authority (for example, if a user has the power to manage users and configure log, then he may create users who do not have any authority, users who can only configure the log and users who can manage users and configure the log. He cannot either create, edit or remove a user who is able to configure the firewall)

3-2 Using the command line interface

Besides the users management graphic user interface, there is a local character-based interface that has the same capability as the graphic user interface. The only unavailable option is the changing of users' permissions. This interface, on the contrary of all the command line interfaces of Aker Firewall, is interactive and does not receive parameters from the command line.

Program location: /etc/firewall/fwadmin

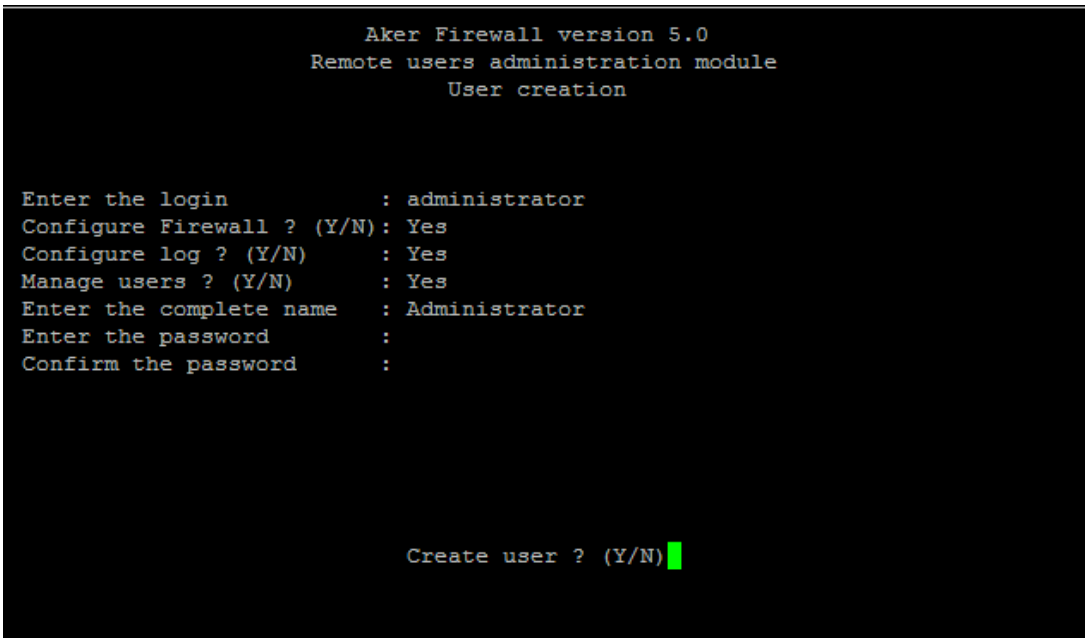
When it is run, the program will show the following screen:



To invoke one of the displayed options, just type in the bold letter. Each one of the options will be shown in details as follows:

- Add a new user

This option allows the creation of a new user who will be able to manage the Aker Firewall remotely. When it is selected, the program will show a screen asking for information about the user. After all the information has been filled in, a confirmation for the addition will be asked.



Important remarks:

1. In the fields where the options (Y/N) are shown, you must type Y, for yes and N for no.
2. The password and the password confirmation will not be shown on the screen.

- Remove an existing user

This option removes a registered user from the system. The login of the user to be removed will be asked. If the user is really registered, a confirmation to go on with the removal will be asked.

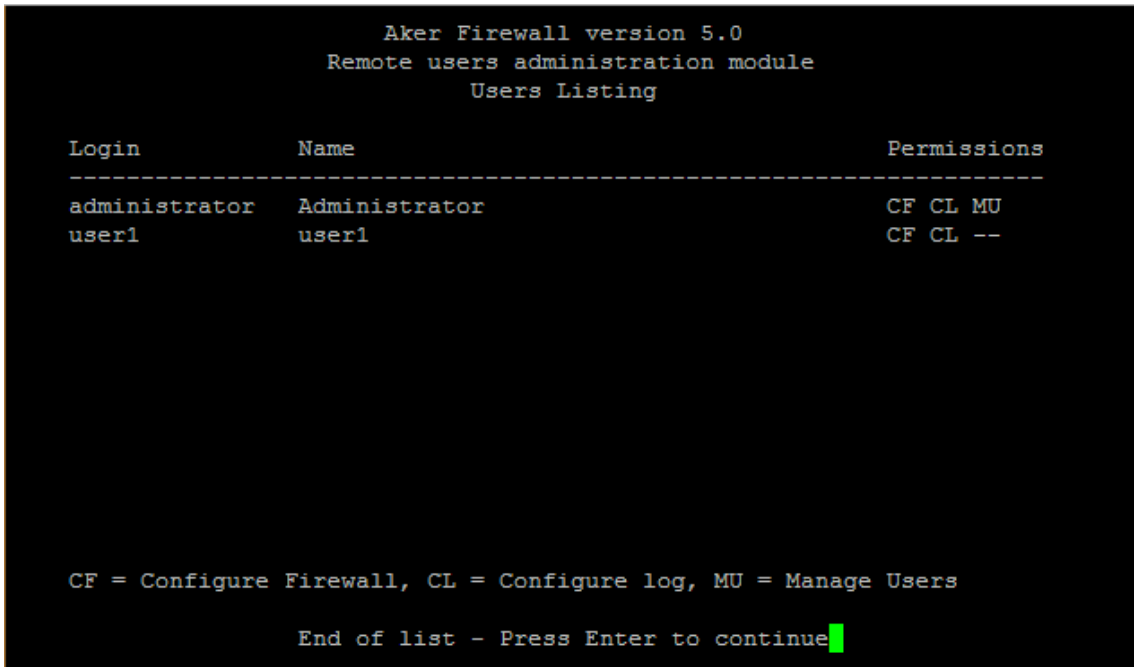
To proceed with the removal, just type Y, otherwise type N.

- Modify an user's password

This option allows to change the password of an existing user. The login of the user will be asked and, in case he exists, the new password and the confirmation of the new password will be asked (as it has already been mentioned, the password and the confirmation will not be displayed).

- List the registered users

This option shows a list with the name and the permissions of all the users authorized to administrate the firewall remotely. One example of a possible list is as follows:



The permissions field consists of 3 possible values: CF, CL and MU, which correspond to the permissions of Configure Firewall, Configure Log and Manage Users, respectively. If a user has a permission, it will be shown with the above code, otherwise the value -- will be shown, indicating that the user does not have it.

- Compact the users file

This option is not present in the graphic user interface and does not have a frequent use. It is used to compact the users file, removing entries no longer used. It should be used only when a great number of users has been removed from the system.

When selected, the file will be compacted and at the end, a message showing that the procedure is complete will be shown (the file compacting is usually a fast procedure. It lasts only a few seconds).

- Exit fwadmin

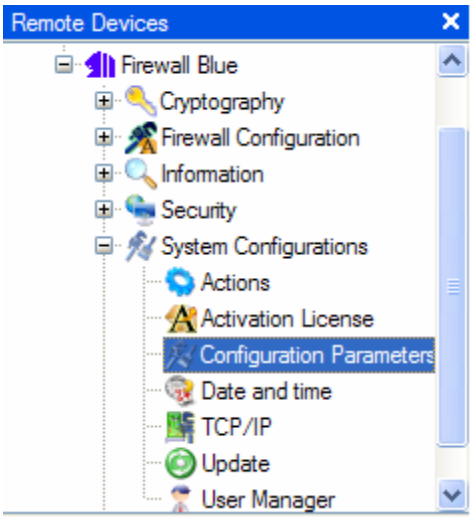
This option ends the fwadmin program and returns to the shell prompt

4-0 Configuring the system parameters

This chapter shows how to configure the variables which will influence the operation of the whole system. These configuration parameters are essential to several aspects such as security, system log, and connections timeouts.

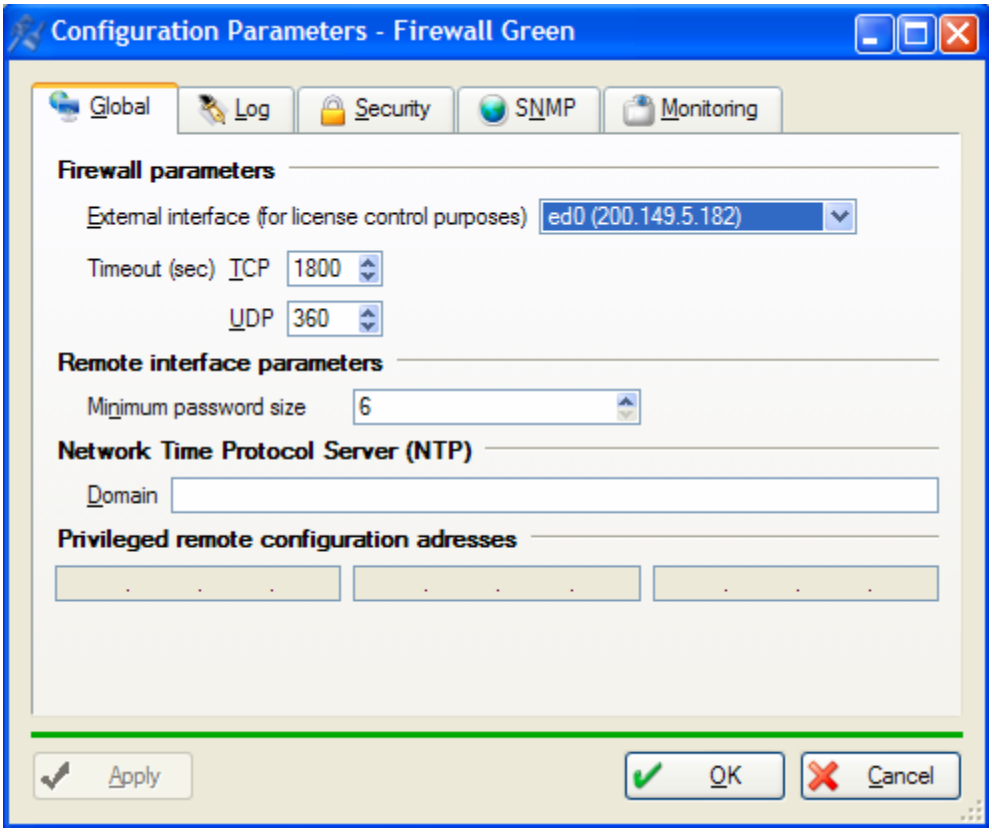
4-1 Using the graphic user interface

In order to access the configuration parameters window, the following should be done:



- Click on the *System Configurations* menu of the firewall window you want to manage.
- Select *Configuration parameters* item.

The configuration parameters window



- The **OK** button will close the parameters window and save all changes.
- The **Cancel** button will close the parameters window and discard all the changes done
- The **Apply** button saves all modifications but keeps the window open

Meaning of the parameters

- **Global tab**

These parameters are used by the stateful filter and by the network address translator. They consist of the following fields:

External Interface: Defines the name of the firewall external interface. Connections which come through this interface will not count in the license.

Default value: Configured during the firewall installation by the administrator.

TCP Timeout: Defines the maximum amount of time, in seconds, during which a TCP connection can remain without traffic and still be considered active by the Firewall. Its value can range from 0 to 30000.

Default value: ***900*** seconds.

UDP Timeout: Defines the maximum amount of time, in seconds, during which a UDP connection can remain without traffic and still be considered active by the Firewall. Its value can range from 0 to 30000.

Default value: ***180*** seconds.

 These fields are vital to the correct firewall operation. High values may cause security problems to services based on the UDP protocol, will make the system use more memory and will make it slower. Low values, on the other hand, may cause constant session failures and bad functioning of some services.

GUI session timeout: Defines the maximum amount of time, in seconds, that the interface will remain connected to the firewall without receiving any command from the administrator. As soon as this time is reached, the interface will automatically disconnect from the firewall, allowing a new session to be established. Its value can range from 30 to 3600.

Default value: **600** seconds.

Minimum password size: Defines the minimum number of characters that the administrators passwords must have in order to be accepted by the system. Its value can range from 4 to 14 characters.

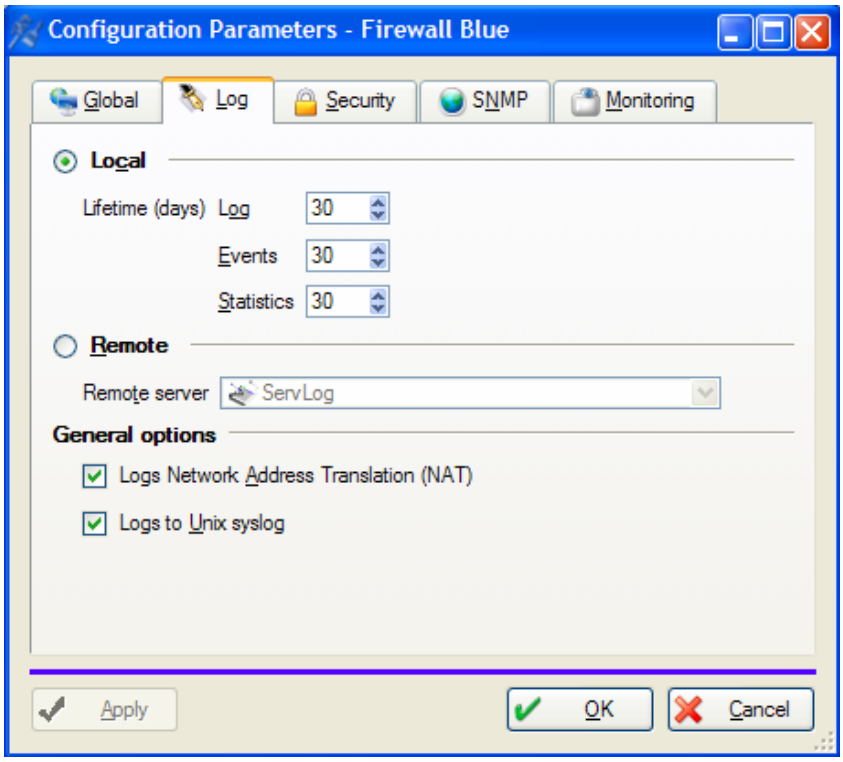
Default value: **6** characters.

It is important that this value be the largest possible, in order to avoid the use of passwords that can be easily guessed.

Network Time Protocol Server (NTP): Defines the time server that will be used by the firewall to synchronize its internal clock.

Privileged remote configuration addresses: These are addresses that, regardless of rules and license limits can administrate the firewall (that is, connect to port 1020). They serve as an anti-blocking preventive measure, since they can be configured only through the command line interface.

- **Log tab**



Local: Indicates that the log/events/statistics records are to be saved in a local disk, in the host where the firewall is running.

Lifetime log / events / statistics: The log, events and statistics records are saved in daily files. This configuration defines the maximum number of files that will be kept by the system, in case they are saved locally. The possible values are from 1 to 365 days.

Default value: *7* days

In case of remote log usage, these options will be disabled and should be configured in the remote log server

Remote: This option indicates that log/events/statistics records are to be sent to a remote log server, instead of being saved locally. With the use of this option, the control of several firewalls can be centralized, making auditing easier.

Remote Server: This option specifies the remote log server where log/events/statistics records will be sent to.

Logs Network Address Translation (NAT): Enables the logging of the network address translations performed by the Firewall.

Default value: ***Address translations won't be logged***

Even with this option activated, only packets translated through 1:N and N:1 translations will be logged. The translations performed through other types of translation rules will not be logged.

The activation of such option does not bring along any important information, and it may be used only for the purpose of tests or debugging.

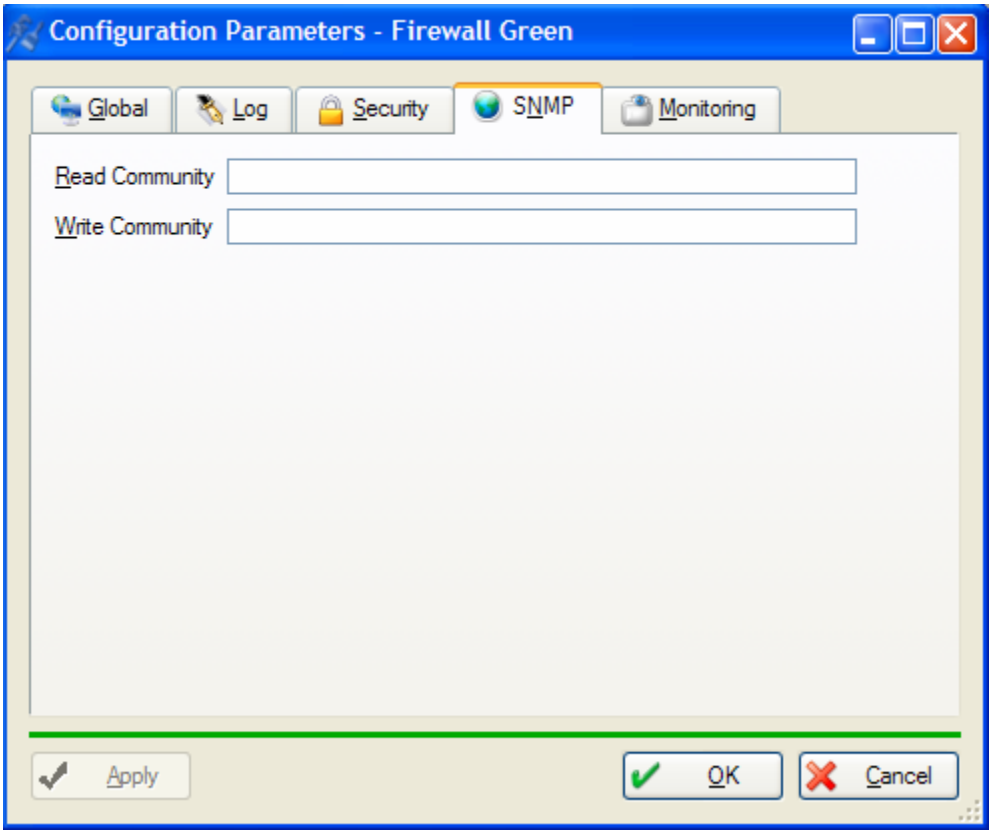
Log to Unix syslog: It enables the sending of the log and event messages of the firewall to the Unix log daemon, *syslogd*.

Default value: ***Log is not sent to syslogd***

In case this option is checked, log records will be sent to *local0* facility and event records will be sent to the *local1* facility.

This option does not modify the internal logging of log and event records performed by the firewall.

- **Security tab**



Allows source routed packets: Enables the acceptance of packets which hold options of record route or source routing. If this option is unchecked, packets with one of these options won't be allowed to pass.

Default value: ***Source routed IP packets are not allowed.***

It is important to point out that the acceptance of packets with any of the options shown above may cause a serious security breach. This option should be left unchecked unless there is a specific reason for letting these packets pass through.

FTP Support: Enables specific support for FTP protocol.

Default value: ***FTP Support is enabled***

This parameter tells the Firewall to deal with FTP protocol in a special way, allowing a transparent operation to all internal and external, client and server hosts. If FTP is going to be used through the Firewall, this option should be checked

Real Audio Support: Enables specific support for Real Audio and Real Video protocols.

Default value: ***Real Audio support is enabled***

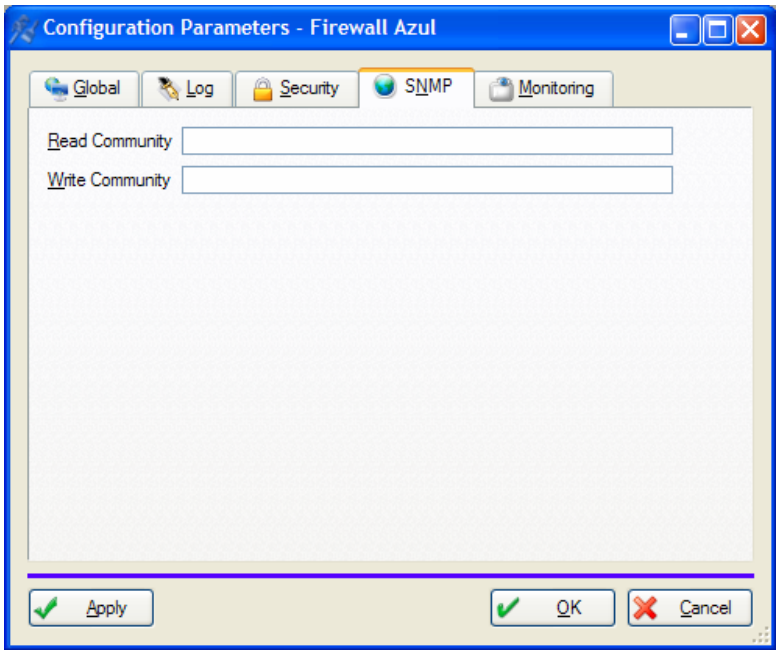
This parameter tells the Firewall to deal with Real Audio / Real Video protocols in a special way, allowing it to operate transparently using TCP and UDP connections. Unless Real Audio protocol is not going to be used or if it's going to be used uniquely with TCP connections, this option should be checked

RTSP Support: Enables specific support for RTSP protocols.

Default value: ***RTSP support is enabled***

RTSP (Real Time Streaming Protocol) is an application level protocol that allows the transportation of real time audio and video data. This parameter tells the Firewall to deal with this protocol in a special way, allowing it to operate transparently using TCP and UDP connections. Unless RTSP protocol is not going to be used or if it's going to be used uniquely with TCP connections, this option should be checked

- **SNMP tab**



Read Community: This parameter sets the name of the community which is authorized to read the Firewall data via SNMP. If this field is blank, no host will be authorized to read it.

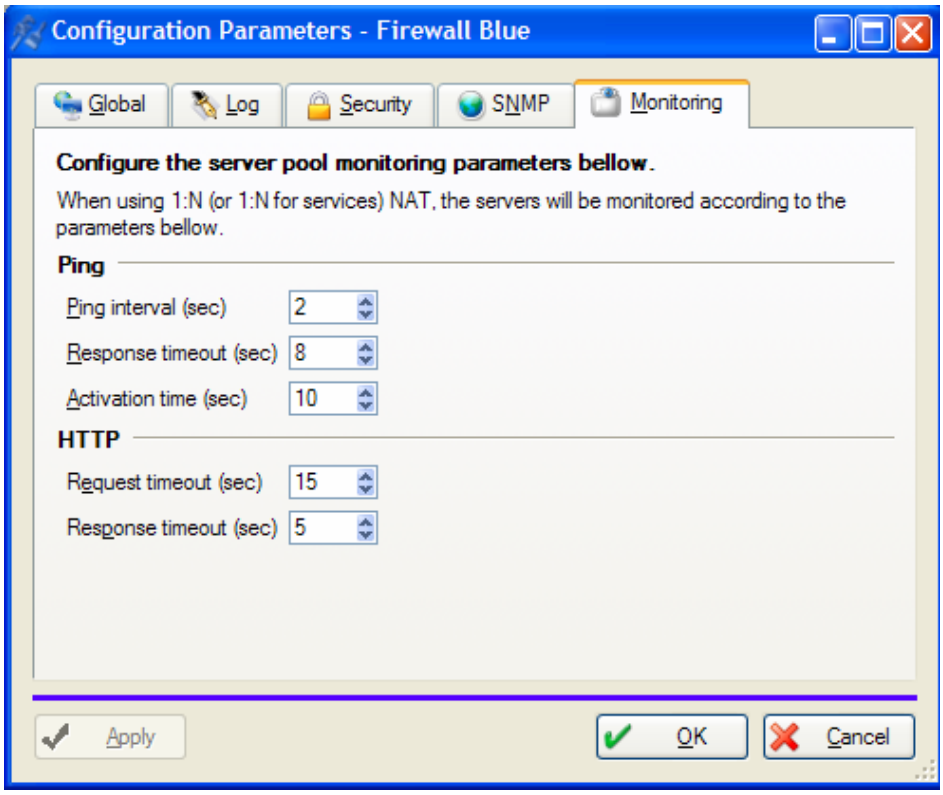
Default value: ***blank field***

Write Community: This parameter sets the name of the community which is authorized to modify the Firewall data via SNMP. If this field is blank, no host will be authorized to modify any data.

Default value: ***blank field***

Even when the write community is defined, for security reasons, only some variables of the ***system group can be modified.***

- **Monitoring tab**



When 1-N translation is being used, that is, load balancing, it is possible to configure the type of monitoring that will be performed by the firewall to check if the hosts participating of the balancing are up. The monitoring parameters allows the modification of the monitoring time intervals, in order to better adjust them to each different environment.

Monitoring by ping

These parameters configure the time values used by the firewall to perform monitoring through *ICMP Echo Request* and *Echo Reply* packets. They are:

Ping interval: This field defines how often a ping will be sent to the hosts being monitored. If it is set to 2, for instance, a ping will be generate each two seconds and so on. Its value ranges from 1 to 60 seconds.

Default value: ***2*** seconds

Response timeout: This field defines the maximum amount of time, in seconds, that a host can remain without responding to the ping packets sent by the firewall and still be considered up. Its value ranges from 2 to 120 seconds.

Default value: ***8*** seconds

Activation time: This field defines the amount of time, in seconds, that the firewall will wait, after receiving a response packet from a host previously down, until it considers the host up again. This time interval is necessary because usually a host responds to ping packets before all its services are up. Its value ranges from 1 to 60 seconds.

Default value: ***10*** seconds

Monitoring by http

These parameters configure the time values used by the firewall to perform monitoring through HTTP requests. They are:

Request timeout: This field defines how often a request will be sent to the hosts being monitored. If it is set to 5, for instance, a HTTP request will be generate each five seconds and so on. Its value ranges from 1 to 300 seconds.

Default value: ***5*** seconds

Response timeout: This field defines the maximum amount of time, in seconds, that a host being monitored can take to respond to a firewall request and still be considered up. Its value ranges from 2 to 300 seconds.

Default value: ***15*** seconds

4-2 Using the Command Line Interface

The command line interface of the parameter configuration is quite simple to use, and it holds the same capacities as the graphic user interface. However, it has the possibility, not available in the remote graphic user interface, of adding up to three hosts capable of managing the firewall remotely, even without the existence of a rule permitting its connection. The objective of this feature is to allow an administrator, that has made an incorrect configuration that blocks his access, to keep managing the firewall remotely. This parameter is called **remote_add**.

Program Location: `/etc/firewall/fwpar`

Syntax:

```
fwpar [show | help]
fwpar [external_interface] <name>
fwpar [tcp_timeout | udp_timeout] <seconds>
fwpar [source_routed_ip] <yes | no>
fwpar [rtsp_support | ftp_support | real_audio_support] <yes | no>
fwpar [log_translation | log_syslog] <yes | no>
fwpar [log_lifetime | events_lifetime | stat_lifetime] <days>
fwpar [remote_log_server <name>]
fwpar [remote_add <n> <ip_add>]
fwpar [read_community | write_community] [name]
```

Program help:

```
fwpar - shows/changes configuration parameters
Usage: fwpar [show | help]
       fwpar [external_interface] <name>
       fwpar [tcp_timeout | udp_timeout] <seconds>
       fwpar [source_routed_ip] <yes | no>
       fwpar [rtsp_support | ftp_support | real_audio_support] <yes |
no>
       fwpar [log_translation | log_syslog] <yes | no>
       fwpar [log_lifetime | events_lifetime | stat_lifetime] <days>
       fwpar [remote_log_server <name>]
       fwpar [remote_add <n> <ip_add>]
       fwpar [read_community | write_community] [name]

       show               = shows active configuration
       help               = shows this message
       external_interface = sets the the external interface name
(connections that
                            come through it do not count in the
license)
       tcp_timeout        = sets the timeout for TCP connections
       udp_timeout        = sets the timeout for UDP connections
       source_routed_ip   = accepts source routed IP packets
       ftp_support        = enables support for the FTP protocol
       real_audio_support = enables support for the  Real Audio
protocol
       log_translation    = logs network address translation messages
       log_syslog         = sends event and log messages to syslogd
       log_lifetime       = sets the log lifetime in days
       event_lifetime     = sets the events lifetime in days
       stat_lifetime      = sets the statistics lifetime in days
```

```
       remote_log_server  = sets the remote log server to use (entity
name)
       maximum_buffer     = sets the maximum send buffer size for
remote log
       remote_add         = sets the three remote controller addresses
       read_community     = sets the name of the read community for
SNMP
       write_community    = sets the name of the read community for
SNMP
```

Example 1: (viewing the configuration)

```
#/etc/firewall/fwpar show
Global parameters:
------------------
tcp_timeout       : 900 seconds
udp_timeout       : 180 seconds
external_interface: de0

Security parameters:
--------------------
source_routed_ip  : no
ftp_support       : yes
real_audio_support: yes
rtsp_support      : yes
remote_add        : 1) 10.0.0.1       2) 10.0.0.2       3)10.0.0.3

Log configuration parameters:
-----------------------------
log_translation   : no
log_syslog        : no
log_lifetime      : 7 days
events_lifetime   : 7 days
stat_lifetime     : 7 days

SNMP configuration parameters:
------------------------------
read_community    : public
write_community   :
```

Example 2: (enabling source routed IP packets)

```
#/etc/firewall/fwpar source_routed_ip yes
```

Example 3: (defining the name of the SNMP read community)

```
#/etc/firewall/fwpar read_community public
```

Example 4: (clearing the name of the SNMP read community)

```
#/etc/firewall/fwpar read_community
```

5-0 Registering Entities

This chapter shows what entities are, what they are used for and how to register an entity in Aker Firewall.

5-1 Planning the installation

What are the entities and what are they used for ?

Entities are representations of real world objects to Aker Firewall. Through them, it's possible to represent hosts, networks, services and other objects.

The main advantage of using entities to represent real world objects is that, from the moment they are defined in the Firewall, they can be referred as the objects themselves, facilitating its configuration and operation. All entities modifications will be automatically propagated to all references.

It is possible to define, for example, a host called **WWW Server**, with an IP address of **`10.0.0.1`**. After that, it's not necessary to worry about this IP address anymore. Any place where it is necessary to refer to this host, the reference will be done by its name. If a modification in its IP address has to be done latter, it is only necessary to modify the definition of the entity itself and the system will automatically propagate this modification to all of its references.

Defining entities

Before explaining how to register entities in Aker Firewall, a brief explanation about all types of possible entities and what characterizes each one of them is necessary.

There are 6 different types of entities in Aker Firewall: hosts, networks, sets, services, authenticators and interfaces.

Entities of host and network type, as the name itself says, represent individual hosts and networks, respectively; entities of set type represent a collection of any number of hosts and networks; entities of service type represent a service to be made available, through any protocol that runs over IP; entities of authenticator type are a special type of host, that can be used to perform users authentication; finally, entities of the interface type represent a firewall network adapter.

By definition, the IP protocol requires each host to have a different address. Usually, these addresses are represented in the dotted byte form, for example `172.16.17.3`. Therefore, it is possible to identify a specific host on any IP network, including the Internet, using only its address.

To define a network, a mask is necessary as well as a IP address. The mask is used to define which IP address bits will be used to represent the network (bits with the value 1)

and which will be used to represent the hosts in the network (bits with the value 0). Thus, to represent the network whose hosts can be assigned the IP addresses from `192.168.0.1` to `192.168.0.254`, it is necessary to use a network value of `192.168.0.0` and a netmask value of `255.255.255.0`. This netmask means that the first three bytes will be used to represent the network and the last byte will be used to represent the host.

To verify if a host belongs to a certain network, it is just necessary to perform a logical **AND** of the network mask with the desired address and compare with the logical **AND** of the network address with its mask. If they are the same, the host belongs to the network, otherwise it doesn't. Follow this two examples:

Suppose we wish to verify if the host 10.1.1.2 belongs to the network 10.1.0.0, netmask 255.255.0.0. We have:

```
10.1.0.0 AND 255.255.0.0 = 10.1.0.0 (to the network)
10.1.1.2 AND 255.255.0.0 = 10.1.0.0 (to the address)
```

Since both results are equal, after the netmask is applied, the host 10.1.1.2 belongs to the network 10.1.0.0.

Now, suppose we wish to know if the host 172.16.17.4 belongs to the network 172.17.0.0, netmask 255.255.0.0. We have:

```
172.17.0.0 AND 255.255.0.0 = 172.17.0.0 (to the network)
172.16.17.4 AND 255.255.0.0 = 172.16.0.0 (to the address)
```

As the final results are different, the host 172.16.17.4 doesn't belong to the network 172.17.0.0.

 If it is necessary to define a network, where any host is considered as belonging to it (or to specify any host on the Internet), just put the value **`0.0.0.0`** as its network IP address and the value **`0.0.0.0`** as its netmask.This is very useful to define *public* services, which all the Internet hosts will have access to.

Whenever there is communication between two hosts, using the IP protocol, it involves not only the source and destination addresses, but also a higher level protocol (transport level) and some other data that identify the communication uniquely. In case of the TCP and UDP protocols (which are the two most often used over the IP), a communication is identified by two numbers: the **Source Port** and the **Destination Port**.

The destination port is a fixed number usually associated to a specific service. For example, the Telnet service is associated to the TCP protocol on port 23, the FTP service with the TCP protocol on port 21 and SNMP service with the UDP protocol on port 161.

The source port is a sequential number, chosen by the client, in order to allow the existence of more than one active session, of the same service, at a certain time. Thus, a complete communication in the TCP and UDP protocols can be defined as:

```
    10.0.0.1        1024    ->     10.4.1.2          23
TCP
-------------------------------------------------------------------
------ Source address  Source Port  Destination address Destination
Port  Protocol
```

For a firewall, the source port is not important, since it is random. Due to it, when a service is defined, only the destination port is considered.

Apart from the TCP and UDP protocols, there is another important protocol, the ICMP. This protocol is used, by the IP itself, to send control messages, to inform about errors and to test connectivity of a network.

The ICMP protocol doesn't use the ports concept. It uses a number that varies from 0 to 255 to indicate the **Type of Service**. Since the type of service defines one specific service between two hosts, it can be used as the destination port of the TCP and UDP protocols when defining a service.

At last, there are other protocols that can run over the IP protocol, which are not TCP, UDP nor ICMP. Each one of these protocols has its own forms to define a communication and none of them are used by a large number of hosts. Nevertheless, Aker Firewall includes support to these protocols, allowing the administrator to control which of them can pass through the firewall and which can't.

To understand how it is done, it is enough to know that each protocol has a unique number which identifies it to the IP protocol. This number varies from 0 to 255. Because of this, we can define services for other protocols using the protocol number as its identification.

What is quality of service (QoS)

Quality of service can be understood in two different ways: from the application or from the network perspectives. For an application, to offer its services with quality means to fulfill the expectations, usually subjective, of the users regarding response time and quality of the service being provided. For example, in case of a video service, the adequate sound fidelity and/or image without noises and not freezing.

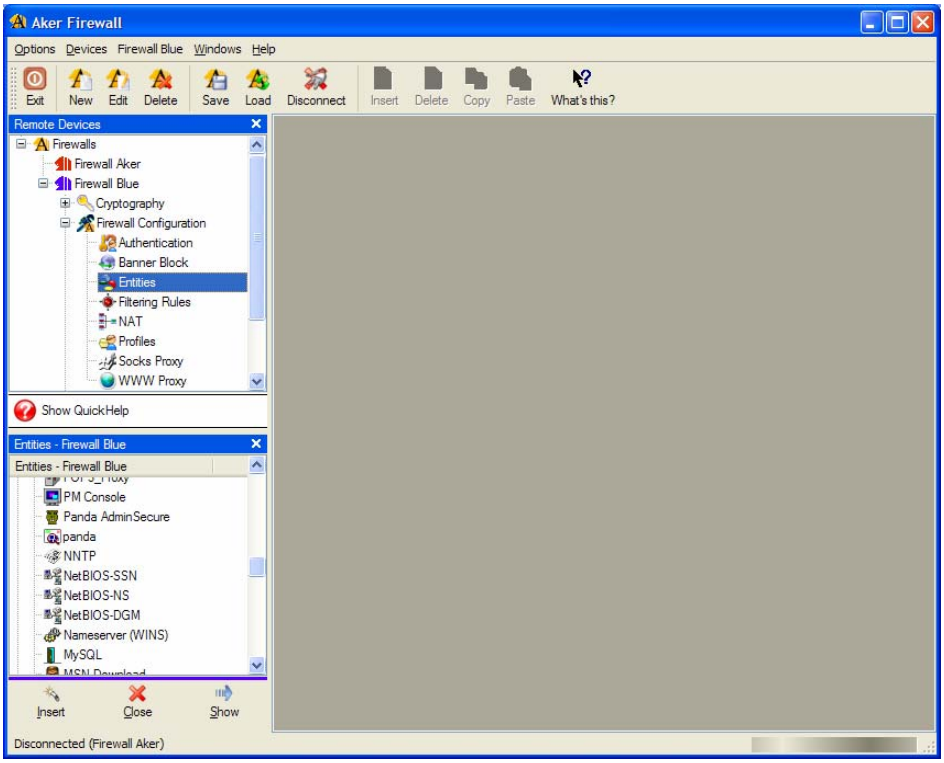
The quality of a network service depends on the needs of an application, that is, what it demands from the network in order to operate well and fulfill the needs of the users. These requirements are translated in parameters that indicate the performance of the network, for example, the maximum traffic delay between the source and destination applications.

Aker Firewall implements a mechanism through which it is possible to define a maximum network bandwidth for specific applications. Through its use, applications that traditionally consume large amount of bandwidth can be controlled. Entities of Pipe type are used for this purpose and will be explained later on.

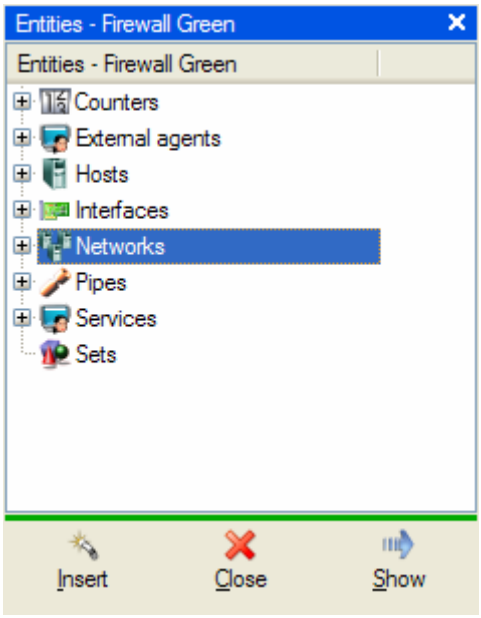
5-2 Registering entities using the graphic user interface

To access the entities registration window, the following must be done:

- Click on the *Firewall Configuration* menu of the firewall window you want to manage.
- Select *Entities* item



The entities window



The entity window is where all the Aker Firewall entities are registered, regardless of its type. This windows due to the fact it is constantly used in almost all firewall configuration windows, is usually kept open, colapsed below the window with the configuration menus for each firewall.

Hint: It is possible to move along the entities windows as if it were a standard window, being it enough to click on its titlebar and drag it to the desired position.

In this window there are eight icons, in a tree structure, representing the eight possible entity types that can be created.

Hint: To view the entities of a given type, just click on the + signal of the corresponding type and the entities will be listed below the icon.

To create a new entity, take the following steps:

1. Right click on the icon representing the type of entity to be created and select the **Insert** option in the pop-up menu.
   or
2. Click on the icon representing the type of entity to be created and press the *Insert* key.

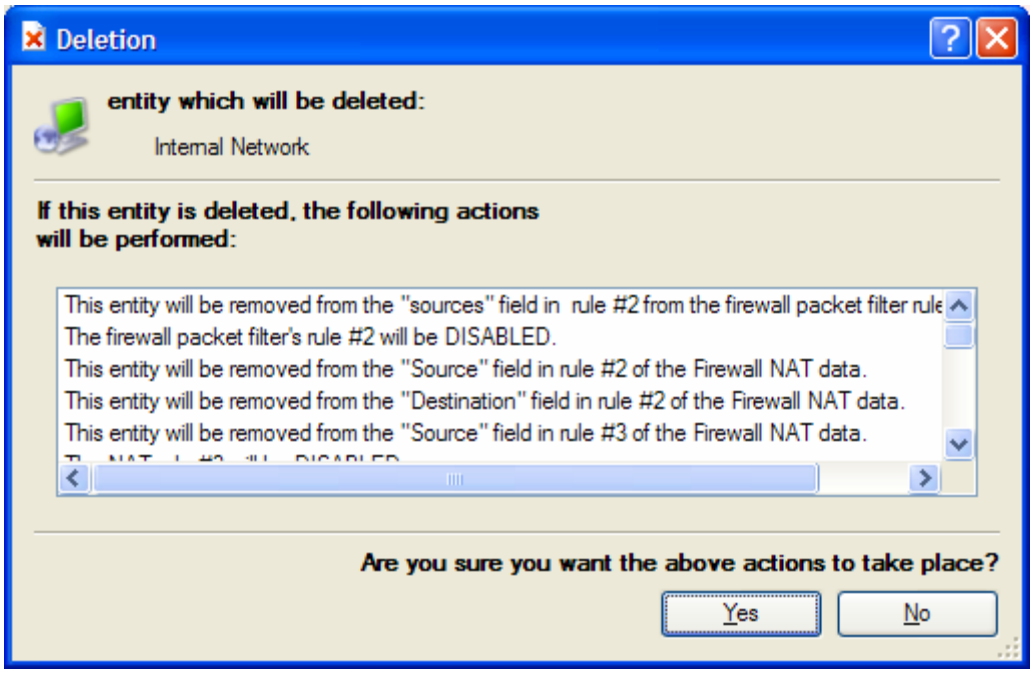
To edit or delete an entity, take the following steps:

1. Select the entity to be edited or removed (if necessary, expand the corresponding entity list)
2. Right click on the entity to be edited or removed and select **Edit** or **Delete** options, respectively, on the pop-up menu
   or
3. Click on the icon representing the type of entity to be edited or deleted and press the *Delete* key .

In case of the options *Edit* or *New,* the entity properties window will appear. This window will be different for each one of the possible entity types.

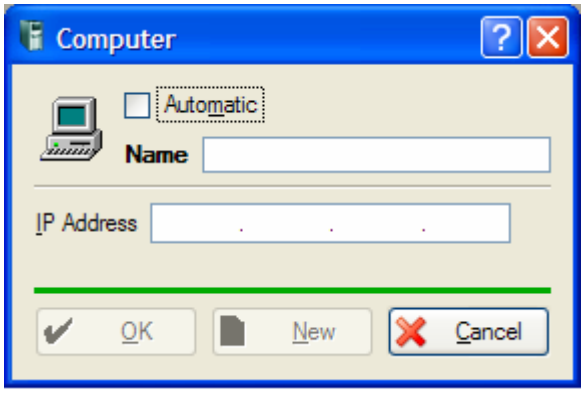
The icon  , in the lower part of the window starts the entity wizard that will be shown at the end of this chapter.

The entity removal confirmation window



Every time an entity is about to be removed the firewall will check if there is any dependency of it in the configuration, in order to keep the configuration integrity. If there is a dependency, it is still possible to remove the entity, but some actions will be taken automatically by the system. The list of actions will be displayed so the administrator can decide whether or not to perform the removal.

Creating / editing hosts



To register an entity of the host type, it is necessary to fill in the following fields:

Name: It is the name which will be used by the firewall to refer to the host from now on. It is possible to specify this name manually or let it be automatically assigned. The option **Automatic** allows to choose between the two operation modes: if it is marked, the assignment will be automatic, otherwise, manual.

Entities names are case sensitive. This way, the existence of many entities whose names consist of the same letters, but with different capital and small letters combinations is possible. The entities **Aker, AKER** and **aker** are, then, considered different.

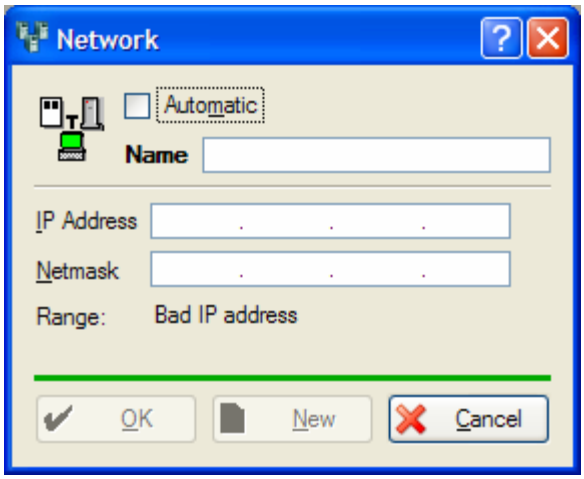
Icon: It is the icon that will appear, associated to the host, in all references. To modify it, just click on the actual icon drawing. The firewall then will show a list of all the possible icons to represent hosts. To select one of them click on the desired icon and on the **OK** button. If you don't want to modify the icon, after seeing the list, just click on the **Cancel** button.

IP: It is the IP address of the host to be created.

After filling in all the fields, click on the **OK** button, to perform the host creation or modification. To cancel the modifications or the creation, click on the **Cancel** button.

To facilitate the creation of many hosts successively, there is a button called **New** (which is disabled during an edition). When clicked, this button will create the host whose data is filled in and the window will be kept open, ready for a new addition. This ways, it is possible to create quickly a large number of hosts.

Creating / editing networks



To register an entity of the network type, it is necessary to fill in the following fields:

Name: It is the name which will be used by the firewall to refer to the network from now on. It is possible to specify this name manually or let it be automatically assigned. The option **Automatic** allows to choose between the two operation modes: if it is marked, the assignment will be automatic, otherwise, manual.

Entities names are case sensitive. This way, the existence of many entities whose names consist of the same letters, but with different capital and small letters combinations is possible. The entities **Aker, AKER** and **aker** are, then, considered different.

Icon: It is the icon that will appear, associated to the network, in all references. To modify it, just click on the actual icon drawing. The firewall then will show a list of all the possible icons to represent networks. To select one of them, click on the desired icon and on the **OK** button. If you don't want to modify the icon, after seeing the list, just click on the **Cancel** button.

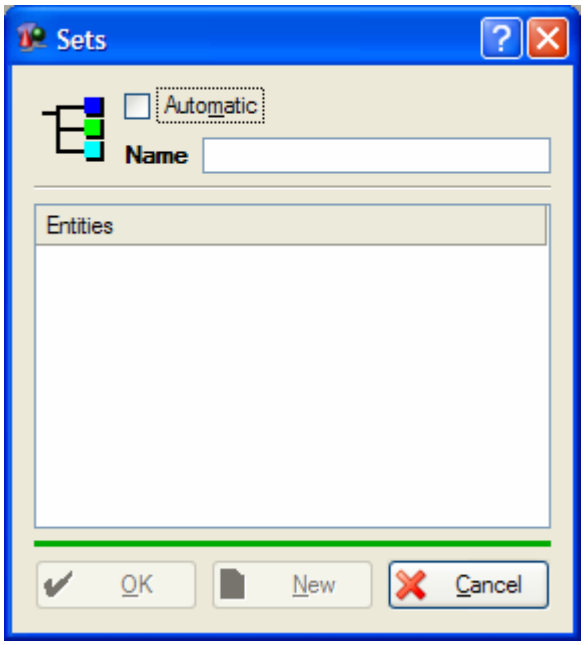
IP: It is the IP address of the network to be created.

Netmask: It is the mask of the network to be created.

After filling in all the fields, it is necessary to click on the **OK** button, to perform the network creation or modification. To cancel the modifications or the creation, click on the **Cancel** button.

To facilitate the creation of many networks successively, there is a button called **New** (which is disabled during an edition). When clicked, this button will create the network whose data is filled in and the window will be kept open, ready for a new addition. This way, it is possible to create quickly a large number of networks.

Creating / editing sets



To register an entity of the set type, it is necessary to fill in the following fields:

Name: It is the name which will be used by the firewall to refer to the set from now on. It is possible to specify this name manually or let it be automatically assigned. The option **Automatic** allows to choose between the two operation modes: if it is marked, the assignment will be automatic, otherwise, manual.

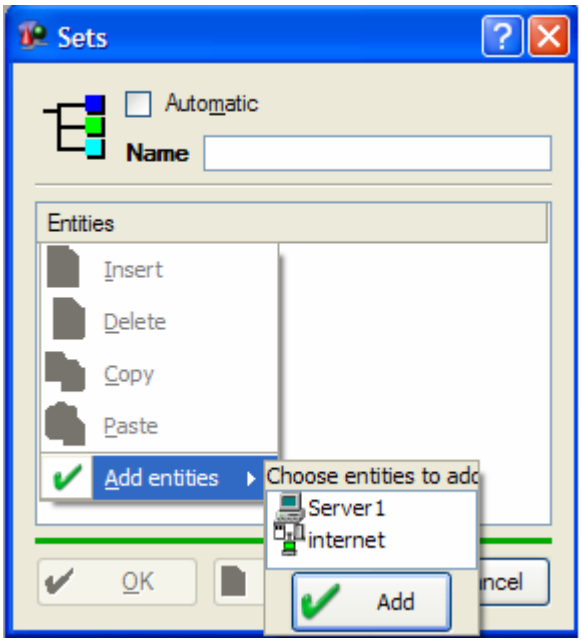
Entities names are case sensitive. This way, the existence of many entities whose names consist of the same letters, but with different capital and small letters combinations is possible. The entities **Aker, AKER** and **aker** are, then, considered different.

Icon: It is the icon that will appear, associated to the set, in all references. To modify it, just click on the actual icon drawing. The firewall then will show a list of all the possible icons to represent sets. To select one of them, click on the desired icon and on

the **OK** button. If you don't want to modify the icon, after seeing the list, just click on the **Cancel** button.

After filling in the name and choosing the icon for the set, it is necessary to define which hosts and networks will belong to it, by following these steps:

1. Right click on the blank field inside the window and select the option **Add entities** (the entity can be added by double clicking on it or by single clicking and then clicking on the **Add** button).
   or
2. Click on the entity to be added, drag and drop it inside the list of entities in the set windows.



To remove a network or a host from the set, it is necessary to follow these steps:

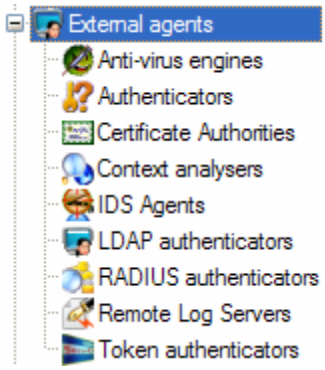
1. Right Click on the entity to be removed and select the **Delete** option.
   or
2. Select the host or network to be deleted from the list of the window and press the *Delete* key.

After filling in all the fields, click on the **OK** button, to perform the set creation or modification. To cancel the modifications or the creation, click on the **Cancel** button.

To facilitate the creation of many sets successively, there is a button called **New** (which is disabled during an edition). When clicked, this button will create the set whose data is filled in and the window will be kept open, ready for a new addition. This way, it is possible to create quickly a large number of sets.

Creating / editing external agents

External agents are used to define complementary programs to Aker Firewall, responsible for specific tasks, that may be running on distinct hosts. When it is necessary to perform a given task by one of the external agents, or vice-versa, the firewall will communicate with them and ask for its execution.



There are 8 different types of external agents, each one responsible for a distinct type of tasks:

- **Antivirus engines**

The antivirus agents are used by SMTP, POP3 and WWW proxy to perform transparent scanning and disinfection of virus in e-mails and FTP / HTTP downloads

- **Authenticators**

The authentication agents are used to perform user authentication in the firewall using username/passwords from databases of several operating systems (Windows NT, Linux, etc).

- **Certification Authority**

Certification authorities are used to perform user authentication through PKI, using Smart Cards.

- **Token authenticator**

The token authenticators are used to perform user authentication in the firewall using SecurID(R).

- **IDS Agent**

The IDS agents (Intrusion Detection Systems) are systems that watch the network at real-time searching for known attack patterns or abuses. When any of these threats are detected, it can add a firewall rule that will block immediately the attacker.

- **LDAP authenticator**

The LDAP authenticator allows the firewall to authenticate users using a X500 compatible database through the LDAP protocol.

- **RADIUS authenticator**

The RADIUS authenticator allows the firewall to authenticate users using a users database through the RADIUS protocol.

- **Remote Log Server**

The remote log servers are used by the firewall to send log to a remote storage server.

 It is possible to install several external agents in a same host, provide each one is of a different type

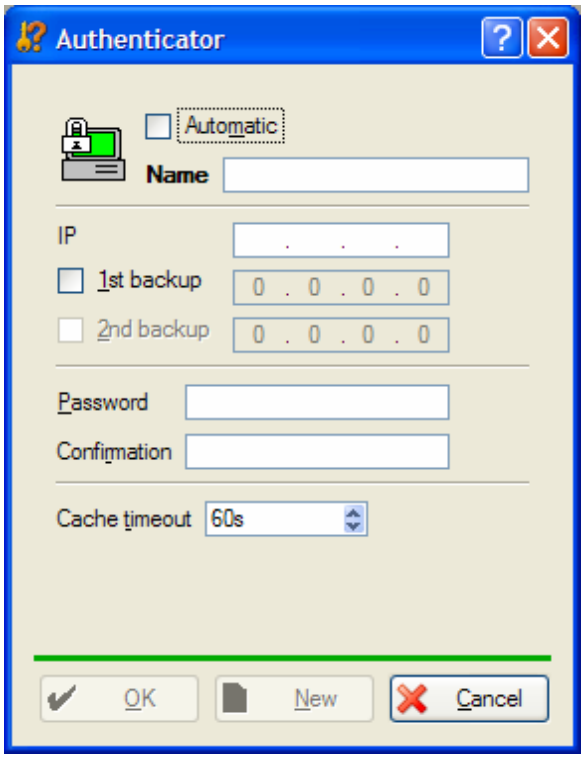
To register an external agent it is first necessary to select its type, by expanding the External Agents list in the entities tree. Regardless of its sub-type, all external agents have the following fields (the remaining fields will be modified according to the agent type and will be explained later on) :

Name: It is the name which will be used by the firewall to refer to the agent from now on. It is possible to specify this name manually or let it be automatically assigned. The option **Automatic** allows to choose between the two operation modes: if it is marked, the assignment will be automatic, otherwise, manual.

 Entities names are case sensitive. This way, the existence of many entities whose names consist of the same letters, but with different capital and small letters combinations is possible. The entities **Aker, AKER** and **aker** are, then, considered different.

Icon: It is the icon that will appear, associated to the agent, in all references. To modify it, just click on the actual icon drawing. The firewall then will show a list of all the possible icons to represent agents of the chosen sub-type. To select one of them, click on the desired icon and on the **OK** button. If you don't want to modify the icon, after seeing the list, just click on the **Cancel** button.

- To register an entity of the **Authenticator** or **Token Authenticator** types, it is necessary to fill in the following additional fields:



IP: It is the IP address of the host where the agent is running.

1st Backup and **2nd Backup**: These fields allow the specification of up to two additional hosts that will also be running the agent and will be used as backup in case of the first host goes down.

The primary and the backup hosts must share a same user database, that is, they must be primary domain controllers or backup domain controllers (PDCs and BDCs), in case of Windows networks, or several Unix hosts using NIS.

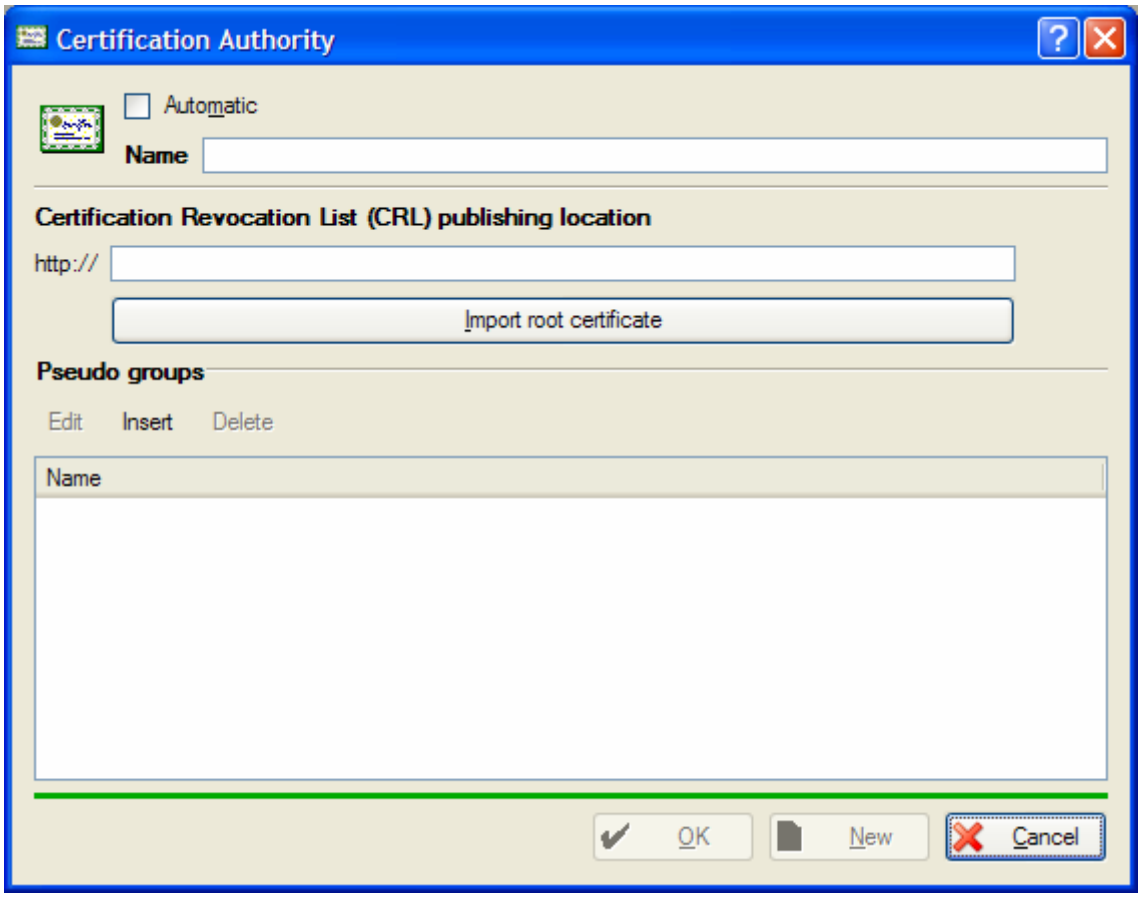
Password: It is the password used to generate the authentication and encryption keys, used on the communication with the authentication agent. This password must be the same as the one configured in the agent. For further information, refer to the chapter Working with proxies.

Confirmation: This field is used only to check if the password was typed correctly. It must be typed exactly as the *Password* field.

Cache timeout: Every time an authentication is successfully performed, the firewall keeps all the data received from the user and authentication agent in the memory. In the subsequent authentications, the firewall has all the necessary data and doesn't have to consult the agent anymore. This allows a better performance.

This parameter allows to define the time, in seconds, that the firewall will keep the authentications information in memory. For further information, refer to the chapter Working with proxies.

- To register an entity of the **Certification Authority** type, it is necessary to fill in the following additional fields:



CRL publishing location: It is the URL which the certification revocation list (CRL) will be downloaded from. This URL must be of the HTTP protocol and must be typed without the http://.

The **Import root certificate** button allows the administrator to load the CA's root certificate in the firewall. When it is clicked, the interface will show a window that allows the specification of the file with the root certificate to be imported.

It is necessary to import a root certificate for each created Certification Authority, otherwise it will not be possible to perform user authentication using it.

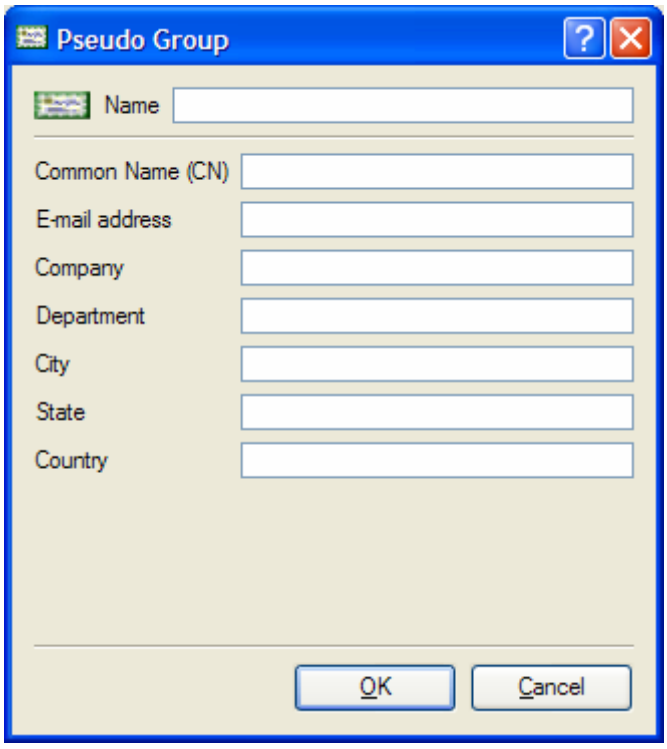
The **pseudo-groups** field allows the definition of groups for users authenticated through the certification authority, in the same way operating system groups are defined. This way, it is possible to define pseudo-groups that represent all users of a given company, department, city, etc. After created, the pseudo-groups can be associated with access profiles in the same way as groups from authenticators or token authenticators.

when right clicking on this field, the following options will be shown:

- **Insert:** This options allows the inclusion of a new pseudo-group.
- **Delete**: This option removes the selected pseudo-group from the list.

- **Edit:** This option opens the edition windows for the selected pseudo-group.

When *Insert* or *Edit* options are selected, the following window will be displayed:

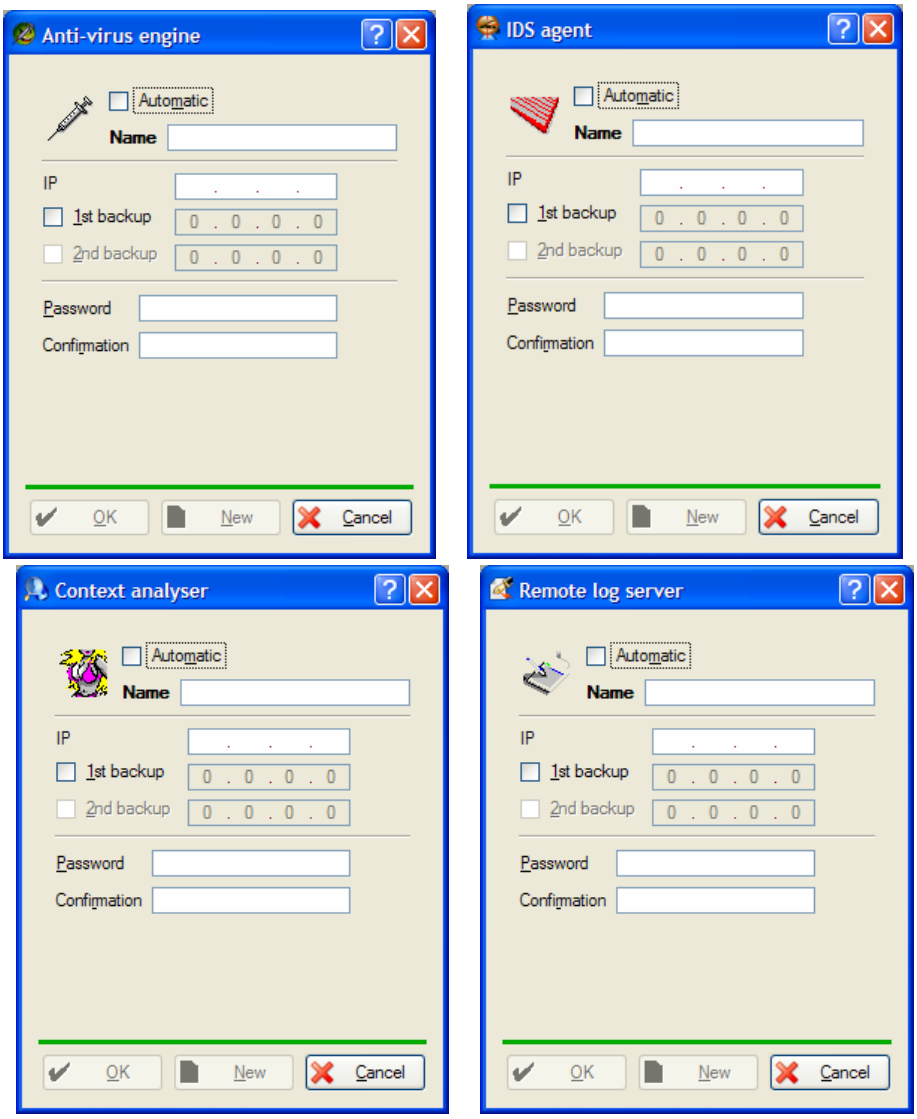


The only mandatory field is the **Name** field, which indicates the name which will be used by the firewall to refer to the pseudo-group. The remaining fields represent data that will be compared with data present in the X509 certificate of each authenticated user. If a given field is left blank then any value will be accepted in the corresponding field of the certificate, otherwise only certificates that have the same value in the corresponding field will be considered as part of the group.

Common name: Represents the name of the person which the certificate was issued to.
E-mail address: Represents the e-mail of the person which the certificate was issued to.
Company: Represents the company name where the person which the certificate was issued to works for.
Department: Represents the department inside the company where the person which the certificate was issued to works in.
City: Represents the city where is located the company where the person which the certificate was issued to works for.
State: Represents the state where is located the company where the person which the certificate was issued to works for.
Country: Represents the country where is located the company where the person which the certificate was issued to works for.

In order for an user authenticated through the certification authority to be considered as part of a pseudo-group, all fields of his X509 certificate must be equal to the values of the corresponding fields of the pseudo-group. Blank fields of a pseudo-group are ignored and then any values in the certificate for these fields will be accepted.

- To register an entity of the **IDS Agent**, **Context Analyser**, **Antivirus** or **Remote Log Server type** types, it is necessary to fill in the following additional fields:



IP: It is the IP address of the host where the agent is running.

1st Backup and **2nd Backup**: These fields allow the specification of up to two additional hosts that will also be running the agent and will be used as backup in case of the first host goes down.

Password: It is the password used to generate the authentication and encryption keys, used on the communication with the authentication agent. This password must be the same as the one configured in the agent.

Confirmation: This field is used only to check if the password was typed correctly. It must be typed exactly as the *Password* field.

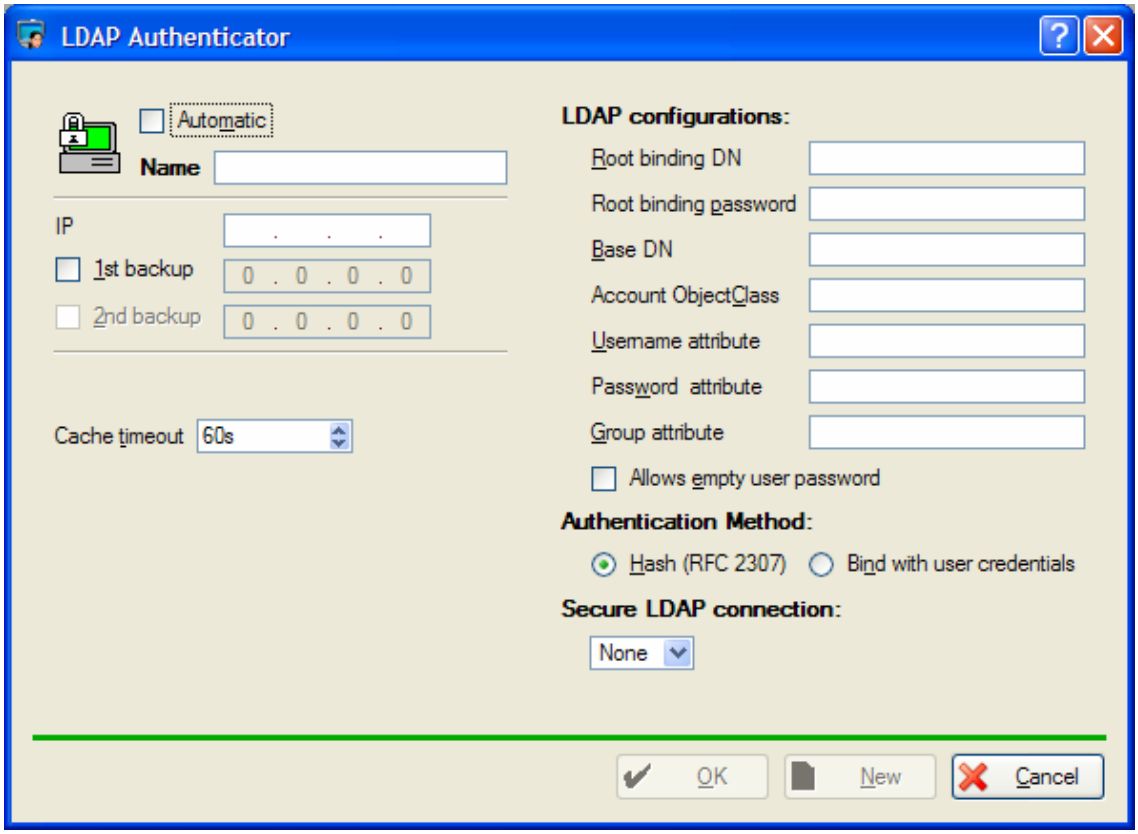
- To register an entity of the **LDAP Authenticator**, it is necessary to fill in the following additional fields:

IP: It is the IP address of the host where the agent is running.

1st Backup and **2nd Backup**: These fields allow the specification of up to two additional hosts that will also be running the LDAP server and will be used as backup in case of the first host goes down.

Cache timeout: Every time an authentication is successfully performed, the firewall keeps all the data received from the user and authentication agent in the memory. In the subsequent authentications, the firewall has all the necessary data and doesn't have to consult the agent anymore. This allows a better performance.

This parameter allows to define the time, in seconds, that the firewall will keep the authentications information in memory. For further information, refer to the chapter Working with proxies.



LDAP configurations: This set of fields is used to specify the configurations regarding the LDAP server that will be used to perform the authentications. The description of each field follows on:

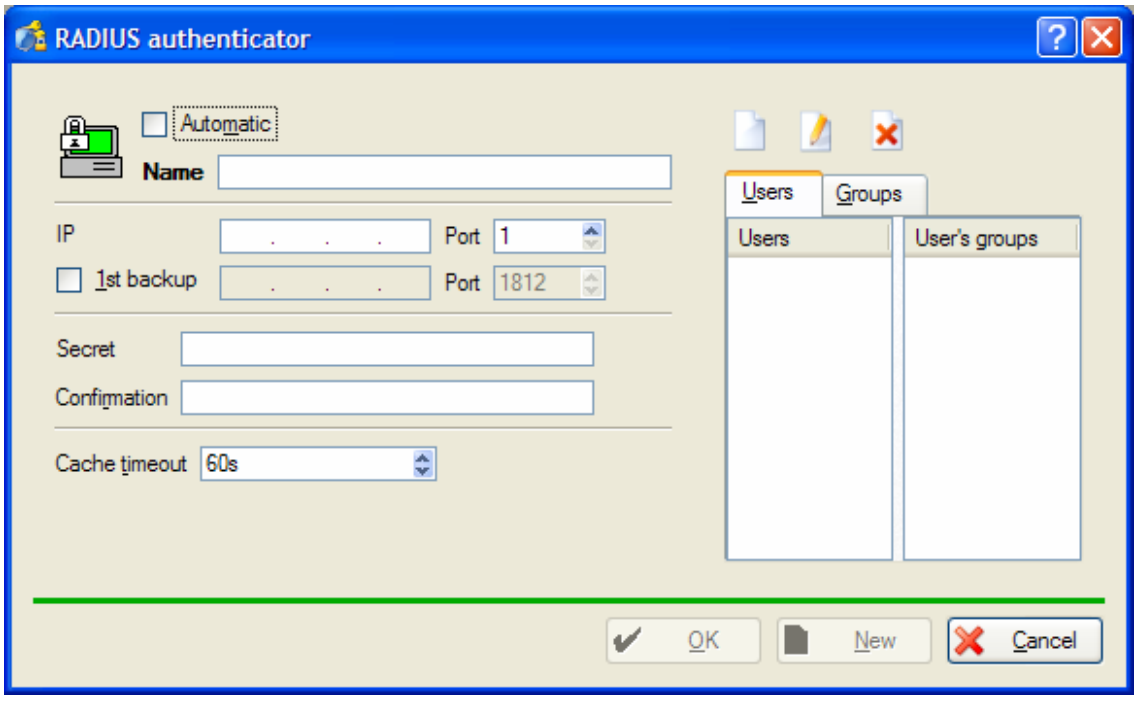
Root binding DN: DN of the user that will be used by the firewall for the queries
Root binding password: the password of the user
Base DN: DN where to start the search
Account ObjectClass: value of *objectclass* that identifies objects from valid accounts
Username attribute: the attribute where the username is located
Password attribute: the attribute where the password is located
Group attribute: the attribute where the group is located
Allows empty user password: allows empty passwords when it is checked

Authentication method: This field specifies if the firewall should search for the password or connect in LDAP database with user credentials in order to validate him.

Secure LDAP connection: This field specifies if the connection with LDAP server will be encrypted or not. It consists of the following options:

- **SSL**: specifies that the firewall will use SSL encrypted connections
- **TLS**: specifies that the firewall will use TLS encrypted connections
- **None**: specifies that the firewall will not use encryption when connecting to LDAP server

- To register an entity of the **RADIUS Authenticator**, it is necessary to fill in the following additional fields:



IP: It is the IP address of the host where the agent is running.

Port: Number of the port that the RADIUS server is listening for authentication requests

1st Backup: This fields allow the specification of an additional hosts that will also be running the RADIUS server and will be used as backup in case of the first host goes down.

Secret: It is the shared secret used in the RADIUS server.

Confirmation: This field is used in order to check if the shared secret was type correctly. It is to be type exactly as in the *Secret* field.

Cache timeout: Every time an authentication is successfully performed, the firewall keeps all the data received from the user and authentication agent in the memory. In the subsequent authentications, the firewall has all the necessary data and doesn't have to consult the agent anymore. This allows a better performance.

This parameter allows to define the time, in seconds, that the firewall will keep the authentications information in memory. For further information, refer to the chapter Working with proxies.

Usuários: Este campo serve para que se possa cadastrar e posteriormente associar usuários específicos RADIUS com perfis de acesso do firewall, uma vez que com este protocolo não é possível para o firewall conseguir a lista completa de usuários. Somente é necessário se realizar o cadastramento dos usuários que se deseje associar com perfis específicos.

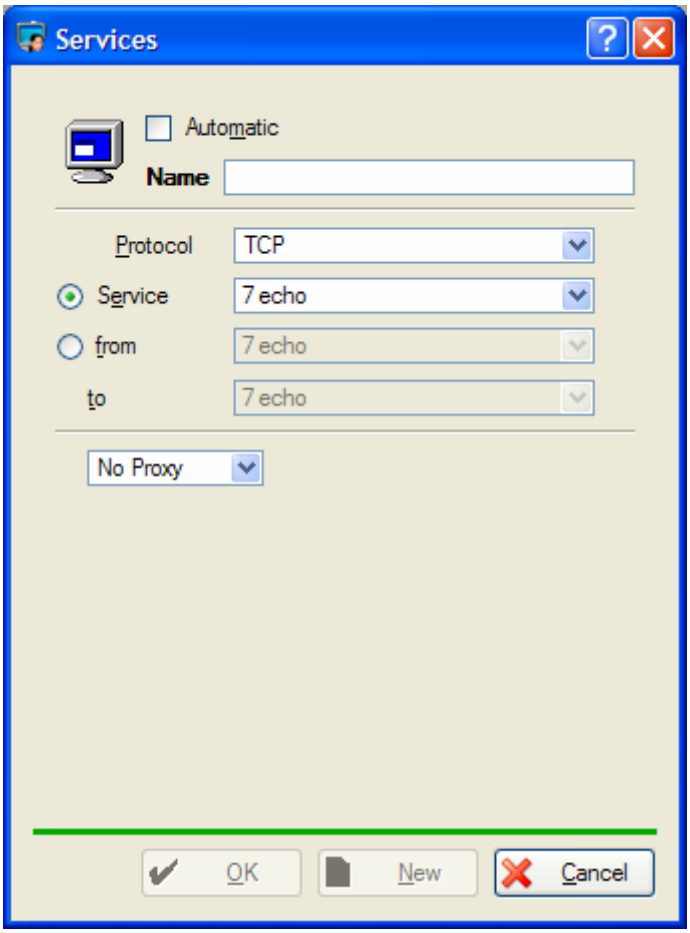
Grupos: Este campo serve para que se possa cadastrar e posteriormente associar grupos específicos RADIUS com perfis de acesso do firewall, uma vez que com este protocolo não é possível para o firewall conseguir a lista completa de grupos. Somente é necessário se realizar o cadastramento dos grupos que se deseje associar com perfis específicos.

Existe um grupo chamado de **RADIUS USERS**, gerado automaticamente pelo firewall que pode ser utilizado para a associação de usuários RADIUS com um perfil de acesso específico. Todos os usuários autenticados em um determinado servidor RADIUS são considerados como pertencentes a este grupo. Desta forma, caso se deseje utilizar um único perfil de acesso para todos os usuários, não é necessário o cadastramento de nenhum usuário e/ou grupo.

After filling in all the fields, click on the **OK** button, to perform the external agent creation or modification. To cancel the modifications or the creation, click on the **Cancel** button.

To facilitate the creation of many agents successively, there is a button called **New** (which is disabled during an edition). When clicked, this button will create the agent whose data is filled in and the window will be kept open, ready for a new addition. This way, it is possible to create quickly a large number of agents.

Creating / editing services



To register an entity of the service type, it is necessary to fill in the following fields:

Name: It is the name which will be used by the firewall to refer to the service from now on. It is possible to specify this name manually or let it be automatically assigned. The option **Automatic** allows to choose between the two operation modes: if it is marked, the assignment will be automatic, otherwise, manual.

Entities names are case sensitive. This way, the existence of many entities whose names consist of the same letters, but with different capital and small letters combinations is possible. The entities **Aker, AKER** and **aker** are, then, considered different.

Icon: It is the icon that will appear, associated to the service, in all references. To modify it, just click on the actual icon drawing. The firewall then will show a list of all the possible icons to represent services. To select one of them, click on the desired icon and on the **OK** button. If you don't want to modify the icon, after seeing the list, just click on the **Cancel** button.

Protocol: It is the protocol associated to the service.

Service: It is the number that identifies the service. In case of the TCP and UDP protocols, this number is the destination port. In case of the ICMP, it is the type of service and in case of other protocols, it is the protocol number. In order to facilitate the service creation, for each protocol, the firewall has a list of the most common service values. However, it is possible to use values that are not part of the list, simply by typing them in the field.

If you want to specify a range of values, instead of only one value, just click on the button beside the names **From** and **To** and specify the lower value of the range in the Service 1 field and the higher in the Service 2 field. All the values within this range, including the lower and higher values, will be considered part of the service.

Proxy: This field is only enabled for the TCP protocol and allows to define if connections that use this service will be automatically redirected to one of the transparent proxies of Aker Firewall. The default value is **No Proxy**, which means that no connections are to be redirected to any proxy. The other options are **HTTP Proxy, SMTP Proxy, POP3 Proxy, Telnet Proxy**, **FTP Proxy** and **User Proxy** that redirect the connection to the HTTP, SMTP, POP3, Telnet, FTP and user defined proxies, respectively.

 Telnet service is associated with port 23, SMTP with port 25, FTP with port 21, HTTP with port 80 and POP3 with port 110. It is possible to specify that connections to any other ports are to be redirected to one of these proxies, but this is not the default setting and shouldn't be done, unless you have the knowledge of all possible consequences.

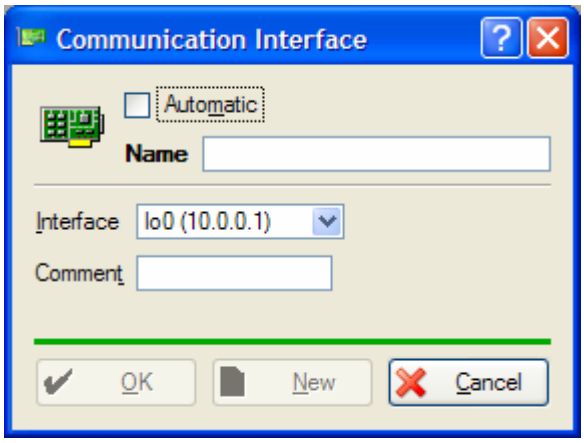
If it is specified that the connection is to be redirected to a proxy, it may be necessary to define the parameters of the context that will be used by the proxy for this service. If it is the case, the window will be expanded to shown the additional parameters that are to be configured.

The definition of the parameters of each context of the standard proxies can be found in the chapters Configuring the SMTP proxy, Configuring the Telnet proxy, Configuring the FTP proxy and Configuring the POP3 proxy. The HTTP proxy does not have configurable parameters and all its settings are described in chapter Configuring the WWW proxy. For further information about transparent proxies, refer to the chapter Working with proxies. User defined proxies are useful only to developers and its description will not be mentioned here.

After filling in all the fields, click on the **OK** button, to perform the service creation or modification. To cancel the modifications or the creation, click on the **Cancel** button.

To facilitate the creation of many services successively, there is a button called **New** (which is disabled during an edition). When clicked, this button will create the service whose data is filled in and the window will be kept open, ready for a new addition. This way, it is possible to create quickly a large number of services.

Creating / editing interfaces



To register an entity of the interface type, it is necessary to fill in the following fields:

Name: It is the name which will be used by the firewall to refer to the interface from now on. It is possible to specify this name manually or let it be automatically assigned. The option **Automatic** allows to choose between the two operation modes: if it is marked, the assignment will be automatic, otherwise, manual.

Entities names are case sensitive. This way, the existence of many entities whose names consist of the same letters, but with different capital and small letters combinations is possible. The entities **Aker, AKER** and **aker** are, then, considered different.

Icon: It is the icon that will appear, associated to the interface, in all references. To modify it, just click on the actual icon drawing. The firewall then will show a list of all the possible icons to represent interfaces. To select one of them click on the desired icon and on the **OK** button. If you don't want to modify the icon, after seeing the list, just click on the **Cancel** button.

Device: It is the name of the network adapter that will be associated with the interface entity. It will be shown automatically a list with all network adapters configured in the firewall and the IP address of each one, if it exists.

Comment: It is a free text field, used only for documentation purposes.

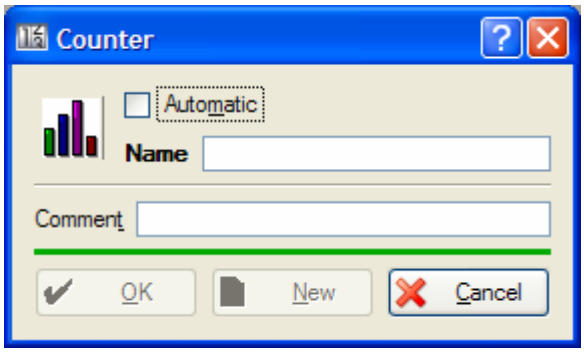
After filling in all the fields, click on the **OK** button, to perform the interface creation or modification. To cancel the modifications or the creation, click on the **Cancel** button.

To facilitate the creation of many interfaces successively, there is a button called **New** (which is disabled during an edition). When clicked, this button will create the interface whose data is filled in and the window will be kept open, ready for a new addition. This ways, it is possible to create quickly a large number of interfaces.

Creating / editing counters

Counters are entities used in filtering rules in order to generate statistics about the network traffic. A same counter can be used in many filtering rules and the traffic that

matches any of these rules is summarized by the counter. It's use is better described in chapters The Stateful filter and Viewing statistics.



To register an entity of the counter type, it is necessary to fill in the following fields:

Name: It is the name which will be used by the firewall to refer to the interface from now on. It is possible to specify this name manually or let it be automatically assigned. The option **Automatic** allows to choose between the two operation modes: if it is marked, the assignment will be automatic, otherwise, manual.

Entities names are case sensitive. This way, the existence of many entities whose names consist of the same letters, but with different capital and small letters combinations is possible. The entities **Aker, AKER** and **aker** are, then, considered different.

Icon: It is the icon that will appear, associated to the interface, in all references. To modify it, just click on the actual icon drawing. The firewall then will show a list of all the possible icons to represent interfaces. To select one of them click on the desired icon and on the **OK** button. If you don't want to modify the icon, after seeing the list, just click on the **Cancel** button.

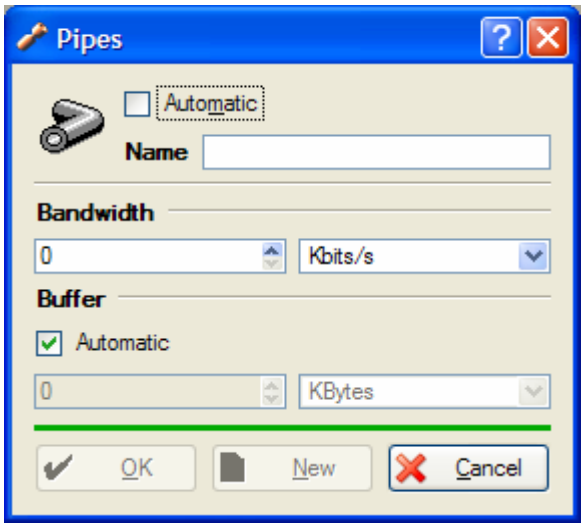
Comment: It is a free text field, used only for documentation purposes.

After filling in all the fields, click on the **OK** button, to perform the interface creation or modification. To cancel the modifications or the creation, click on the **Cancel** button.

To facilitate the creation of many interfaces successively, there is a button called **New** (which is disabled during an edition). When clicked, this button will create the interface whose data is filled in and the window will be kept open, ready for a new addition. This ways, it is possible to create quickly a large number of counters.

Creating / editing pipes

Pipes are entities used in filtering rules in order to limit the bandwidth of specific services, hosts, networks and/or users. It's use is described in chapter The Stateful filter.



To register an entity of the counter type, it is necessary to fill in the following fields:

Name: It is the name which will be used by the firewall to refer to the interface from now on. It is possible to specify this name manually or let it be automatically assigned. The option **Automatic** allows to choose between the two operation modes: if it is marked, the assignment will be automatic, otherwise, manual.

Entities names are case sensitive. This way, the existence of many entities whose names consist of the same letters, but with different capital and small letters combinations is possible. The entities **Aker, AKER** and **aker** are, then, considered different.

Icon: It is the icon that will appear, associated to the interface, in all references. To modify it, just click on the actual icon drawing. The firewall then will show a list of all the possible icons to represent interfaces. To select one of them click on the desired icon and on the **OK** button. If you don't want to modify the icon, after seeing the list, just click on the **Cancel** button.

Bandwidth: This field is used to specify the network bandwidth (maximum transmission speed in bits per second) of this pipe. This bandwidth will be shared among all connections that fit in this pipe. The most convenient measure unit can be selected.

Buffer: This field is used to specify the size of the buffer (temporary data space used to store packets that will be sent) of this pipe. The most convenient measure unit can be selected. It is possible to specify the size of the buffer, or let it be selected automatically. The option **Automatic** permits the selection between these two operation modes.

After filling in all the fields, click on the **OK** button, to perform the interface creation or modification. To cancel the modifications or the creation, click on the **Cancel** button.

To facilitate the creation of many interfaces successively, there is a button called **New** (which is disabled during an edition). When clicked, this button will create the interface

whose data is filled in and the window will be kept open, ready for a new addition. This ways, it is possible to create quickly a large number of pipes.

5-3 Using the command line interface

The use of command line interface for entities configuration is very simple and has almost the same capacities of the graphic user interface. The only missing options are the creation of services that use the transparent proxies and the edition of pseudo-groups of a certification authority. It is important to mention, however, that in the command line interface the external agents are created and displayed directly by their sub-type.

Program location: `/etc/firewall/fwent`

Syntax:

```
fwent help
fwent show
fwent remove <name>
fwent add host <name> <IP>
fwent add network <name> <IP> <mask>
fwent add set <name> [<entity1> [<entity2>] ...]
fwent add authenticator <name> <IP1> [<IP2>] [<IP3>] <passwd> <t.
cache>
fwent add token <name> <IP1> [<IP2>] [<IP3>] <passwd> <t. cache>
fwent add ldap <name> <IP1> [<IP2>] [<IP3>] <root_dn> <root_pwd>
               <base_dn> <act_class> <usr_attr> <grp_attr>
               < <pwd_attr>|<-bind> > < <-ssl>|<-tls>|<-none> >
               < <-no_pwd>|<-pwd> > <t. cache>
fwent add radius <name> <IP1> <port1> [ <IP2> <port2> ] <passwd> <t.
cache>
fwent add ids <name> <IP1> [<IP2>] [<IP3>] <passwd>
fwent add anti-virus <name> <IP1> [<IP2>] [<IP3>] <passwd>
fwent add url-analyzer <name> <IP1> [<IP2>] [<IP3>] <passwd>
fwent add ca <name> <root certificate filename> <CRLs download URL>
fwent add service <name> [TCP | UDP | ICMP | OTHER] <value>[..<value>]
fwent add interface <name> <device> [<comment>]
fwent add pipe <name> <bandwidth in Kbit/s.> [<queue size>
<bytes|slots>]
fwent add counter <name> [<comment>]
went add logger <name> <IP> [IP] [IP] <password>
```

Program help:

```
fwent - Command line interface for configuring entities
Usage: fwent help
       fwent show
       fwent remove <name>
       fwent add host <name> <IP>
       fwent add network <name> <IP> <mask>
       fwent add set <name> [<entity1> [<entity2>] ...]
       fwent add authenticator <name> <IP1> [<IP2>] [<IP3>] <passwd>
<t. cache>
       fwent add token <name> <IP1> [<IP2>] [<IP3>] <passwd> <t.
cache>
       fwent add ldap <name> <IP1> [<IP2>] [<IP3>] <root_dn>
<root_pwd>
                     <base_dn> <act_class> <usr_attr> <grp_attr>
                     < <pwd_attr>|<-bind> > < <-ssl>|<-tls>|<-none> >
                     < <-no_pwd>|<-pwd> > <t. cache>
       fwent add radius <name> <IP1> <port1> [ <IP2> <port2> ]
<passwd> <t. cache>
```

```
       fwent add ids <name> <IP1> [<IP2>] [<IP3>] <passwd>
       fwent add anti-virus <name> <IP1> [<IP2>] [<IP3>] <passwd>
       fwent add url-analyzer <name> <IP1> [<IP2>] [<IP3>] <passwd>
       fwent add ca <name> <root certificate filename> <CRLs download
URL>
       fwent add service <name> [TCP | UDP | ICMP | OTHER]
<value>[..<value>]
       fwent add interface <name> <device> [<comment>]
       fwent add pipe <name> <bandwidth in Kbit/s.> [<queue size>
<bytes|slots>]
       fwent add counter <name> [<comment>]
       fwent add logger <name> <IP> [IP] [IP] <password>
       show     = shows all the entities configured in the system
       add      = adds a new entity
       remove   = removes an existent entity
       help     = shows this message

For the remove / add commands:
       name     = name of the entity to be created or removed

For the add command:
       IP       = IP address of the network or host
       mask     = network mask

       entity   = name of the entities to be added to the set
                  (Only host and network entities can be added to a
set)

       passwd   = authentication agent access password
       t. cache = lifetime in seconds of an entry in the
authentication cache
       TCP      = service uses the TCP protocol
       UDP      = service uses the UDP protocol
       ICMP     = service uses the ICMP procotol
       OTHER    = service uses a protocol other than the above listed
       value    = Number that identifies the service. For the TCP and
UDP
                  protocols, it is the number of the port associated
with the
                  service. For the ICMP, it is the Type of Service and
for the
                  other protocols, the number of the protocol itself.
A range
                  can be specified through the value1..value2
notation, which
                  means the range between the value1 and value2
(inclusive).
For the add ldap command:
       root_dn  = DN of the root user the firewall will impersonate to
log on
       root_pwd = this user's password
       base_dn  = DN of the entry at which to start the search
       act_class= objectclass value for valid account objects
       usr_attr = the attribute where the username is stored
       grp_attr = the attribute where the groupname is stored
       pwd_addr = the attribute where the password is stored
       -bind    = does not try to fetch the password. Instead
                  try to bind to the LDAP server with the user's
credentials
       -ssl     = use ssl encrypted connection
       -tls     = use tls encrypted connection
```

```
       -none    = do not use encrypted connection
       -no_pwd  = allows users with blank passwords
       -pwd     = does not allow users with blank passwords
```

Example 1: (viewing the defined entities)

```
#fwent show
Hosts:
------
cache                     10.4.1.12
firewall                  10.4.1.11

Networks:
---------
AKER                      10.4.1.0        255.255.255.0
Internet                  0.0.0.0         0.0.0.0

Sets:
-----
Internal Hosts            cache                     firewall

Authenticators:
---------------
Authenticator NT          10.0.0.1
10.0.0.2                        600
Unix                      192.168.0.1     192.168.0.2
192.168.0.3      600

Token Authenticators:
---------------------
Token Authenticator        10.0.0.1
10.0.0.2                        600

IDS Agents:
-----------
IDS Agent                  10.10.0.1

Anti-Virus:
-----------
Local Anti-virus           127.0.0.1

Services:
---------
echo reply                ICMP  8
echo request              ICMP  0
ftp                       TCP   21
snmp                      UDP   161
telnet                    TCP   23

Interfaces:
-----------
External Interface        xl0
Internal Interface        de0
```

Example 2: (creating an host entity)

```
#/etc/firewall/fwent add host Server_1 10.4.1.4
Entity added
```

Example 3: (creating a network entity)

```
#/etc/firewall/fwent add network Network_1 10.4.0.0 255.255.0.0
Entity added
```

Example 4: (creating a service entity)

```
#/etc/firewall/fwent add service DNS UDP 53
Entity added
```

Example 5: (creating an authenticator entity)

```
#/etc/firewall/fwent add authenticator "Unix Authenticator" 10.4.2.2
password_123 900
Entity added
```

 The use of inverted commas ("") around the entity's name is mandatory when creating or removing entities whose names contain blank characters.

Example 6: (creating a set entity whose members are the hosts cache and firewall, previously created)

```
#/etc/firewall/fwent add set "Test set" cache firewall
Entity added
```

Example 7: (creating an entity of the interface type, without specifying a comment)

```
#/etc/firewall/fwent add interface "DMZ Interface" fxp0
Entity added
```

Example 8: (creating a token authenticator, using a primary host and a secundary one, as backup)

```
#/etc/firewall/fwent add token "Token Authenticator" 10.0.0.1 10.0.0.2
password 600
Entity added
```

Example 9: (removing an entity)

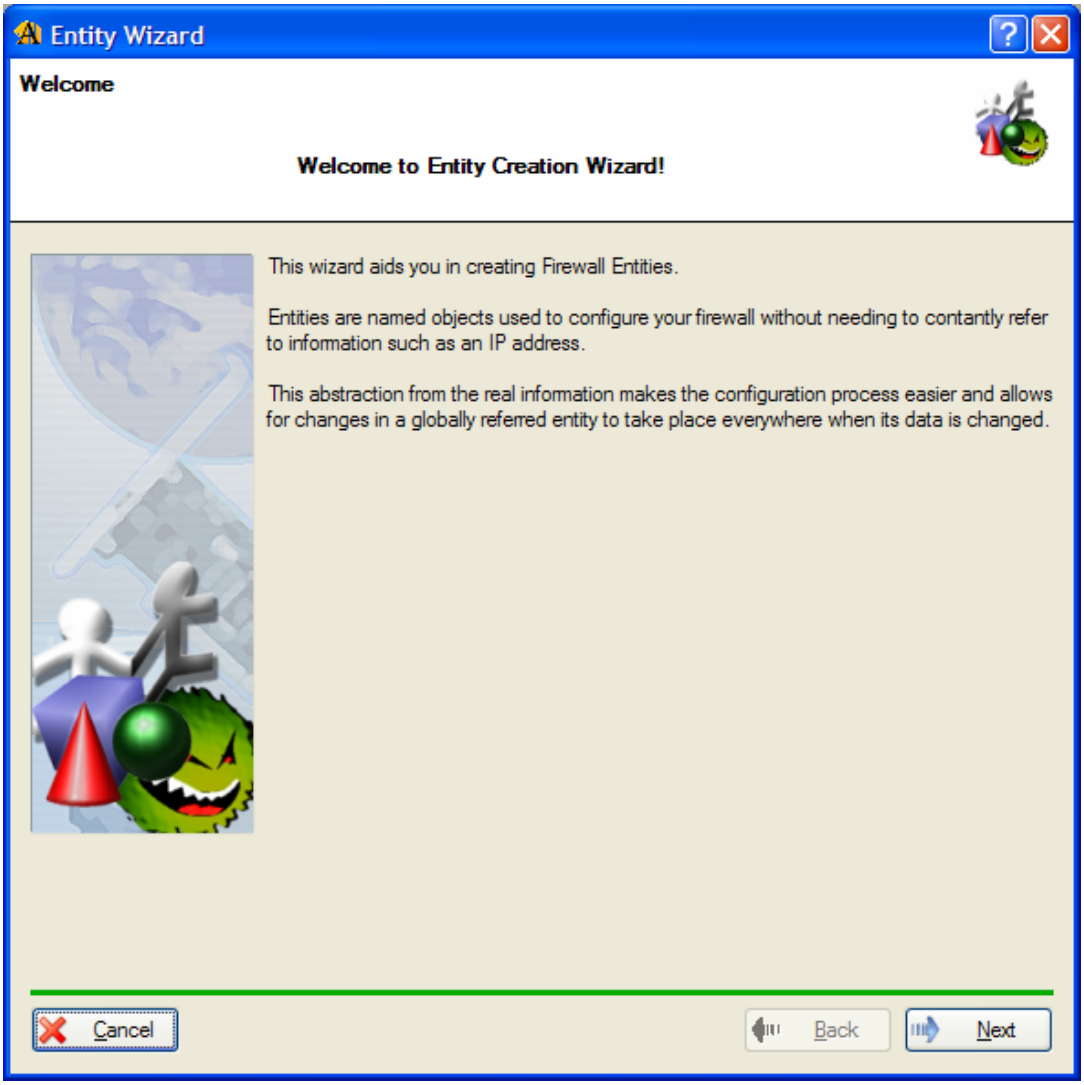
```
#/etc/firewall/fwent remove "Unix Authenticator"
Entity deleted
```

5-4 Using the Entities Wizard

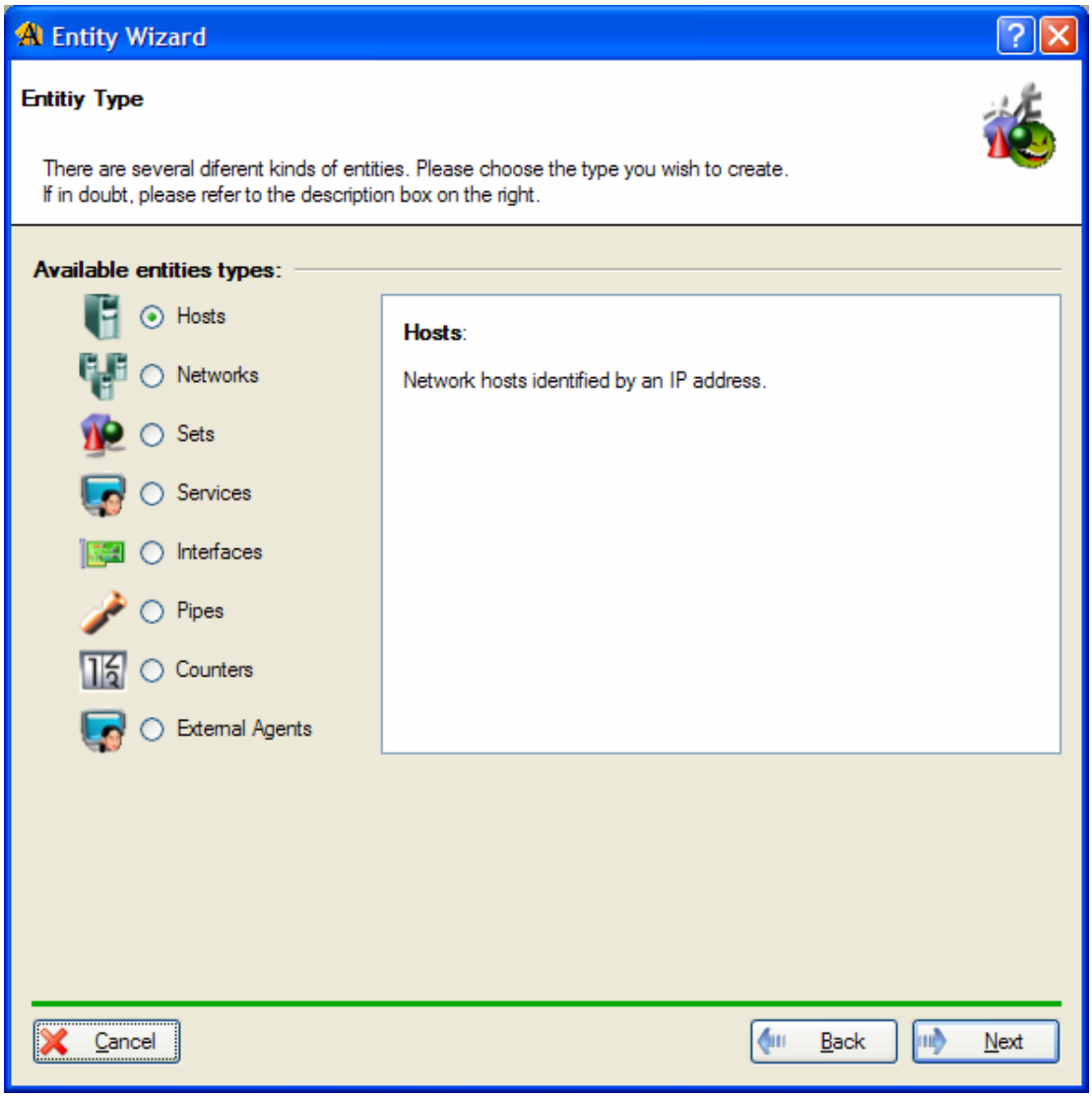
The entities creation wizard can be invoked by clicking on the icon , located in the lower part of the entities window. Its objective is to simplify the task of entities creation and can be used whenever you want. It consists of several windows displayed sequentially, depending on the type of entity to be created.

Its use is very simple and here will be shown, as an example, the creation of an entity of host type:

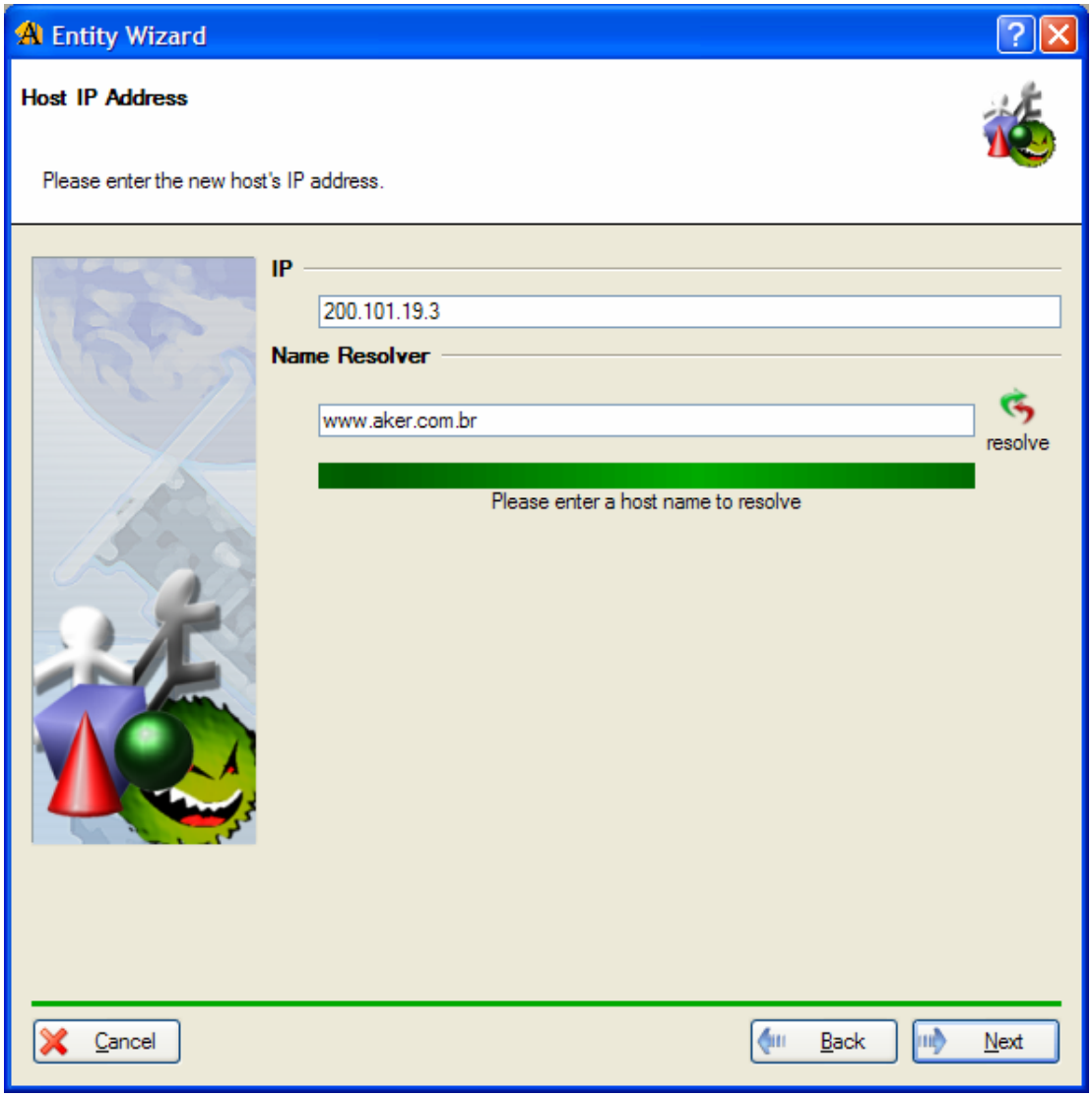
1 - The first widow displayed consists of a brief explanation of the procedures to be performed:



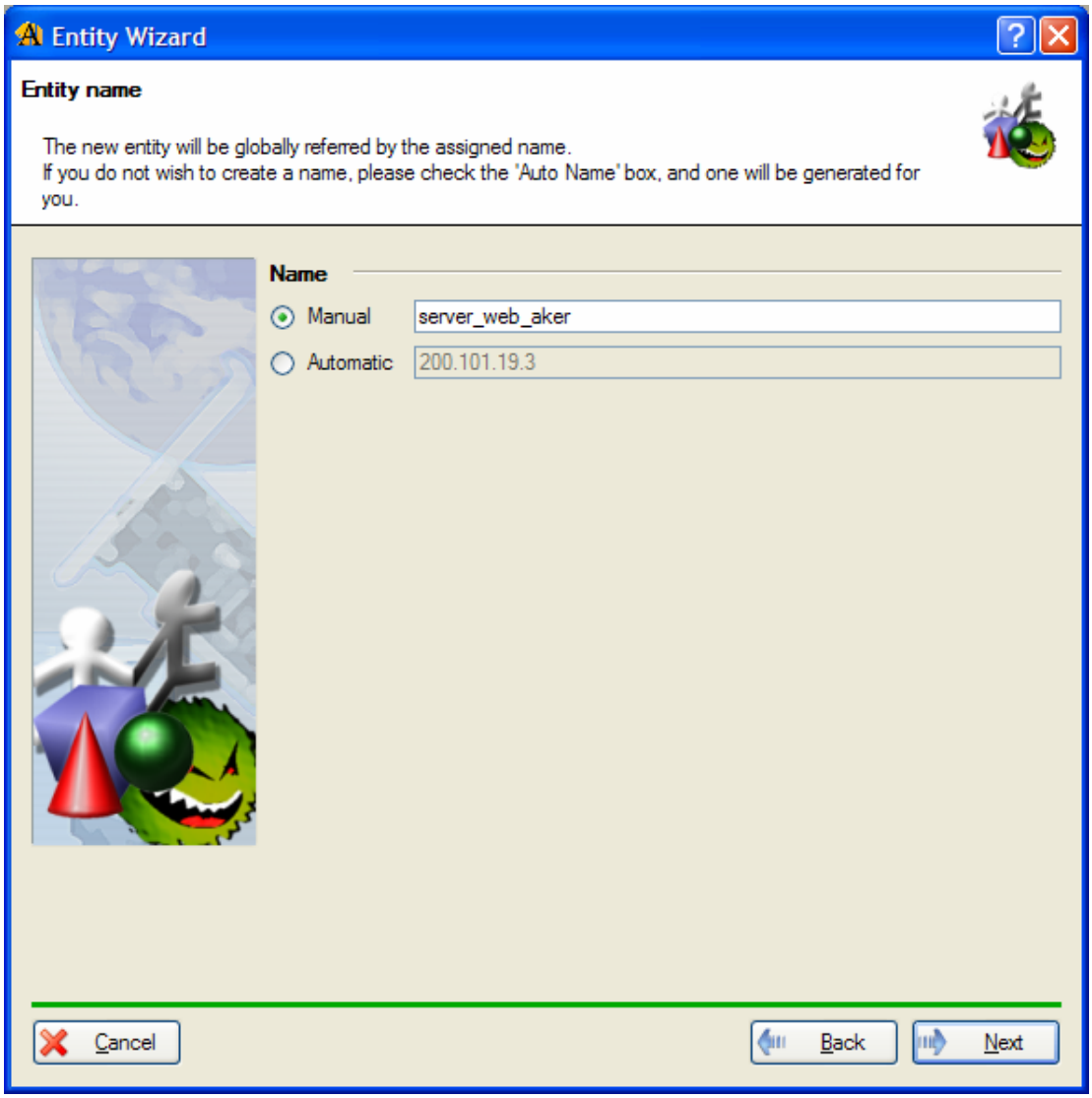
2 - In the second window, it is necessary to select the type of entity to be created:



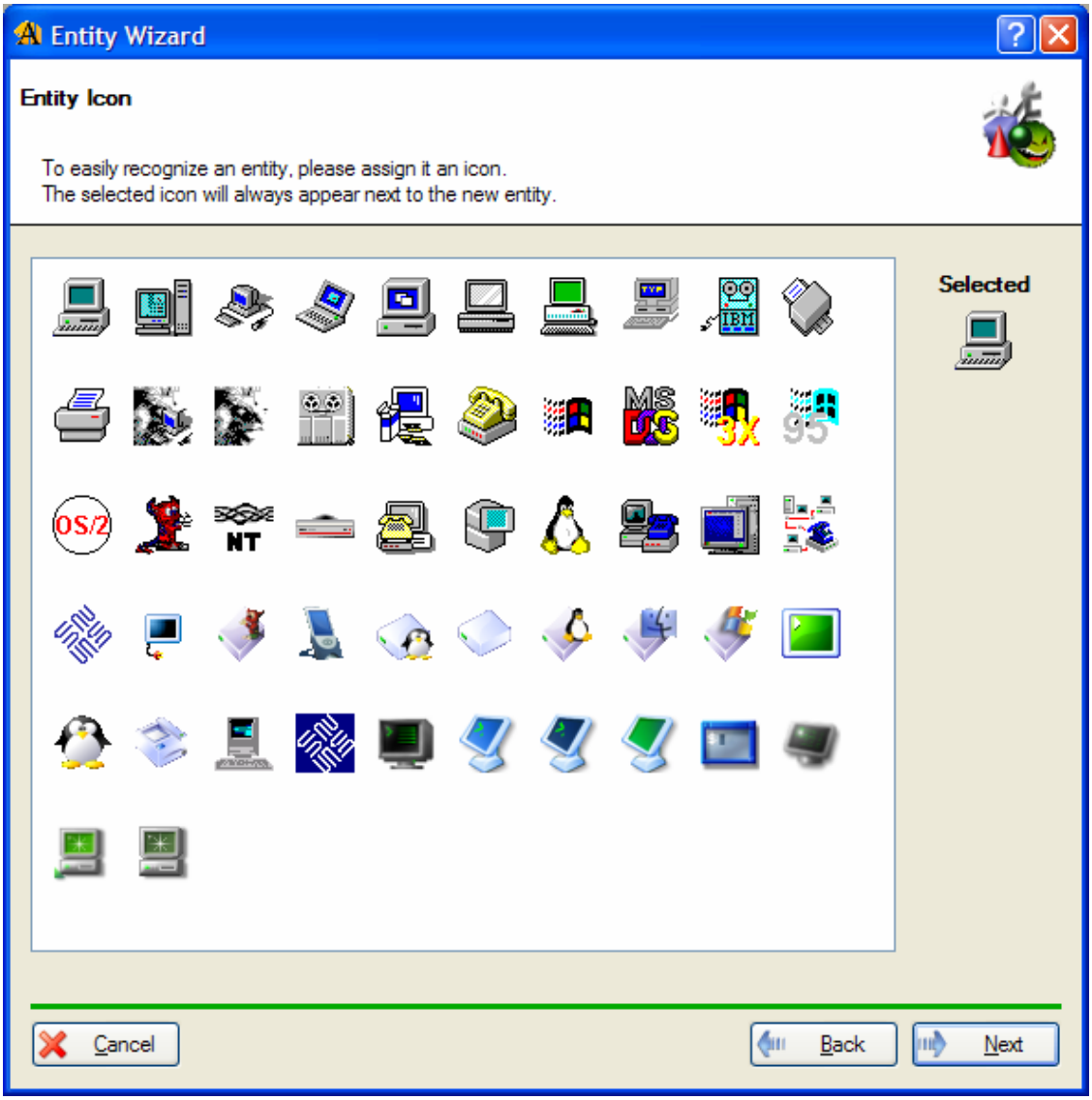
3 - In case of creation of a host entity, this window is used to define its IP address. It is possible to type in the name of the host and click on the *Resolve* button in order to obtain the corresponding IP address.



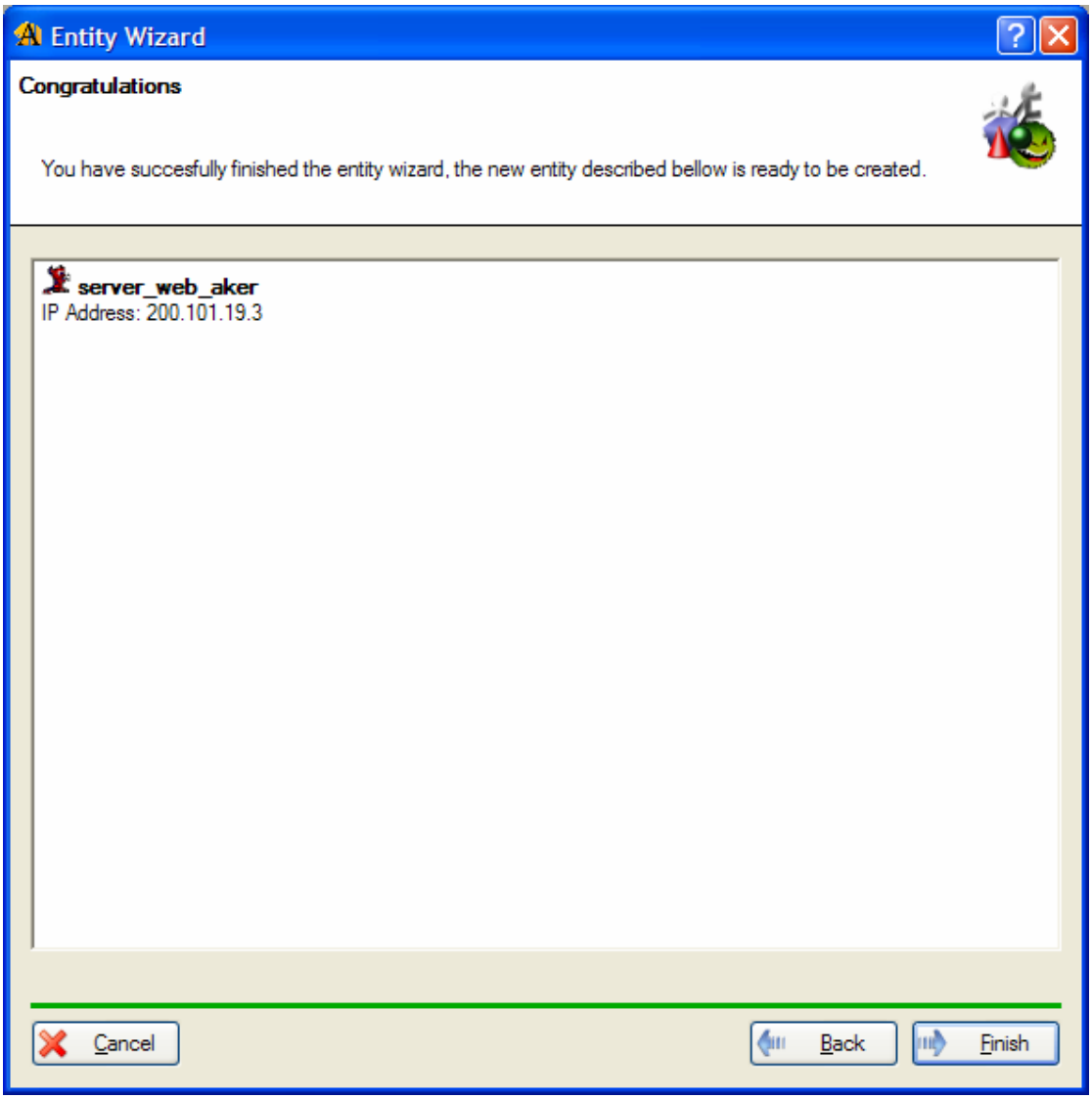
4 - This window is used to assign the entity name. You can choose a name or select the automatic naming option.



5 - This window is used to select the icon that will represent the entity. Click on any of the icons that appear on the window. Pay attention that the selected icon will be shown at the right of the window.



6 - Last step. It will be shown a summary of consisting of all entity data. It is enough to click on the **Finish** button in order to create the entity.



6-0 The Stateful Filter

This chapter shows how to configure the rules that will enable acceptance or rejection of connections by the Firewall. This module is the heart of the system and its configuration is also the most time consuming.

6-1 Planning the Installation

What's a packet filter?

A packet filter is the module that decides whether or not a packet will be allowed to pass through the firewall. Allowing a packet to pass implies the acceptance of a specific service. Blocking a packet means impeding consumption of this service.
The packet filter has a set of rules, configured by the system administrator, to help determine which action should be taken with each incoming packet. Every time a packet is received by the Firewall, the packet filter verifies if it matches any of the rules, in the order in which they are listed. If there is a match, the action associated with the rule is executed. Otherwise, the default action is taken.

What's the Firewall Aker stateful filter?

A traditional packet filter takes its action based solely on the set of rules configured by the administrator. For each packet that may pass the filter, the administrator must configure a rule that will accept or reject it. Sometimes it is simple, but in others it is just impossible to be done, or at least, with the necessary security and flexibility.
The Firewall Aker packet filter is called stateful filter because it stores information about the state of all connections flowing through it, and uses this information, along with rules configured by the administrator, to accept or reject a specific packet. In addition, unlike packet filters that only use packet header data to decide, the stateful filter verifies the data in every packet layer before accepting or rejecting it.
Let's analyze how this capability resolves several commonly found problems with traditional packet filters.

The problem with the UDP protocol:

To use a UDP service, the client machine initially chooses a port number (which changes every time a service is used), and sends a packet to the fixed port of the server hosting the service. At the request, the server responds with one or more packets to the port chosen by the client machine. To establish communication, the firewall has to accept the request and response packets. The problem is that the UDP protocol is not connection-oriented, which means that if a specific packet is observed in isolation, without its context, it becomes impossible to determine if the packet is a service request or a response.

With traditional packet filters, since the administrator cannot anticipate which port will be chosen by the client machine to access a certain service, it can only either block all

UDP traffic, or accept packets through every possible port. Both approaches have obvious problems.

The Firewall Aker solves these types of problems by dynamically adapting itself to the traffic. Every time a UDP packet is accepted by one of the rules configured by the administrator, a record is added to an internal table, called the “Stateful Table”. This table is consulted again later to allow the return of the corresponding service response packets to the client machine.

This stateful table record remains active only for a short period of time, before being removed (this period of time is configured in the parameters configuration window, shown in the Configuring the system parameters chapter). Thus, the administrator does not need to worry about the UDP response packets. It is just necessary to configure the rules to allow incoming packets to have access to the services. This can easily be done, since all services have fixed ports.

The problem with the FTP protocol:

FTP is one of the most popular Internet protocols, but it’s also one of the most complex for a firewall. Let’s analyze its operation:

To access an FTP service, the client host initially opens a TCP connection between one of its ports and port 21 of the server (the port used by the client machine varies). This connection is called control or data connection. Afterwards, for every downloaded file or directory listing, a new control connection is established. It’s called data connection. This data connection can be established in two different ways:

1. The server can initiate a connection from port 20 to a variable client port, provided by the client, through the control connection (this is called **active FTP**).
2. The client can open the connection from one of its variable ports to a variable port at the server, provided to the client by the server itself, through the control connection (this one is called **passive FTP**).

In both cases, the administrator defining filtering rules has no way to know which ports will be chosen to establish the data connection. Therefore, if the FTP protocol is to be used with a traditional packet filter, packages from all possible client and server ports must be accepted. This has serious security implications.

Firewall Aker scans the data traffic going through the FTP control connection and finds out which type of transfer will be used (active or passive) and which ports will establish data connection. This way, every time the packet filter detects that a file transfer will take place, it adds an entry into the stateful table, allowing data connection. This entry remains active while the transferring process is going on and the control connection is open, to ensure maximum flexibility and security. In this case, to configure FTP access, it is only necessary to add a rule allowing access to the control connection port (21). Everything else is done automatically.

The problem with Real Audio protocol:

The Real Audio protocol is the most popular for real time Internet audio and video transfers.

To make an audio or video transmission, the client needs to establish a TCP connection to the Real Audio server. Additionally, in order to improve sound quality, the server can open a UDP connection to the client, to a random port informed in real time to the client. In turn, the client can also open another UDP connection to the server, also in a random port informed by the server during the connection.

For not knowing the ports in advance, traditional packet filters do not allow UDP connections from the server to the client and vice-versa. Therefore, causing very low audio and video quality.

Firewall Aker stateful filter keeps track of all the negotiation between the Real Audio server and the client, in order to determine if the UDP connections will be opened and to which ports, and adds this information to an entry in its stateful table. This entry remains active while the TCP control connection is open, ensuring maximum security.

The problem with Real Video protocol (RTSP):

Firewall Aker now supports the Real Video protocol. As it happens with Real Audio, the firewall controls the transactions, ensuring total security in Real Video applications.

Creating filtering rules in a simple packet filter

Before showing the configuration of Firewall Aker stateful filter, it is interesting to explain the basic operation of a simple packet filter:

There are several possible criteria to perform packet filtering. Address filtering may be considered the most simple: it compares the packet addresses with the rules addresses. If they match, the packet is accepted. This comparison occurs as follows:

We will work with the following rule:

"All hosts of network 10.1.x.x can communicate with hosts of network 10.2.x.x." We will write this rule using the masking concept (for more information, read chapter Registering Entities). Thus, we will have:

```
10.1.0.0 & 255.255.0.0 => 10.2.0.0 & 255.255.0.0
--------- Source ---------       ------- Destination -------
```

Let's now apply the rule to a packet that runs from host 10.1.1.2 to host 10.3.7.7. We will apply the rule's mask to both the rule and the packet addresses. And will verify if the source and destination addresses are the same.

For the source address we have:

```
10.1.0.0 AND 255.255.0.0 => 10.1.0.0 (for the rule)
10.1.1.2 AND 255.255.0.0 => 10.1.0.0 (for the packet)
```

After applying the mask, both source addresses match. Now, let's check the destination address.

```
10.2.0.0 AND 255.255.0.0 = 10.2.0.0 (for the rule)
10.3.7.7 AND 255.255.0.0 = 10.3.0.0 (for the packet)
```

Since, after applying the mask, the packet destination address does not match the rule destination address, by definition, this rule would not apply to this packet.

This operation is performed on the entire list of source and destination addresses and masks, or until a rule-packet match is found. A list of rules would look like the following:

```
10.1.1.2 & 255.255.255.255  =>    10.2.0.0 & 255.255.0.0
10.3.3.2 & 255.255.255.255  =>    10.1.2.1 & 255.255.255.255
10.1.1.0 & 255.0.0.0        =>    10.2.3.0 & 255.255.255.0
10.1.0.0 & 255.255.0.0      =>    10.2.0.0 & 255.255.0.0
```

In addition to source and destination addresses, each IP packet has associated service and protocol. This combination of service plus protocol can be used as one more filtering criterion.

TCP protocol services, for example, are always associated to a port (for more information, go to chapter Registering Entities). Therefore, it is also possible to associate a list of ports to addresses.

Let's use POP3 and HTTP, two well-known services, as examples. POP3 is associated to server port 110, and HTTP to port 80. We will add these ports to the rule format. We, then, will have:

```
10.1.0.0 & 255.255.0.0 => 10.2.0.0 & 255.255.0.0     TCP        80 110
-------- Source --------       ------ Destination ----   - Protocol -   --Ports--
```

This rule allows every packet that goes from network 10.1.x.x to network 10.2.x.x, and that uses HTTP or POP3 services, to pass through the firewall.
Then, as a first step, we compare rule addresses with packet addresses. If they match, after applying the masks, we continue comparing the packet protocol and destination port with the protocol and list of ports associated to the rule. If the protocol is the same, and if there is a rule port equal to the packet port, by definition, this rule applies to the packet. Otherwise, the search continues with next rule.

Thus, a set of rules would have the following format:

```
10.1.1.2 & 255.255.255.255 => 10.2.0.0 & 255.255.0.0 UDP 53
10.3.3.2 & 255.255.255.255 => 10.1.2.1 & 255.255.255.255 TCP 80

10.1.1.0 & 255.0.0.0 => 10.2.3.0 & 255.255.255.0 TCP 21 20 113
10.1.0.0 & 255.255.0.0 => 10.2.0.0 & 255.255.0.0 ICMP 0 8
```

Creating Firewall Aker Filtering Rules

It is very easy to configure filtering rules in the Firewall Aker because of its intelligent conception. IP addresses, masks, protocols, ports and interfaces are configured through the entities (for further information, refer to chapter Registering Entities). Therefore, when configuring a rule, there is no need to worry about which port a specific service uses or with the IP address of a determined network. All these things have been previously configured. Furthermore, to make it even easier, the most used Internet services are factory pre-set, which means no wasting time researching their data.

Basically, to create a rule, the administrator must specify source and destination entities, as well as the services that will make up the rule. A source interface for the packets might define when the rule will be active, within a weekly timetable. With this timetable, it is possible to make specific services available at certain times of the day (for instance, freeing IRC or chat only after working hours). If a packet is received when a certain rule is not active, the rule will be ignored, and the search will continue with the following rule of the list.

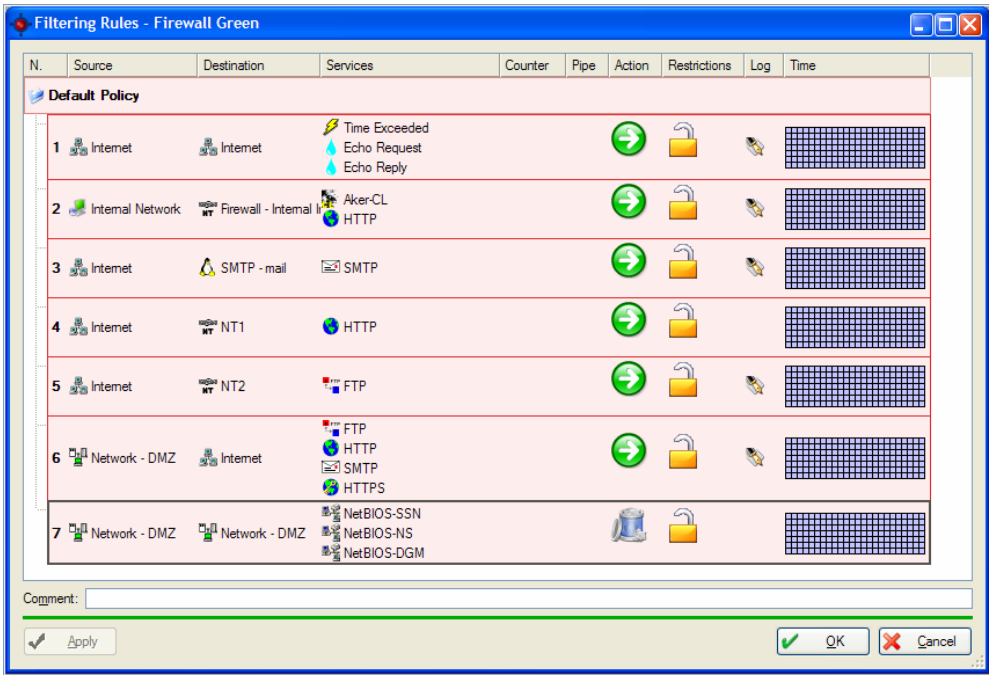
The filter operation is simple: the firewall searches each single rule defined by the administrator, in the specified order, until the packet matches one of them. Then, it executes the action associated to the matching rule, which can be either “accept,” “reject” or “discard” (these values are explained in the following section). If the search reaches the end of the list and the packet does not match any rule, then it will be discarded (it is possible to configure actions to be executed in this case. This is explained in the Configuring System Actions chapter).

6-2 Editing a List of Rules Using the Graphical User Interface

In order to have access to the rules configuration window, you need to:

- Click on the Firewall *Configuration in main* window
- Select the *Filtering Rules* item

The Filtering Rules Window

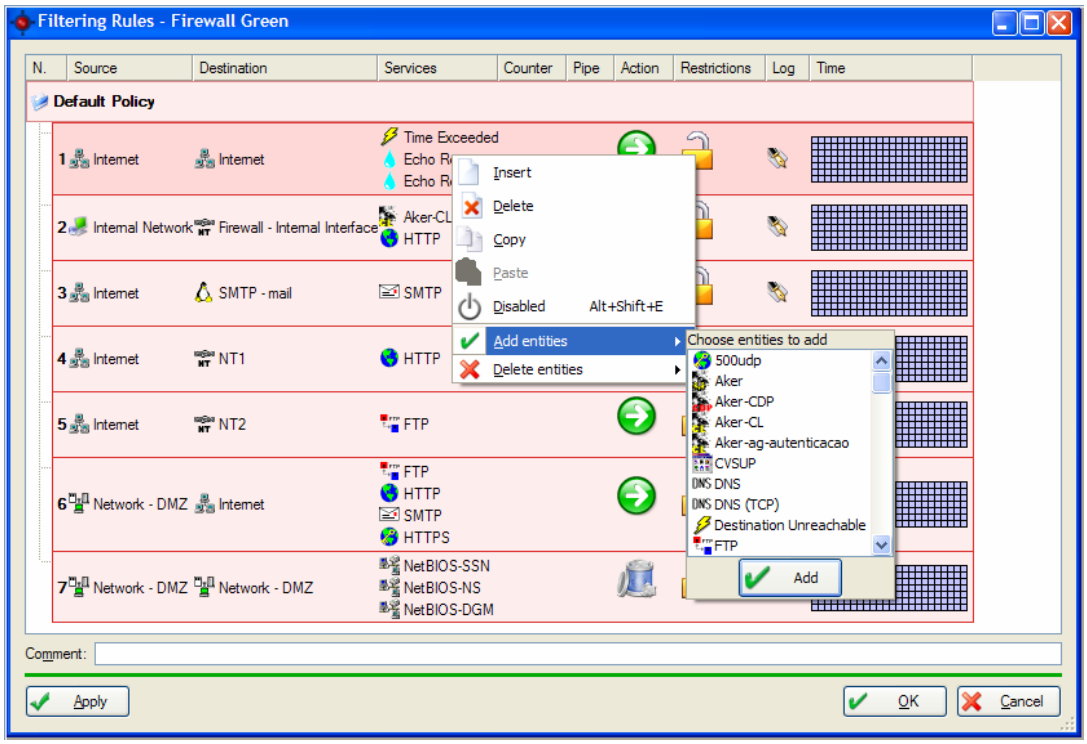


The rules window contains all filtering rules defined in the Firewall Aker. Each rule is displayed on a separate row, made of several cells. A selected rule will be displayed in a different color.

- The OK button updates the set of rules and makes it immediately active.
- The Cancel button discards any modification and closes the window.
- The Apply button sends all alterations to the firewall and keeps the window open.

- If a rule is selected and it has a comment, this comment will be displayed at the bottom of the window.

To execute any operation on a specific rule, just right click over the field you want to modify. A menu will be displayed with the entities options for that field, as shown below:



- Insert: This option records a new rule into the list. If any existing rule is selected, the new one will be inserted in its place, pushing it down the list. Otherwise, the new rule is appended to the end of the list.
- Delete: This option removes the selected rule from the list.
- Edit: Opens the editing window with the selected rule.
- Copy: Copies the selected rule into a temporary area.
- Paste: Copies the rule from the temporary area to the list. If any rule is selected, the new one will be copied into its place, pushing it down the list. Otherwise, it will be appended to the end of the list.
- Enable/Disable: This option enables/disables the chosen rule.

Hint: You can change the position of a rule on the list just by clicking on it, dragging and dropping it at the new position.

Adding and removing entities and services from a rule

There are two ways to add an entity to one of these fields:

1. In the entities table (located at the bottom left corner of the window), click on the entity you wish to add to a field. Drag it to the target field. The Insert and Delete keys can insert and remove entities respectively.
2. Right click on the field where you want to add the entities. An entities list for that field will be displayed, as well as the type of action applicable to them.
3. To edit an entity, double-click on it.

To remove an entity from one of these fields, do the following:

1. Right click on the field that contains the entity you wish to remove. A list of that field's entities will be displayed along with a delete option, in the following format: delete 'entity_deleted'.
2. You can use the Delete Entities option to eliminate several entities at the same time.

- **Rule parameters:**

In addition to basic rule specifications, such as source entities, destination entities, and services, we must consider other configuration parameters:

Counter: Defines rule packets counter. When the None option is chosen, the system stops counting the packets that match this rule. If a counter is chosen, the amount of bytes and packets matching this rule will be added to it.

Pipe: Defines the pipe that will control the rule bandwidth. The None option deactivates bandwidth control for this rule.

Action: This field defines the action that will be executed with all packets that match this rule. It has the following options:

Accepts: The packets matching this rule will be allowed to pass through the firewall.

Rejects: Packets matching this rule will not pass through the firewall. An ICMP packet informing that the destination is unreachable will be sent to the source host.

Discards: The packets that match this rule will not be allowed to pass through the firewall, and no packet will be sent to the source host.

Restrictions: This field is to specify additional requirements a packet needs to satisfy in order to match the rule. It has the following options:

None: There is no additional requirement.

Only if encrypted: To match this rule, a packet must have been previously Encrypted/authenticated, i.e., must come from a secure channel: This option is especially useful when encryption clients are being used and it is desired that only connections coming from these clients be accepted (or from firewall-firewall secure channels). For more information on encryption and secure channels, go to chapter Creating Secure Channels.

Only if encrypted and from an authenticated user: In this case, packets must be not only encrypted and authenticated, but also the user who established the secure channel must have been authenticated by the firewall. The only way a packet can meet this requirement, is if it comes from an encryption client, and the authenticated users option is active. For more information on encryption and secure channels, read chapter Creating Secure Channels.

Log: Defines the types of actions the system will execute when a packet matches this rule. It has several options that can be independently selected.

Logs: When this option is selected, all packets matching this rule will be registered in the system log.

Sends email: When this option is selected, an email is sent every time a packet matches this rule (email address configuration can be found in chapter Configuring System Actions.)

Sends SNMP Trap: If this option is selected, for each packet that matches this rule, an SNMP Trap will be sent (trap sending configuration parameters are explained in chapter Configuring System Actions.)

Executes Program: With this option selected, every time a packet meets this rule, a program defined by the administrator is executed (the configuration of the program name is shown in chapter Configuring System Actions).

Triggers Alarm: If this option is on, the firewall will show a warning window every time a packet matches this rule. This window will be displayed in the host where the remote GUI is open. And, if the host allows, there will also be a sound warning. If the GUI is not open, no message will be displayed and this option will be ignored.

With TCP protocol, only the actions defined in the opening connection packet rule will be executed. With UDP protocol, all packets sent by the client host, and which match the rule, will trigger the actions. The same does not apply to response packets.

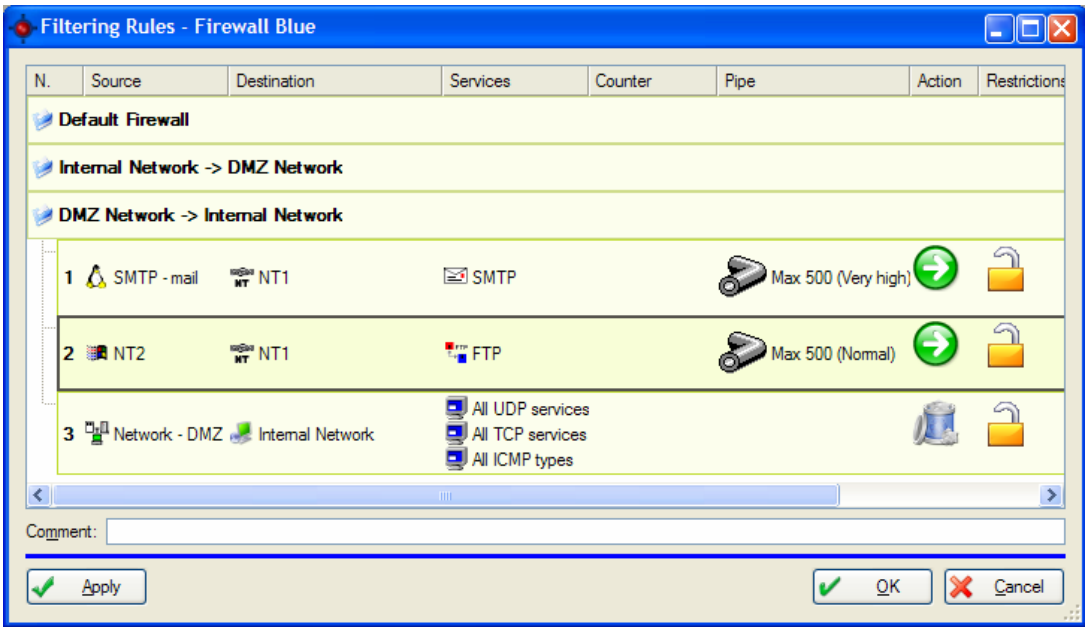
Time: Defines times of the day and days of the week during which the rule is applicable. Rows represent days of the week, and columns represent time of day. To apply the rule at a specific time, the corresponding square must be filled, otherwise, it must be left blank.

To make this configuration easier, just click on a square and drag the mouse over the table, keeping the left button pressed. The timetable is modified as the mouse passes over it.

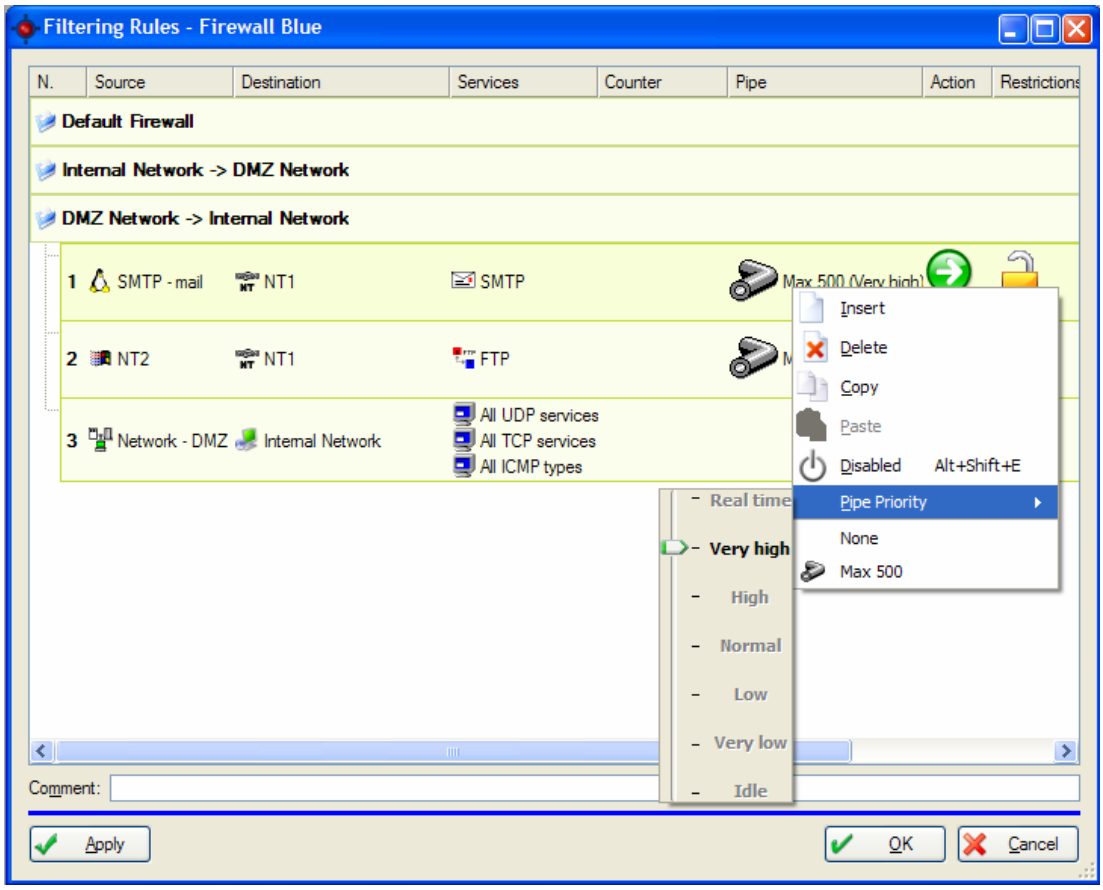
Comment: Used to add a comment about the rule. Very useful for usage documentation and rule maintenance purposes.

Using Pipes in the Firewall Aker Filtering Rule

The administrator can define different Quality of Service (QoS) levels for each rule type. In the example below, a 500 Kbit-pipe/channel was created and rules 8 and 9 were applied. The server Mail_SMTP has traffic priority, because its pipe/channel priority is set as “Very high.”



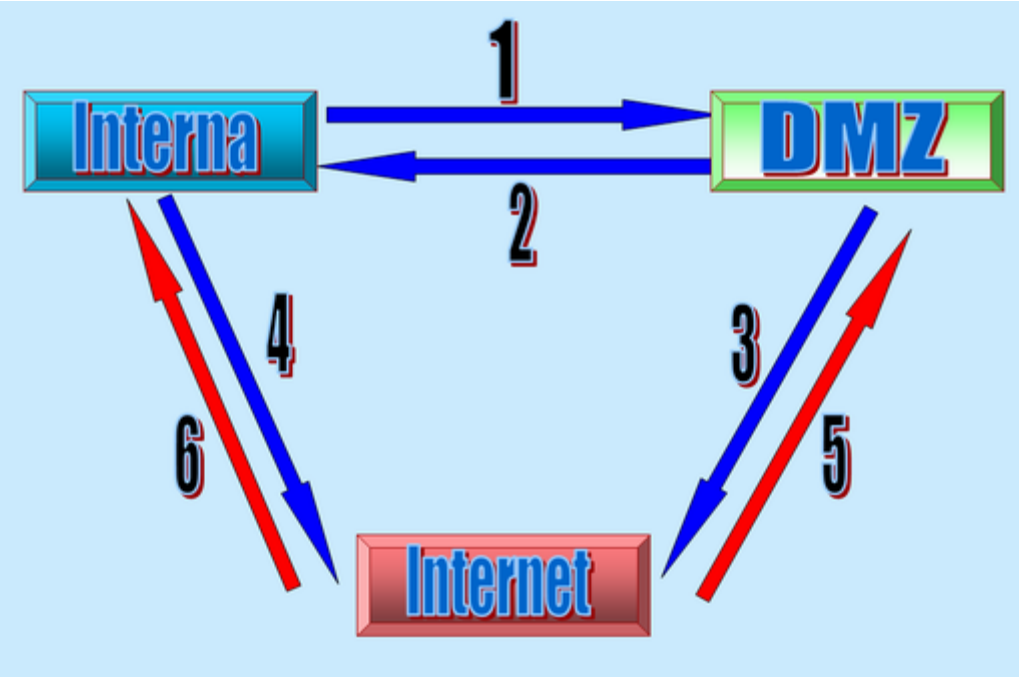
To adjust pipe priority, right-click on the entity Pipe and slide along the button to choose the priority. See the graphical representation below:



6-3 Working with Filtering Policies

Filtering Policies is a new feature added to the Firewall filtering rules configuration. This resource allows the firewall administrator to group rules according to subnetworks traffic flows.

To illustrate it better, let's suppose that the administrator has a firewall placed between the Internal network, the DMZ network and the Internet, as seen below:



We can verify the possible data flow that may happen between these networks. Each flow was given a number. We can conclude that flows number 5 and 6 are considered the least secure, because they represent Internet access to DMZ and Internal networks, respectively.

These flows into the firewall will be architected as filtering rules. Thus, we could have the following rules:

Filtering Rules

N.	Origem	Destino	Serviços	Acumulador	Canal	Ação	Restrições	Log	Hora
1	Maquina_Admin	Firewall_Interno	Aker						
2	Internet	Internet	Echo Reply Echo Request						
3	Internet	Firewall Externo	Aker-CDP Aker-CL						
4	Internet	Firewall Externo Firewall_Interno Firewall DMZ	todos TCP todos UDP todos ICMP todos Outros						
5	server1	Correio_SMTP	SMTP						
6	Rede_Interna	servidor_web	HTTP						
7	Rede_Interna	Rede_DMZ	todos ICMP todos Outros todos TCP todos UDP						
8	Correio_SMTP	server1	SMTP						
9	NT2	server1	FTP						
10	Rede_DMZ	Rede_Interna	todos ICMP todos Outros todos TCP todos UDP						
11	Rede_Interna	Server_pop3	POP3						
12	squid_proxy	Internet	HTTP HTTPS						
13	Rede_Interna	Internet	todos ICMP todos Outros todos TCP todos UDP						
14	NT1	Internet	DNS DNS (TCP)						
15	NT3	Rede_Verde	FTP						
16	Rede_DMZ	Internet	todos ICMP todos Outros todos TCP todos UDP						
17	Internet	NT3	DNS (TCP) DNS						
18	Internet	servidor_web	HTTP						
19	Internet	Rede_DMZ	todos ICMP todos Outros todos TCP todos UDP						
20	Internet	Rede_Interna	todos ICMP todos Outros todos TCP todos UDP						

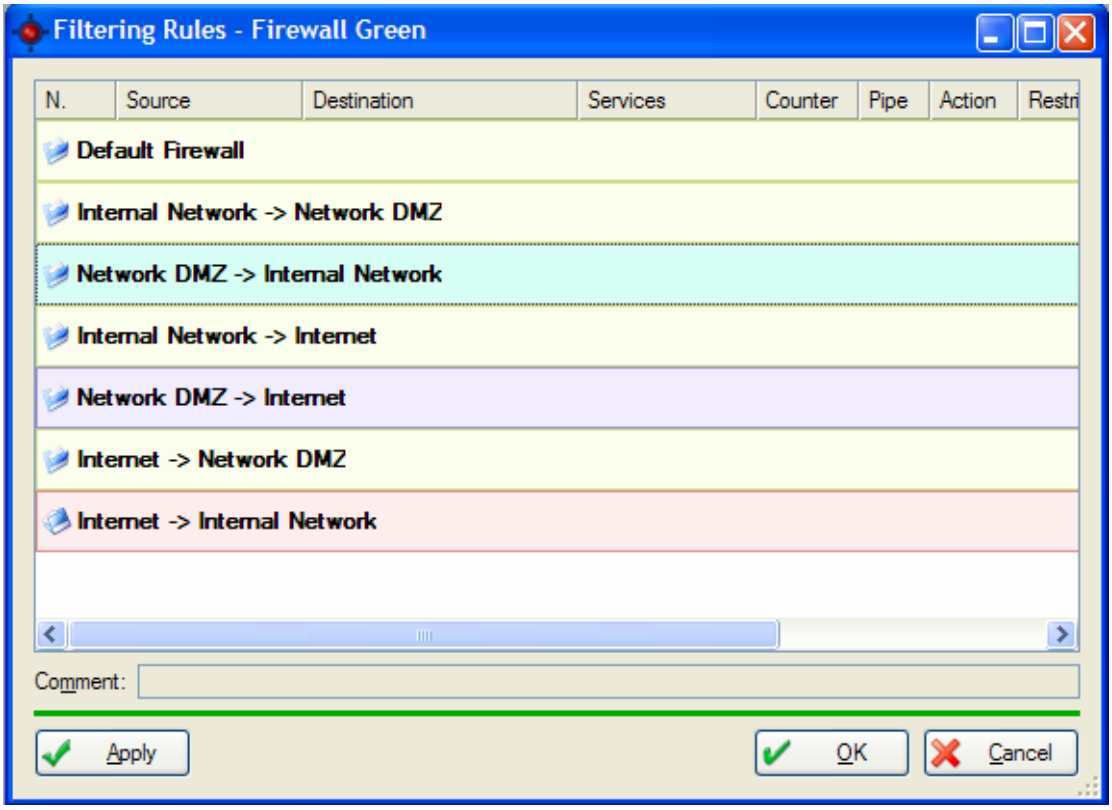
In the above example the following rules were created:

General Firewall Rules -> 1 to 4
Internal to DMZ flow -> 5 to 7
DMZ to Internal flow - > 8 to 10
Internal to Internet flow -> 11 to 13
DMZ to Internet flow -> 14 to 16
Internet to DMZ flow -> 17 to 19
Internet to Internal flow -> 20

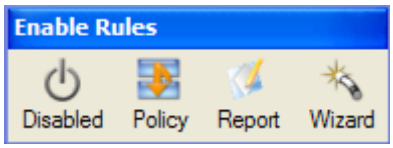
Note that a rule was placed at the end of each flow, blocking it (4, 7, 10, 13, 16, 19 and 20). The objective of this technique is to avoid that mistakes made during filtering rules configuration may open, unexpectedly, a non-authorized access. Thus, if a rule is not correctly placed in the flow, it will eventually fall in one of these rejection blocks, avoiding unauthorized access.

Observe that in the Internet-to-Internal network flow there is no configured rule, just the block.

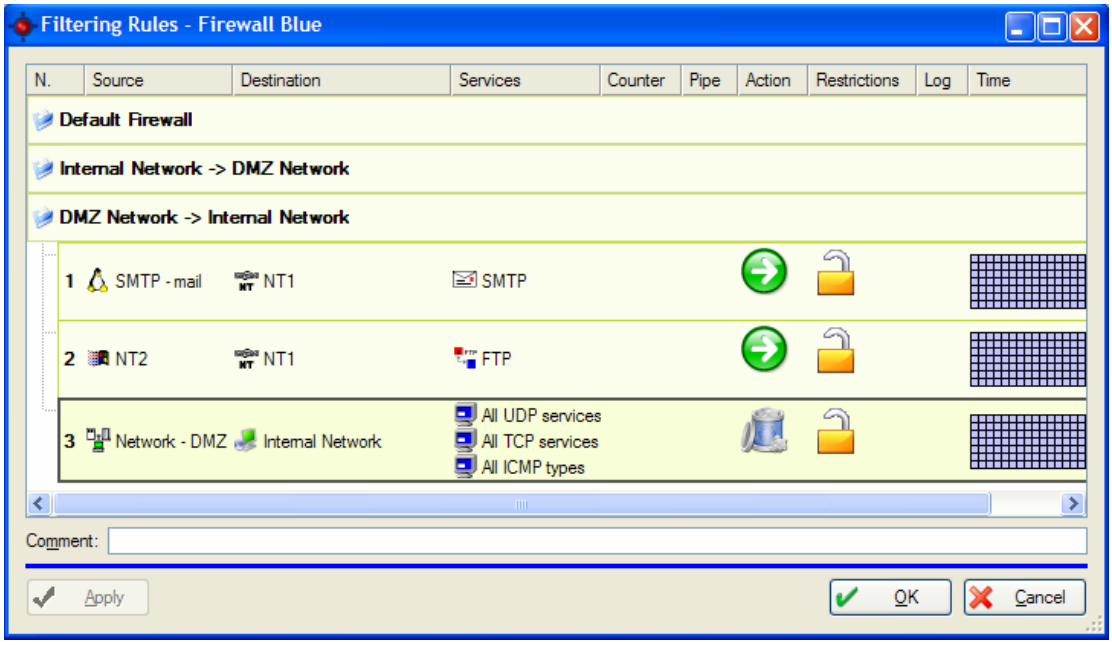
For increased visualization and control, the firewall enables the grouping of these rules according to the flow type. The interface would look like the following:



To create Policies, just click on the Policy icon in the toolbar.



The picture below shows how the policy rules unfold. Just double click on the row to display its rules:



If a policy is disabled, all rules associated to it are also disabled.

6-4 Using the Command Line Interface

Configuring filtering rules through the command line interface is comparatively harder than through the GUI because of the great number of parameters that must be input.

It is not possible to configure the timetable, or to add comments to the rules using the text interface. Specifying more than one entity to the rule source or destination is also not feasible. All rules added through the command line interface are considered permanent, to be applicable all times of the week.

Program location: `/etc/firewall/fwrule`

Syntax:

Usage:

```
fwrule [help| show]
fwrule [enable | disable | remove] <pos>
fwrule add <pos> <source> <destination> <accept | reject | discard>
                 [pipe <pipe> <weight>] [counter <counter>]
                 [log] [email] [trap] [program] [warning]
                 [encrypted | user ] [<service> ...]
```

Program Help:

```
Firewall Aker - Version 5.0
fwrule – Configures rules table for the stateful filter
Usage: fwrule [help | show]
fwrule [enable | disable | remove] <pos>
fwrule add <pos> <source> <destination> <accept | reject | discard>
                [pipe <pipe> <weight>] [counter <counter>]
                [log] [email] [trap] [program] [warning]
                [encrypted | user ] [<service> ...]

show             = displays all rule table records
add              = adds a new filtering rule
enable           = enables a disabled filtering rule
disable          = disables an existing filtering rule
remove           = deletes an existing rule
help             = displays this message

For the ‘add’ command, we have the following:

pos              = rule position where to add the new rule
                   (It can be a positive integer, or the word END to
add
                    the rule to the end of the table)
accept           = the rule accepts connections that match it
reject           = the rule rejects matching connections and sends an
                   ICMP packet of unreachable destination to the
source
discard          = the rule discards packets received (does not send
an
                   ICMP packet)
pipe             = directs the traffic that matches this rule to the
                   specified “pipe,” with a relative  weight given
```

```
by:
counter          = adds the traffic matching this rule to the entity
                   counter specified.
weight           = "idle", "v_low" (very low), "low", "normal",
"high",
                   "v_high" (very high) or "rt" (real time)
log              = logs the packets that match the rule
email            = sends an email each time a packet matches the rule
trap             = generates an SNMP trap each time a packet matches
the
                   rule
program          = executes a program each time a packet matches the
                   rule
warning          = shows a warning window for each packet that
matches
                   the rule
encrypted        = indicates that the rule is only valid if packets
come
                   encrypted and user has been previously
authenticated
                   in the firewall. This condition can only be met by
                   connections originated from Encryption Clients.
service          = list of services for the new rule

For the 'enable / disable / remove' commands, we have:
pos              = number of the rule to be enabled, disabled, or
                   removed
```

Example 1: (showing filtering rules)

```
#/etc/firewall/fwrule show

Rule 01
--------
Source         : Internet
Destination    : firewall cache
Action         : Discard
Log            : Log Trap Warning
Services       : all_tcp all_udp all_icmp

Rule 02
--------
Source         : cache firewall
Destination    : Internet
Action         : Accept
Log            : Log
Services       : http ftp

Rule 03
--------
Source         : Internet
Destination    : Mail server
Action         : Accept
Log            : Log
Services       : smtp

Rule 04
--------
Source         : External companies
Destination    : Aker
Action         : Accept
```

```
Log             : Log
Services        : smtp
```

Example 2: (removing the fourth filtering rule)

```
#/etc/firewall/fwrule remove 4
Rule 4 removed
```

Example 3: (adding a new rule to the end of the table)

```
#/etc/firewall/fwrule add end Internet "Mail server" accept log smtp
Rule added into position 4
```

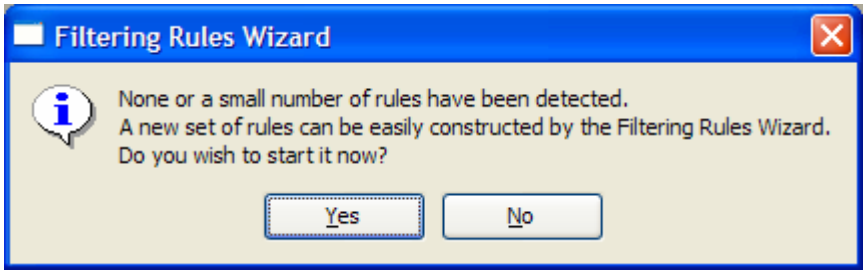
The Internet and Mail server entities, as well as the smtp service, must have been previously configured in the system. For more information on how to configure entities in the Firewall Aker, go to chapter Registering Entities.

When an entity name to be included in the rule contains blanks or spaces, it is mandatory that it comes between double quotes (" ").

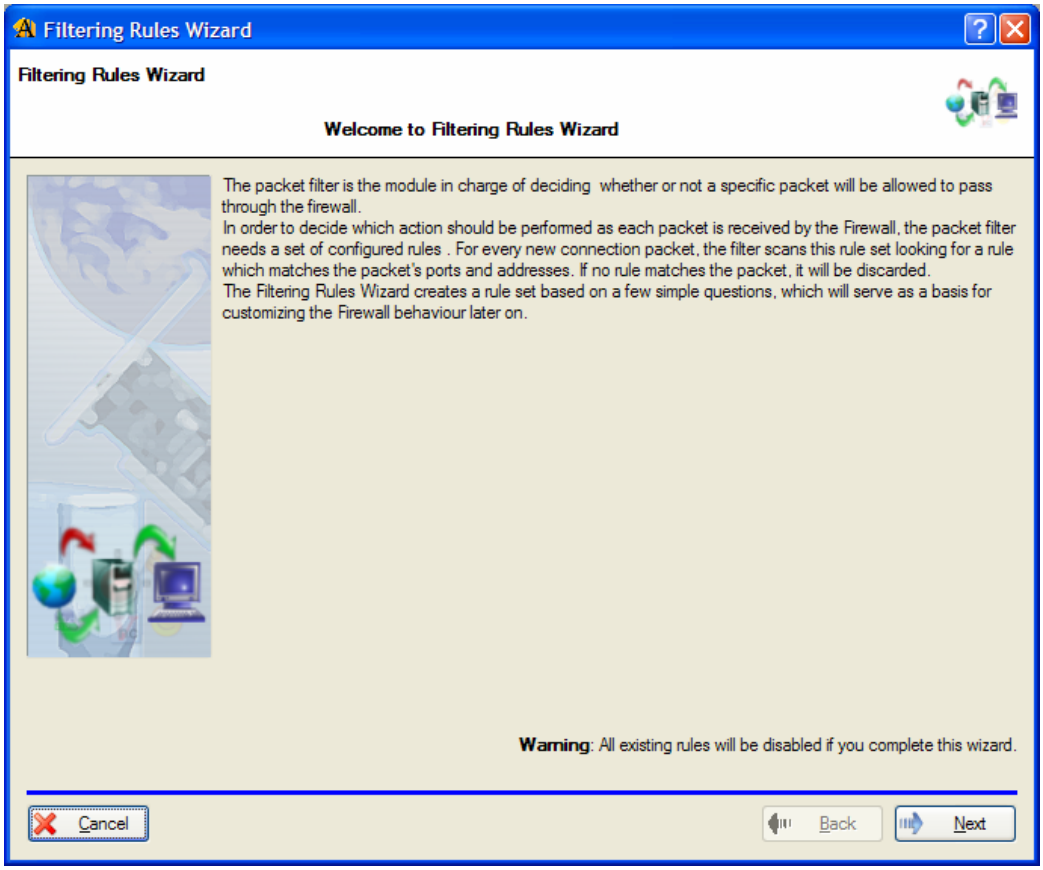
6-5 Using the Rules Wizard

The Rules Wizard can be turned on through the menu or the toolbar. If there are a small number of rules, the wizard will run automatically.

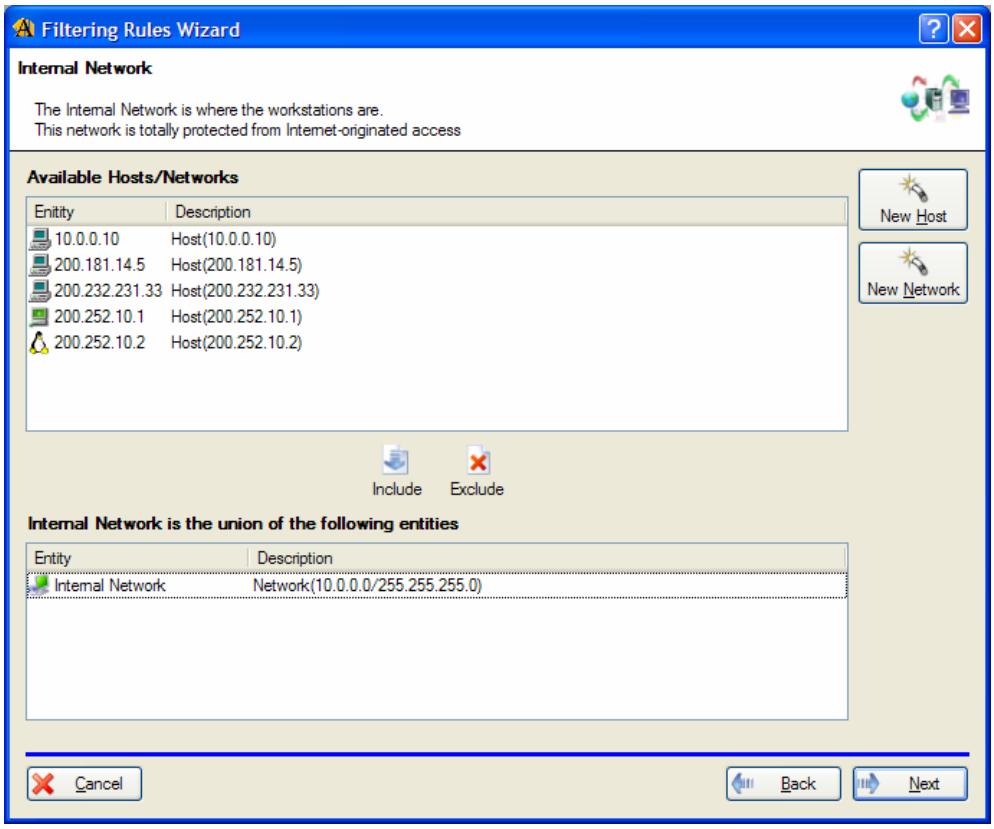
1 – Turning the Rules Wizard on. The window below will be displayed when a very small number of rules are detected.



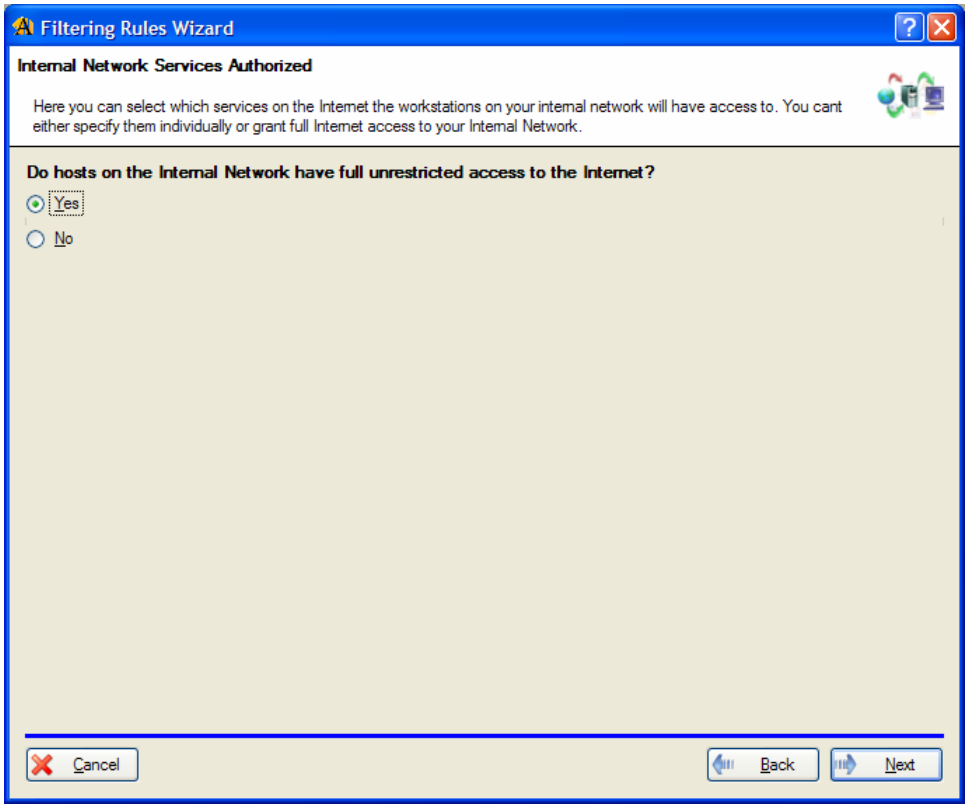
2 – Initial explanatory screen.



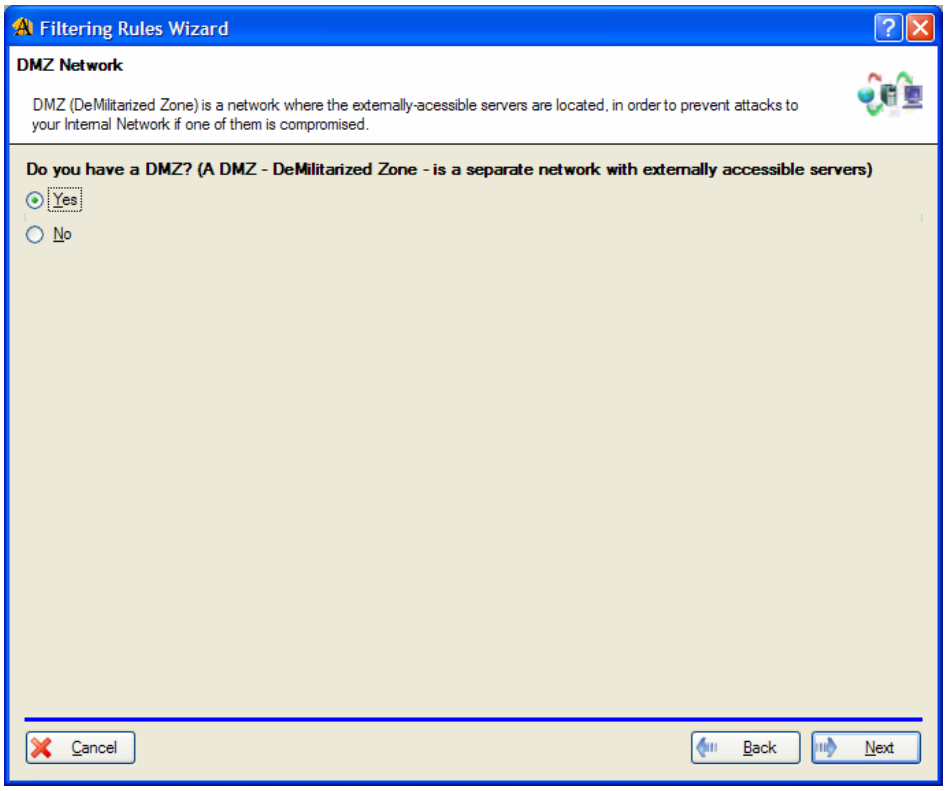
3 – Selection of the internal network.



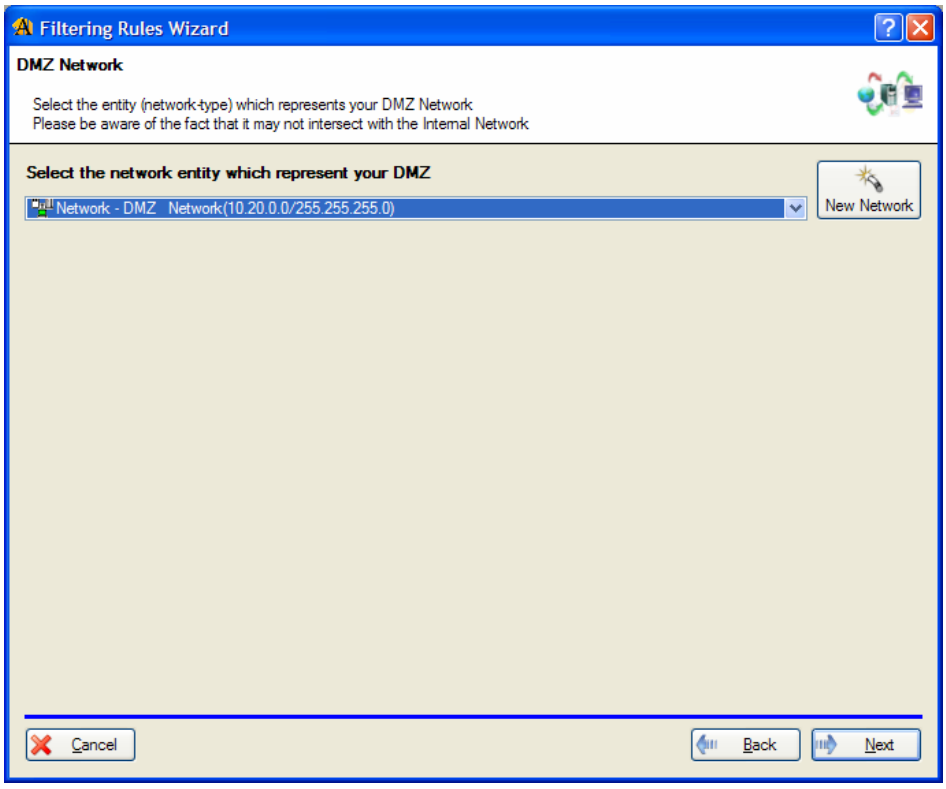
4 – Information needed to determine if hosts would have unrestricted access to the Internet.



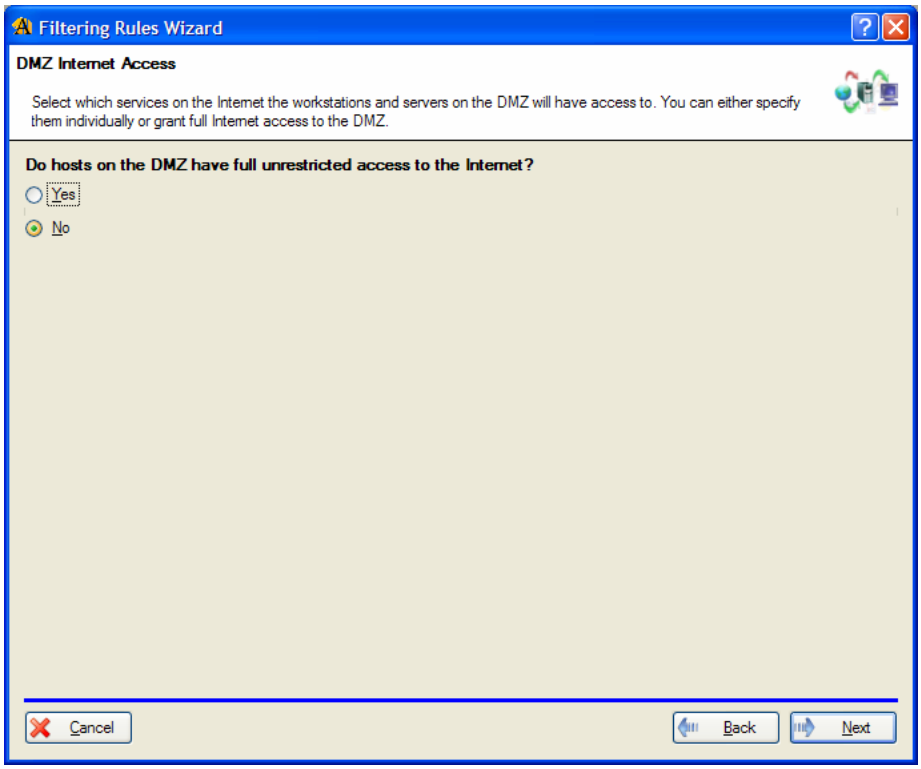
5 – DMZ configuration.



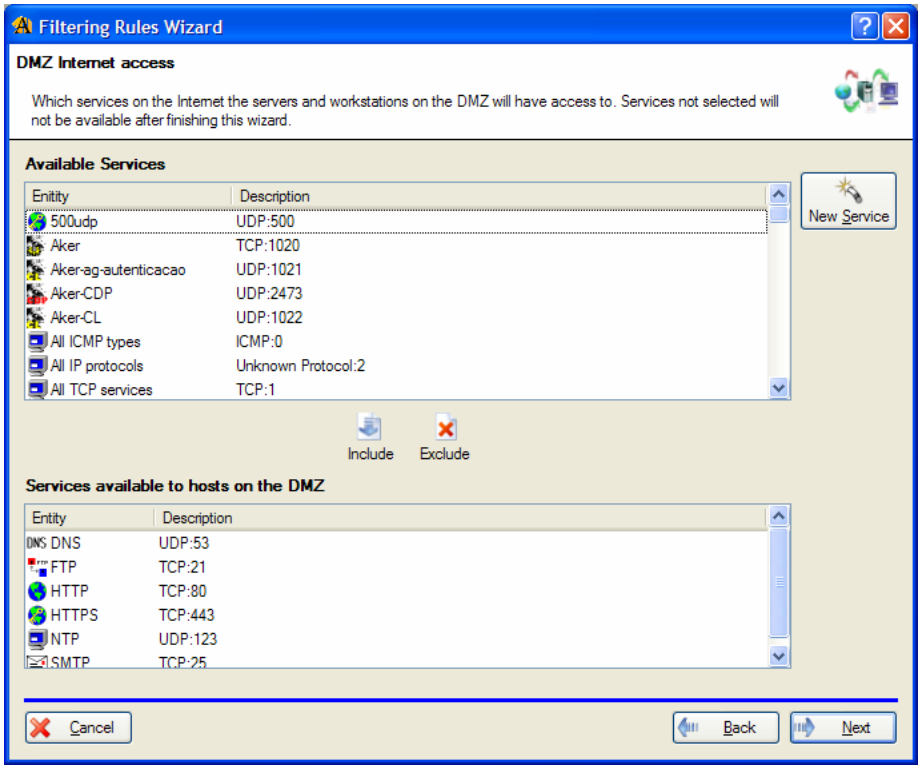
6 – Selection of DMZ entity.



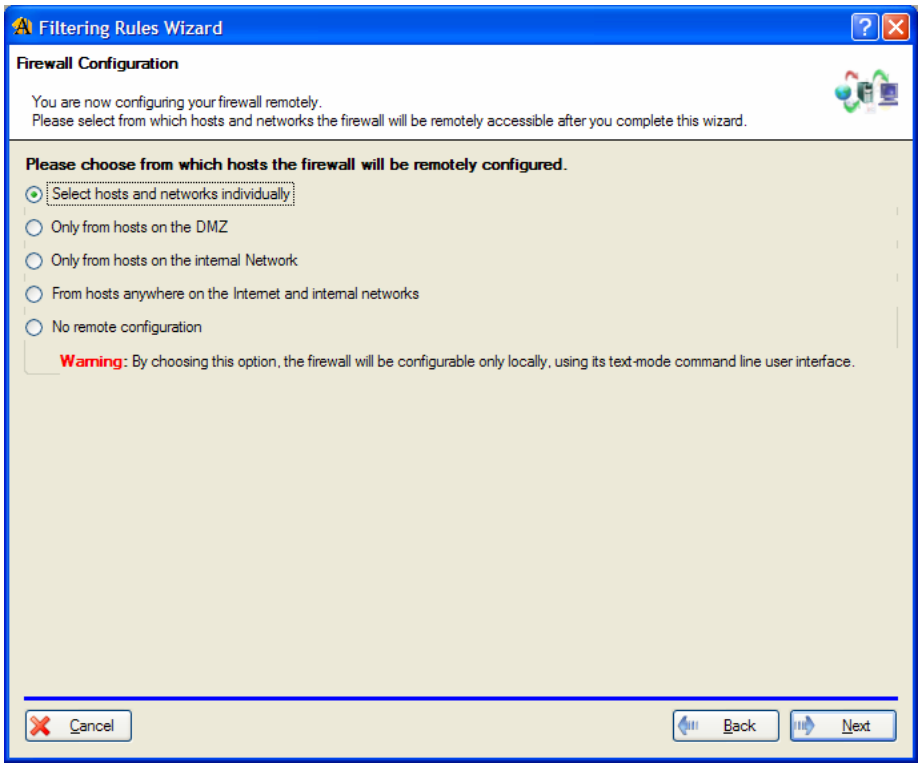
7 – Information about DMZ's access to the Internet.



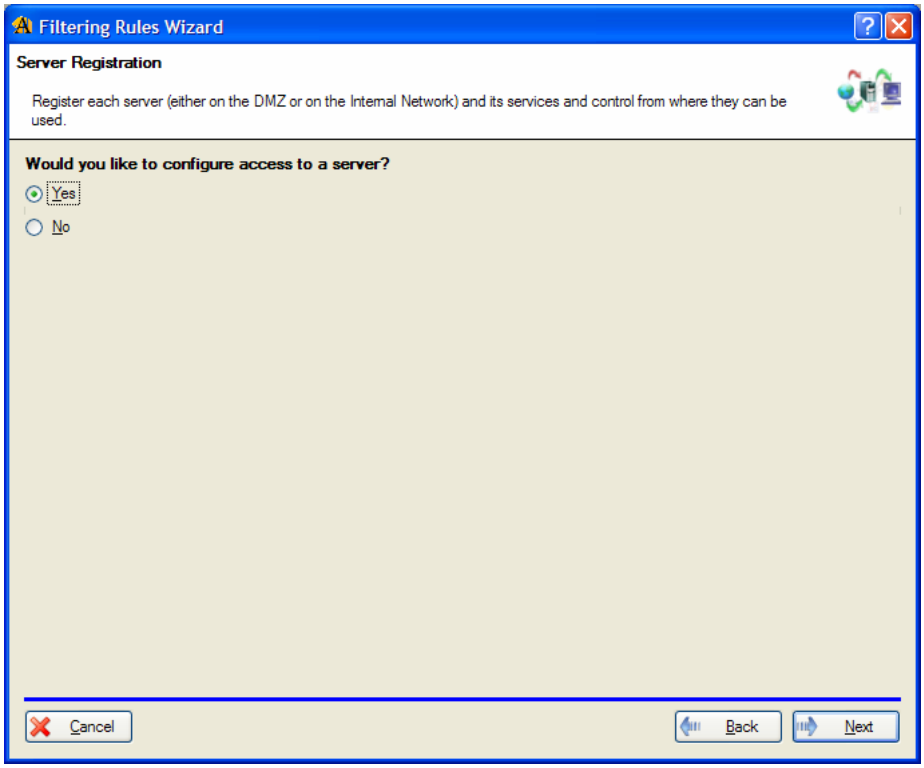
8 – Services available to DMZ.



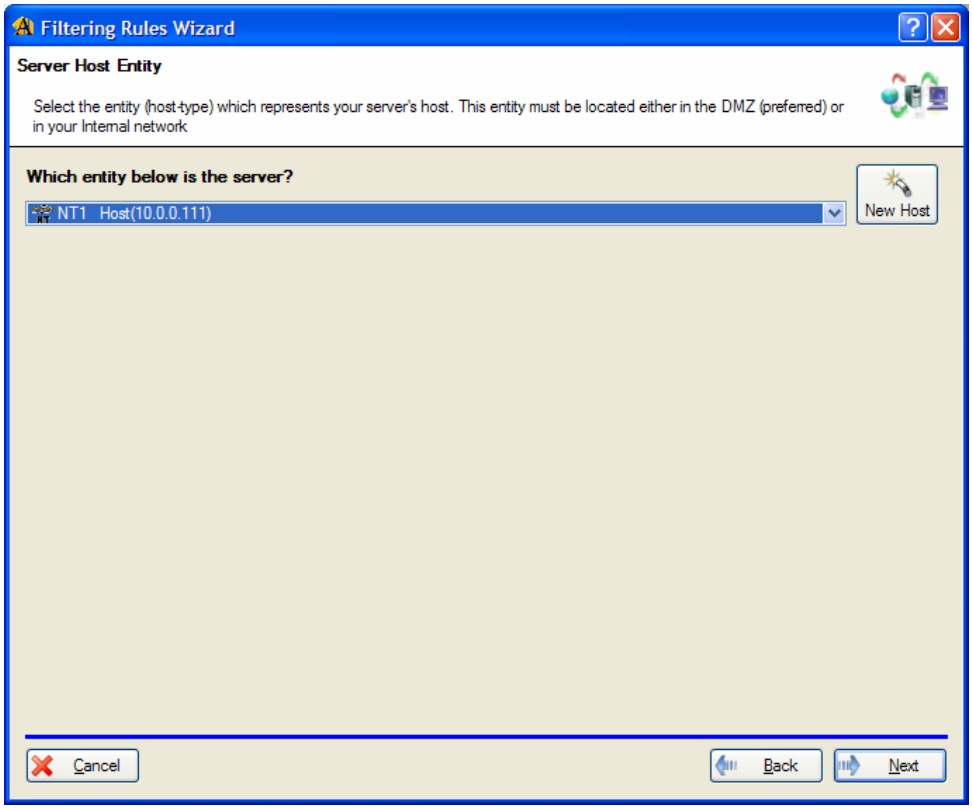
9 – Firewall administration. Notify who will have administration access to it.



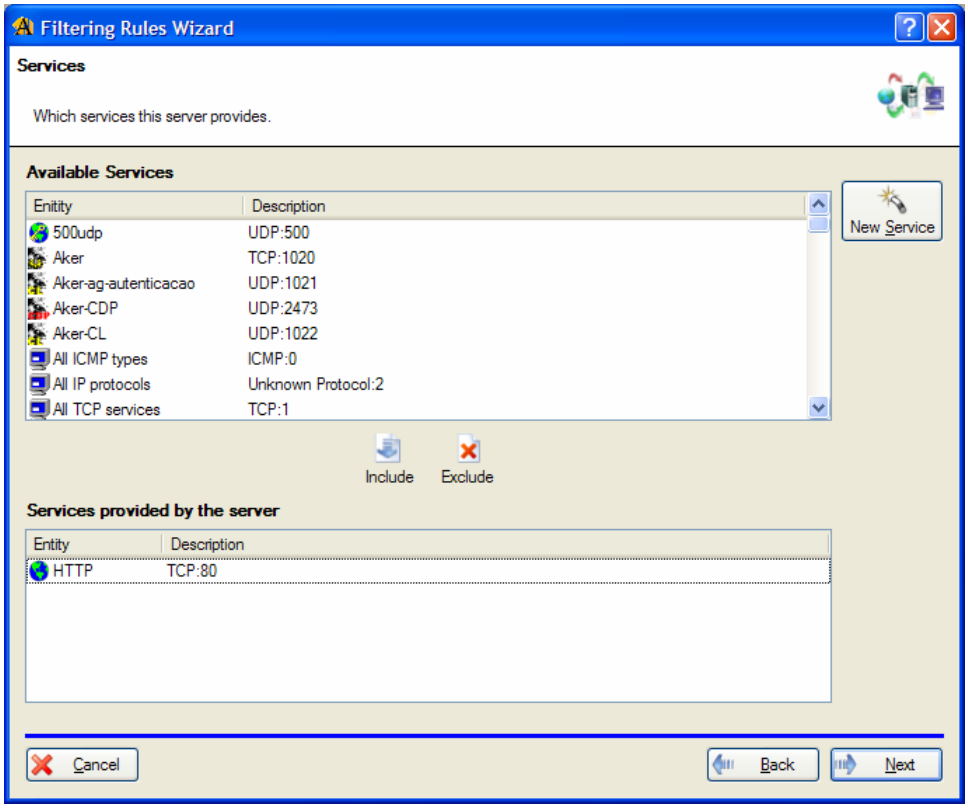
10 – Individual DMZ server registration.



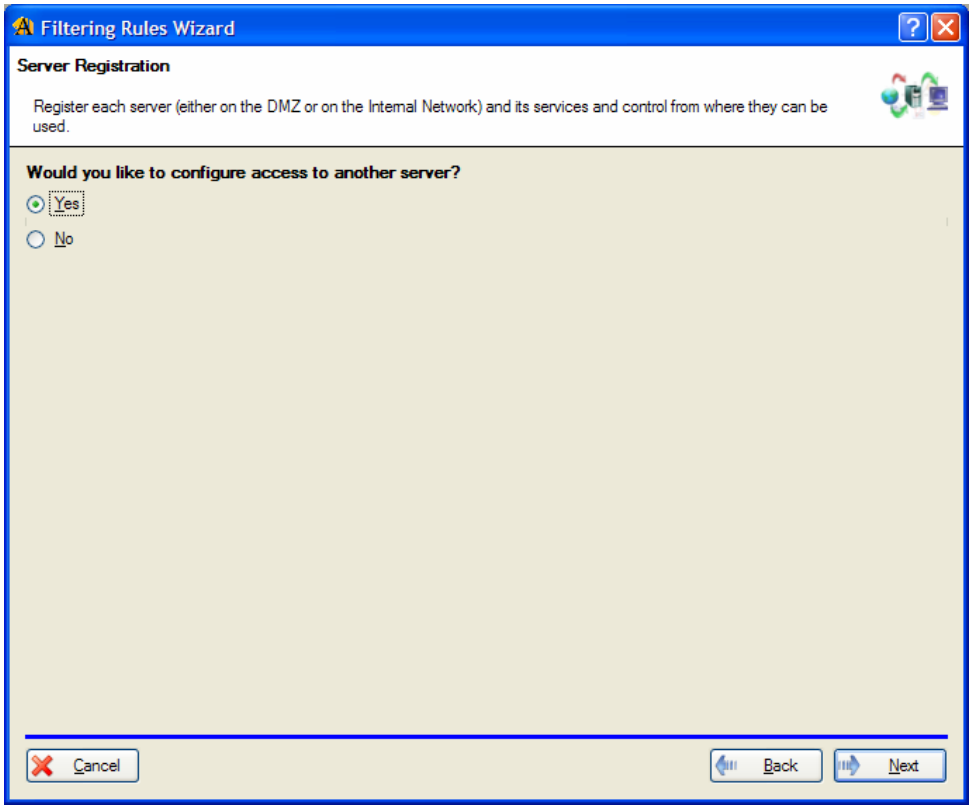
11 – Notification of specific server to DMZ.



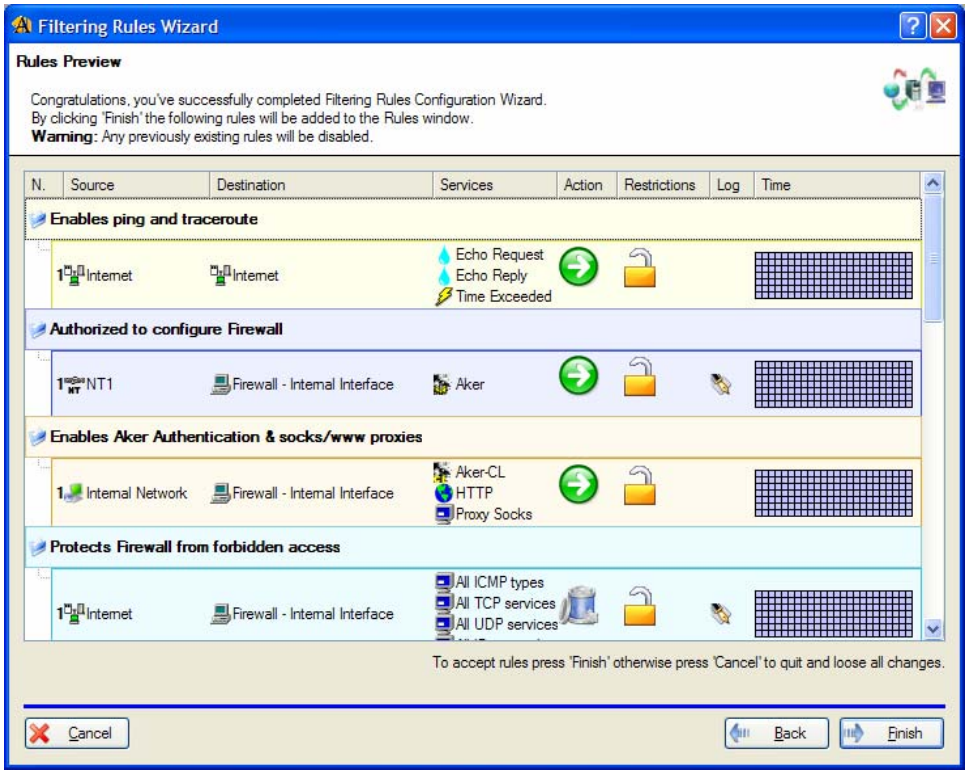
12 – Selection of server services for the DMZ.



13 – Checking whether another server configuration is desired.



14 – Preview of filtering rules configured by the wizard.



7-0 Configuring the Network Address Translation (NAT)

We will show here how to configure the network address translation (NAT) to enable internal network use of reserved addresses, increasing its address space, hiding internal network hosts, and still accessing the Internet, in a totally transparent manner. With this new version, it is also possible to make connection load balancing in a more intelligent way.

7-1 Planning the Installation

What is Network Address Translation?

Every network that connects to the Internet needs a set of IP addresses issued by an appropriate authority. Basically, there are three possible sets of addresses: the so called class A, with 16,777,214 hosts inside the network, the class B, with 65,533 hosts and class C, with 254 hosts on the network.

Due to the fast expansion of the Internet in the recent years, there are no class A or B addresses available anymore. Therefore, any connecting network will receive a class C address, which allows the addressing of only 254 hosts. If the number of machines is greater than that, either several class C addresses are required, which makes the administration more difficult, or Network Address Translation (NAT) is required.

NAT is a technology that allows the addresses of internal network hosts to be distributed as desired, making viable the use of reserved class A addresses, and still have all hosts simultaneously and transparently accessing the Internet.

Its operation is simple: every time an internal host with a reserved address tries to access the Internet, the Firewall detects it and automatically translates its address into a valid one. When the destination host responds and sends data to the valid address, the Firewall translates this address back into the reserved one and redirects the data to the internal host. This process is transparent, so that neither the client hosts, nor the server, know it is being done.

Another advantage in addition to the one above is that, with NAT, all hosts of your internal network become invisible to the external network, further increasing the level of security of the installation.

NAT is not compatible with services that send IP addresses or port numbers as part of the protocol. The only services of these types supported by Firewall Aker are FTP, Real Audio and Real Video.

What are my internal networks?

Internal networks are made of all hosts of one or more subnets protected by Firewall Aker. It includes all network internal devices, such as routers, switches, servers, clients, etc. These are either equipment that store important network information, or key components of its operation.

What are my external networks?

External networks are made of all hosts that are not part of the internal network. They may or may not be under the administrative responsibility of your organization.

When a company network is connected to the Internet, the external network is actually the entire Internet.

Addressing my internal networks

Despite of being technically possible, your internal network addresses should not be chosen randomly. There are a few addresses especially reserved for this purpose. These addresses are not and will never be assigned to any machine connected to the Internet.

The reserved addresses are:

From **10.0.0.0** to **10.255.255.255**, mask 255.0.0.0 (class A)
From **172.16.0.0** to **172.31.0.0**, mask 255.255.0.0 (class B)
From **192.168.0.0** to **192.168.255.255**, mask 255.255.255.0 (class C).

Types of NAT

There are three different types of Network Address Translation: 1-1, N-1, and 1-N. Each has its own characteristics. They are usually combined to ensure better results.

- 1-1

The 1-1 type is the most intuitive, however it is usually the least useful. It involves the binary 1-1 mapping between reserved and valid addresses. Thus, different hosts would have different translated addresses.
This operation is limited because it is not possible to use more hosts than the number of valid addresses, once they are always translated on a one to one basis. It allows, however, that hosts with reserved addresses be externally accessed with valid addresses.

- N-1

N-1 translation, as the name implies, allows several machines with reserved addresses to use the same valid address. To do it, it uses IP addresses combined with ports (TCP and UDP), or with sequential numbers (ICMP). The firewall dynamically performs this mapping, every time a new connection is established. Because there are 65,535 different ports or sequential numbers, it is possible to have up to 65,535 simultaneous active connections using the same address.

The only limitation of this technology is that it does not allow internal hosts to be accessed externally. All connections must be initiated internally.

- 1-N

This type of translation is also called load balancing and allows the placement of several servers behind a single valid IP address. Each time a new connection is established for this address, it is redirected to one of the internal servers. The main advantage of this technology is to enable services that demand great amount of resources to be separated into several machines, and still be accessed in a transparent way, through a single address. In case any of these hosts fails, new connections are automatically redirected to those still working, establishing a fault tolerant mechanism.

Usage Scenarios of Firewall Aker NAT

Aker Firewall allows any type of translation. It is not limited to the valid firewall external interface address, also providing flexibility for the administrator to use any address inside the network, even performing the translation between networks with reserved addresses.

Let's suppose that a given organization receives a class C address, with the format A.B.C.0. This is a valid address that supports up to 254 hosts (addresses A.B.C.0 and A.B.C.255 are reserved for specific use and may not be used, leaving available values between A.B.C.1 and A.B.C.254). Let's suppose again, that this network has 1000 hosts to be connected. Since it's not possible to allocate all machines with the received address range, NAT must be used. A class A reserved address was chosen to be used in the internal network hosts: 10.x.x.x with subnet mask 255.0.0.0.

Aker Firewall will be installed on the boundary between the Internet and the internal network with reserved addresses. The Firewall will be responsible for the translation of the reserved 10.x.x.x addresses into the valid A.B.C.x addresses. Therefore, the Firewall must have at least two addresses: a valid one that can be reached from the Internet, and another, reserved address, to be reached from the internal network. (Most installations use two or more network adapters in the firewall: one for the external network, and one or more for the internal network. It is possible, however, although not recommended, to have the same configuration with only one network adapters, assigning both a valid and a reserved address to the same card.)

Let's assume that address A.B.C.2 is chosen for the valid segment, and 10.0.0.2 for the reserved segment. This valid address will be used by the firewall to translate all connections that originate in the internal network and target the Internet. Externally, all connections will be seen as if they were originated in the firewall.

Another example could be an organization with Internet connections and three classes of valid addresses. In this case, the administrator can distribute the address translation among these three classes, obtaining much more configuration flexibility.

With NAT, all internal hosts can transparently access any Internet resource, as if they had their own valid addresses. On the other hand, no external host can initiate a connection to an internal machine because they don't have valid addresses. As a

solution, Firewall Aker allows the configuration of 1-1 translation rules, which enables valid address simulation to any reserved address.

Going back to our example, let's suppose there is a WWW server in your network, with address 10.1.1.5. It is desired that this server send information to the internal network, as well as to the Internet. In this case, a valid address is necessary, so that external clients can use it to connect to this server. If the chosen address were A.B.C.10, a 1-1 translation rule should be added, in order to map the A.B.C.10 address to the 10.1.1.5 internal address. From this moment on, all connections to A.B.C.10 would be automatically remapped by the firewall to 10.1.15.

The valid addresses chosen to perform the 1-1 translation cannot be assigned to any real host. In our example, it is possible to configure up to 253 servers in the internal network, which can be accessed externally (one of the 254 valid addresses is already used by the firewall to translate all client hosts traffic).

Aker Firewall uses proxy-arp technology to enable *virtual servers* to be treated as real machines, by the hosts that belong to the valid network (the external router, for example).

Examples of configurations using NAT

- **Connecting to the Internet with a leased line**

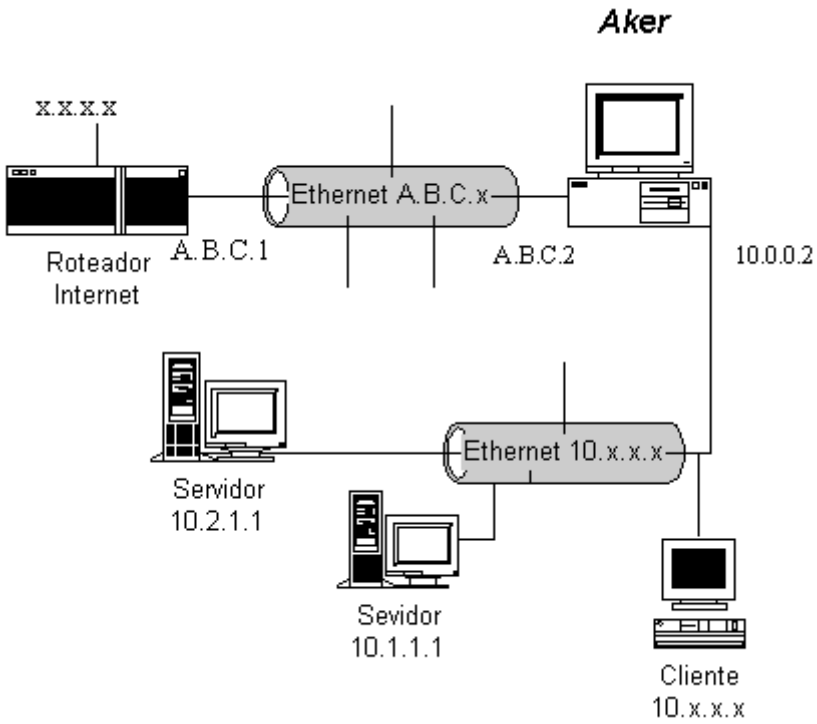
Equipment: 1 router, 1 *Aker Firewall*, n clients, 2 servers on the internal network
Valid address: A.B.C.x, netmask 255.255.255.0
Reserved address: 10.x.x.x; netmask 255.0.0.0
Server addresses: 10.1.1.1, 10.2.1.1
Client addresses: 10.x.x.x
Router addresses: Valid network: A.B.C.1 , Internet:x.x.x.x

Aker Firewall Configuration:

Adapter addresses: internal network: 10.0.0.2, valid network A.B.C.2
Virtual IP: A.B.C.2
Private network: 10.0.0.0
Private netmask: 255.0.0.0

1-1 translation rules:

A.B.C.10 - 10.1.1.1
A.B.C.30 - 10.2.1.1



Drawing: Example 1

- **Interconnection of departments**

This example will show how to interconnect departments of a same company, using an address translator between these departments.

Equipment: 1 router, 3 *Aker Firewalls*, n clients, 4 internal network clients
Valid address: A.B.C.x, netmask 255.255.255.0
Reserved address: 10.x.x.x netmask 255.255.0.0
Reserved address:172.16.x.x, netmask 255.255.0.0

Subnet 1 addresses:

10.1.x.x
Server address: 10.1.1.1
Client addresses: 10.1.x.x
Router addresses: Valid network A.B.C.1 , Internet:x.x.x.x

Aker Firewall Configuration:

Internal network: 10.1.0.1, Valid network A.B.C.2
Virtual IP: A.B.C.2
Private network: 10.0.0.0
Private netmask: 255.0.0.0

Subnet 2 Addresses:

Externally: 10.1.0.2
Internally: 172.16.x.x

Server address: 172.16.1.1
Client addresses: 172.16.x.x

Aker Firewall Configuration:

Subnet 2: 172.16.0.1, Subnet 1:10.1.0.2
Virtual IP: 10.1.0.2
Private network (2): 172.16.0.0
Private netmask: 255.255.0.0

1-1 translation rules:

10.2.1.1 - 172.16.1.1

Subnet Addresses 3:

Externally: 10.1.0.3
Internally: 172.16.x.x

Server address: 172.16.1.1
Client addresses: 172.16.x.x

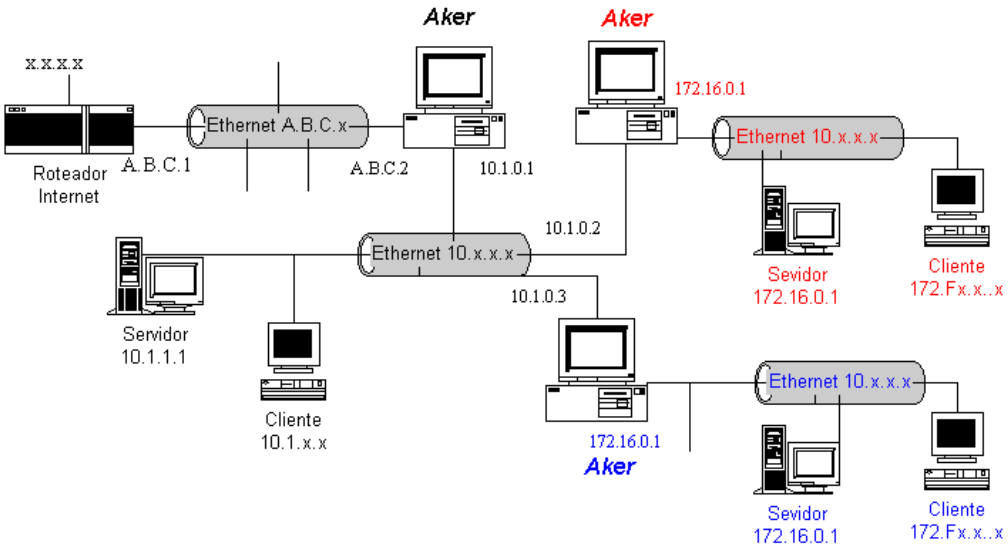
Aker Firewall Configuration:

Subnet 3: 172.16.0.1, Subnet 1:10.1.0.3
Virtual IP: 10.1.0.3
Private network (3): 172.16.0.0
Private netmask: 255.255.0.0

1-1 translation rules:

10.3.1.1 - 172.16.1.1

 For this kind of installation, routes to the subnets 10.1.x.x, 10.2.x.x, and 10.3.x.x should be inserted into the routing table.



Drawing: Example 2

- **Multiple connections with the Internet**

In this example, far more complex, it will be shown how to use three connections with the Internet and two with internal networks, using the network address translator among them.

Equipment: 3 routers, 1 *Aker Firewall*, n clients, 2 servers in the DMZ network
Valid addresses: A.B.C.x, D.E.F.x, G.H.I.x, all with netmasks 255.255.255.0
Reserved address used in the internal network: 10.x.x.x netmask 255.255.0.0
Reserved address used in the DMZ: 172.16.x.x, netmask 255.255.0.0
Router addresses: Valid network A.B.C.1, D.E.F.1, G.H.I.1, Internet: x.x.x.x.

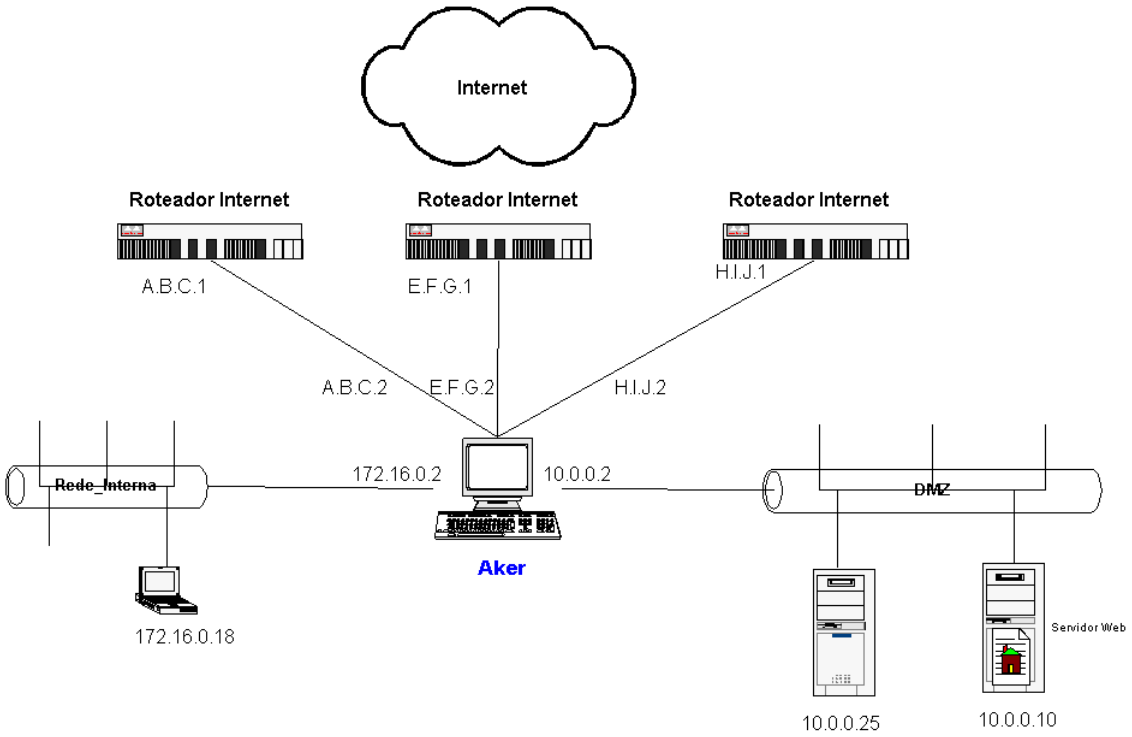
Aker Firewall configuration:

Network addresses: Adapter 1: 10.0.0.2, Adapter 2: 172.16.0.2, Adapter 3: A.B.C.2, Adapter 4: D.E.F.2, Adapter 5: G.H.I.2
Private networks: 10.0.0.0 and 172.16.0.0
Private network masks: 255.255.0.0

DMZ Servers:
Web Server: 10.0.0.10
SMTP Server: 10.0.0.25

Network address translation rules:

1. Source - 10.0.0.10 translate to A.B.C.10 when accessing the Internet
2. Source - 10.0.0.25 translate to D.E.F.25 when accessing the Internet
3. Source - 172.16.x.x translate to 10.0.0.4 when accessing network 10.0.0.0
4. Source - 172.16.x.x translate to D.E.F.25 when accessing the Internet
5. Source - 10.x.x.x translate to A.B.C.20 when accessing the Internet



Drawing: Example 3

Creating address translation rules for the Firewall Aker

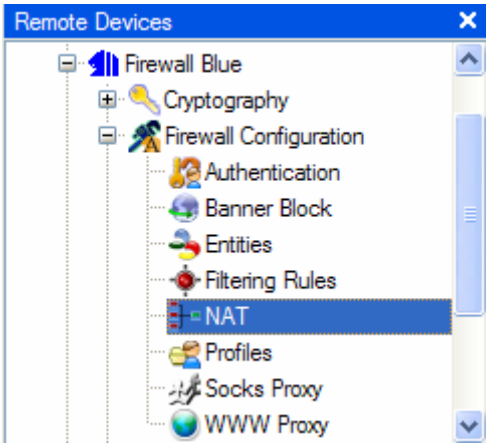
It is simple to create address translation rules in the Firewall Aker because of its intelligent design. IP addresses, masks, protocols, and ports are configured through entities (for further information, refer to chapter Registering Entities. Therefore, when configuring a rule, there is no need to worry about which port a specific service uses, or about the IP address of a determined network or host. All these things have been previously configured. Furthermore, to make it even easier, the most frequently used Internet services are pre-configured, which means no wasting time researching their data.

Basically, to configure a translation rule, you must specify source and destination entities, type of translation, virtual interface, and service (if applicable).

Translation operation is simple: the firewall searches each single rule defined by the administrator, in the specified order, until the packet matches one of them. Then, it executes the translation type associated to the rule. If the search reaches the end of the list and the packet does not match any rule, then it will not be translated.

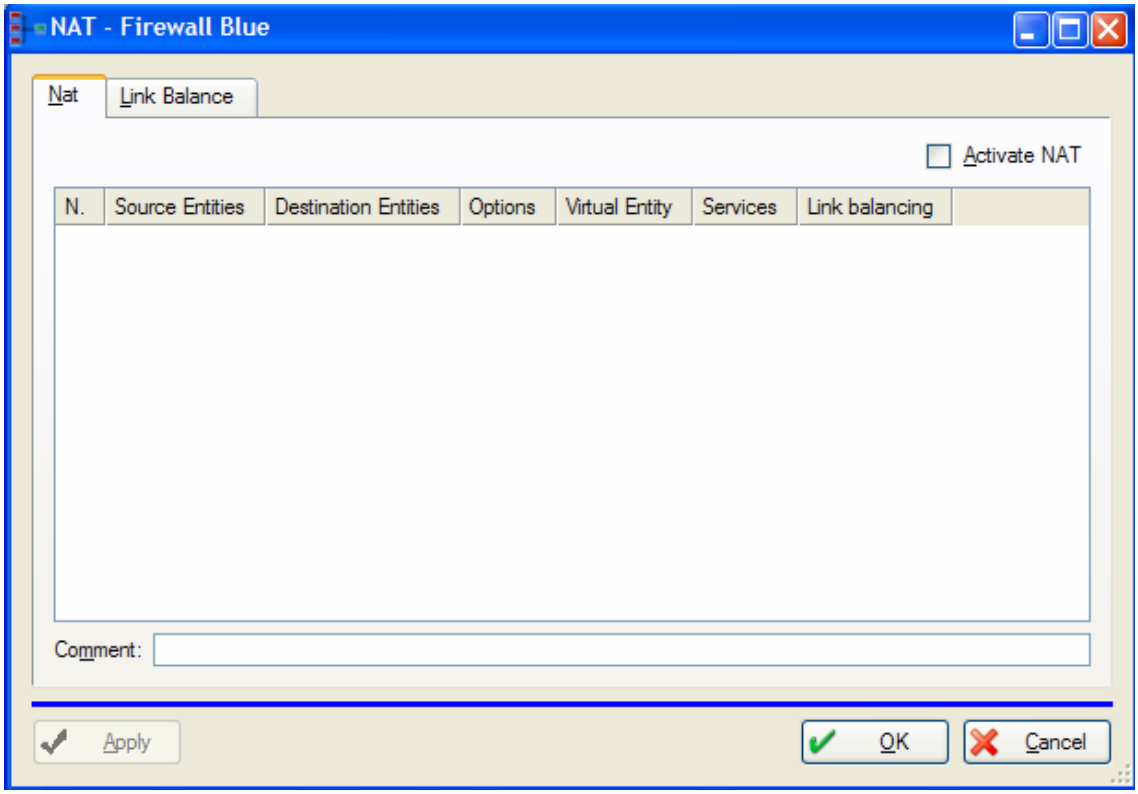
7-2 Using the Graphic user interface

To have access to the NAT configuration window, do the following:



- Click on the *Firewall Configuration* menu
- Select *NAT*

The NAT Configuration Window



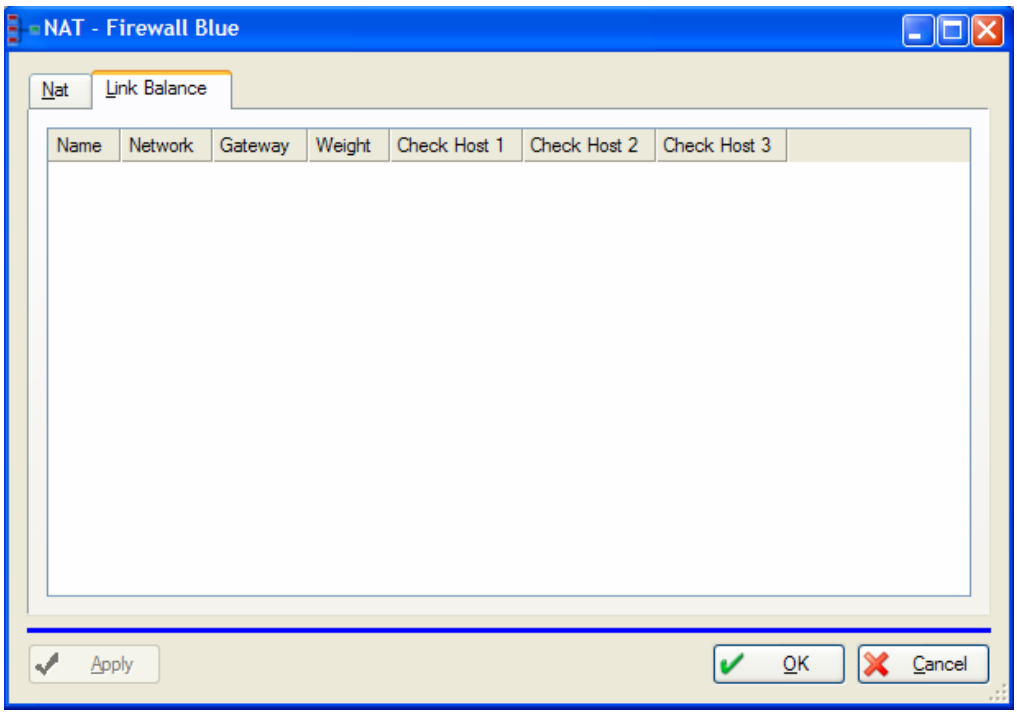
The NAT window has all the translation rules defined in the Firewall Aker. Each rule is displayed on a separate row, made of several cells. Selected rules are shown on a different color.

- The **OK** button updates the set of rules and immediately enables them.
- The **Apply** button sends all modifications to the firewall and keeps the window open.
- The **Cancel** button discards all modifications and closes the window.
- There is a comment bar to add comments about the translation rule.

- The **Activate NAT** option, if checked, makes the firewall translate the addresses according to the configured rules. If this option is not checked, no network address translation will be done.

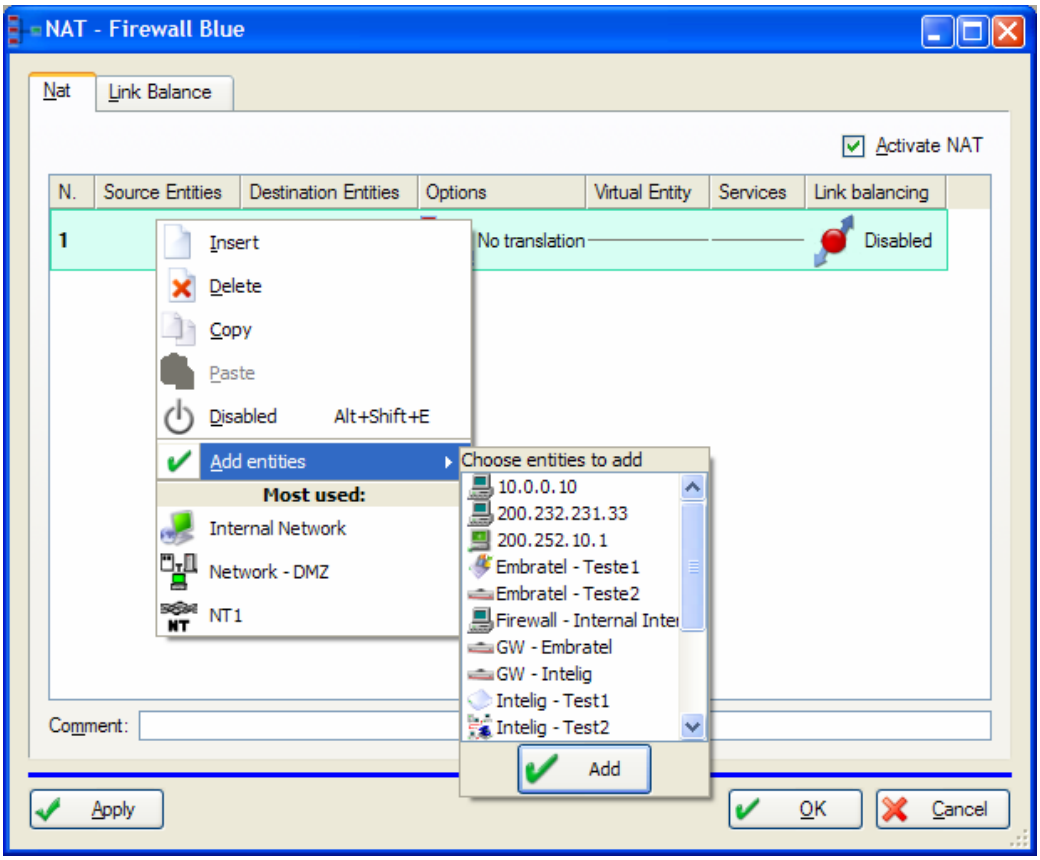
- The scrollbar on the right side of the window is used to view the rules that do not fit the window.
- If a selected rule has a comment associated to it, it will be displayed on the bottom part of the window.
- A rule position may be modified by clicking and dragging it to the desired position.

Link Balance Configuration Window



- The **OK** button updates the set of rules and immediately enables them.
- The **Apply** button sends all modifications to the firewall and keeps the window open.
- The **Cancel** button discards all modifications and closes the window.

To execute any operation on a specific rule, just right click on it. The following menu will show up: (This menu comes up every time the right mouse button is pressed, even if no rule is selected. In this case, only the *Insert* and *Paste* options will be active.)



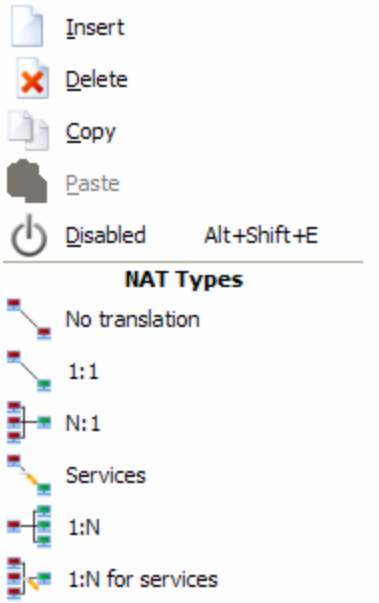
- **Insert:** This option adds a new rule to the list. If any rule is selected, the new one will be inserted in its position, pushing it down the list. Otherwise, the new rule will be appended to the end of the list.
- **Delete:**Removes the selected rule from the list.
- **Copy:** Copies the selected rule into a temporary area.
- **Paste:** Copies the rule from the temporary area into the list. If any rule is selected, the new one will be copied in its position, pushing it down the list. Otherwise, it will be copied at the end of the list.
- **Enable/Disable:** Enables or disables the selected rule. If disabled, the rule will remain configured, but the Firewall will act as if it did not exist and will proceed searching the next rule.
- **Add entities:** In the very spot you click, it is possible to insert an entity in the corresponding field of the translation rule. Only a certain number of entities can be viewed at a time. To choose another entity, scroll down the window.

Hint: The easiest way to create a translation rule is to drag and drop the entities directly onto the rule.

Hint 2: Each rule position may be modified by drag and dropping it at the new location. Note that the cursor will change into a dotted line box . Note that a dotted line box appears below the cursor arrow.

If you are adding or editing rules, you will see the properties window described below:

The NAT Rules Insert Window



- **NAT Types**: In this field you define the type of translation a rule will perform. Options are:

- **No Translation:** This option tells the firewall that no address translation should occur when any of the *Source Entities* hosts accesses any of the *Destination Entities hosts*, and vice-versa.

- **1-1 Translation**: Indicates to the firewall that, when a host in the *Source Entities* list accesses any host listed in the *Destination Entities* list, it will have its address translated into the *Virtual Entity* address. Every time a *Destination Entities* host accesses the *Virtual Entity* address, the virtual address will be automatically translated into the real address, defined by the entity in the *Source Entities*. This type of translation is useful to enable external access to internal servers.

An entity with the real address (internal, reserved) of the machine for which the 1-1 translation will be done should be added to the *Source Entities*. And, defined as *Virtual Entity*, an entity with the address into which the internal address will be translated (valid address), and which will be accessed by external hosts.

- **N-1 Translation**: This option tells the firewall that when any *Source Entities* host accesses any *Destination Entities* host, it will have its address translated into the *Virtual Entity*. This type of translation is useful to enable a large number of hosts to use only one valid IP address to connect to the Internet. However, it does not allow external hosts (listed in the *Destination Entities*) to initiate any communication with internal hosts (listed in the *Source Entities*).

When the Cooperative Cluster module is operating in the N-1 translation type, the *Virtual Entity* IP cannot be any of the ones assigned to the firewall interfaces.

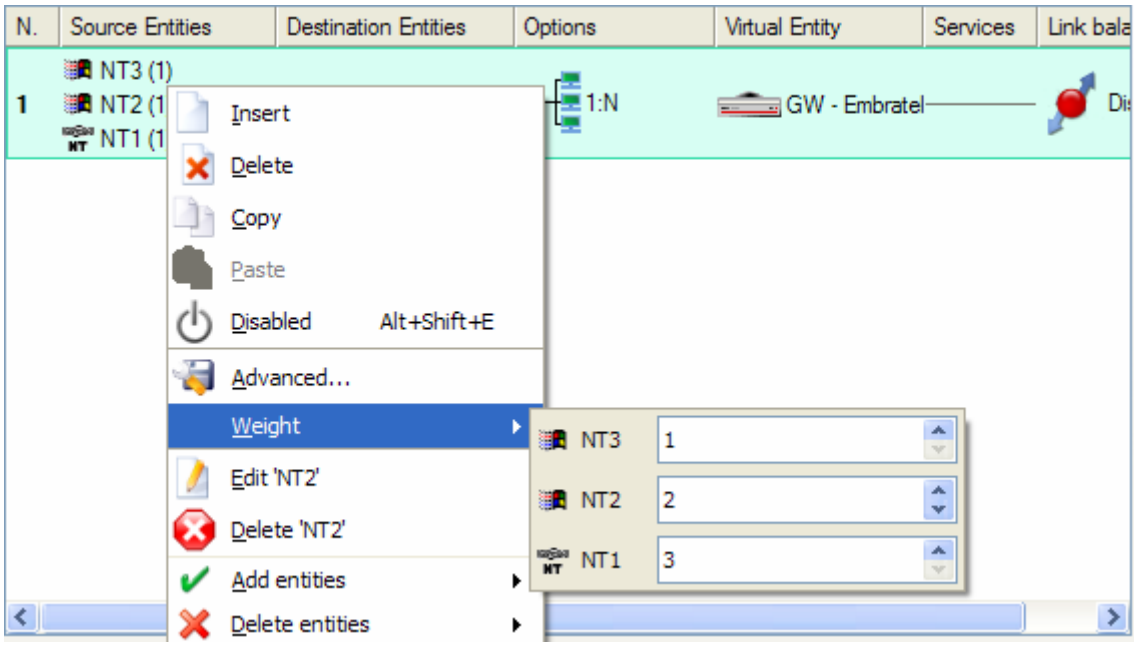
- **Services Translation**: This option is useful for networks that have only one IP address and need to enable Internet services. It allows that certain services, when accessed in the firewall, be redirected to the internal machines.

The internal IP address (real address) of the host to which the services will be redirected, must be listed in the *Source Entities* field. The hosts that will externally access the services must be listed in the field *Destination Entities*. Services that will be redirected to the *Source Entities* host, when a *Destination Entities* host accesses them in the *Virtual Entity* IP address, must be chosen in the *Services* field.

When the Cooperative Cluster module is operational, services translation is not possible.

- **1-N Translation**: This option is used for load balancing, i.e., to enable several hosts to respond as if they were only one.

In the *Source Entities* field you must add the list of hosts that will take part in the balancing, and that will start responding as if they were only one. In the *Destination Entities*, you must add the machines that will access the internal hosts through the address specified in the entity present in the V*irtual Entity* field.



- In this type of translation, hosts belonging to the *Source Entity* field may have different weights. So, if a host has weight 1, and another has weight 2, it means that at every three connections, one will be redirected to the first host and two to the second.

- **1-N Services Translation:** This option is used to perform load balancing for some services, that is, to enable that several hosts respond to these services requests as if they were one.

- In the *Source Entities* field, you must place the list of the hosts that will take part in the balancing, and that will start responding as one. In the *Destination Entities* field, you must place the hosts that will access the internal hosts through the address specified in the entity present in the *Virtual Entity* field. In the *Services* field, you must choose all services that will take part in the load balancing.

  In this type of conversion, the machines belonging to *the Source Entity* field may have different weights. So that, if a host has weight 1, and another has weight 2, it means that at every three connections, one will be redirected to the first host, and two to the second.

  When the Cooperative Cluster is on, it is not possible to perform services translation.

  Virtual Entity: In this field, you must configure the entity into which the internal addresses will be translated, or to which external requests must be redirected. The virtual entity must always be a host-type entity.

  Source Entities: This field is used to specify the list of all entities which addresses will be translated into the *Virtual Entity* address described above. The 1-1 Translation, or Services Translation, allows the selection of only one entity to this field. It must be a host-type entity.

  In case 1-N Translation, or 1-N Services Translation, is being used, each host belonging to this field will have a weight associated to it, between parentheses, to the right of the entity name. To modify a host weight, i.e., to change the number of connections that host will activate, relative to other servers, just right-click over the entity name, on the list to the right, select the **Modify weight** option, and choose the new value.

  The *Source Entities* field must always contain the internal addresses (reserved or invalid) of the machines participating in the translation, regardless of their type.

  Destination Entities: This field is used to specify the entities to which the address translation will be performed (in case of N-1 translation), or the hosts that will access the internal hosts through the address in the *Virtual Entity* field (for remaining translation types). By creating several rules with different values in this field, the same machine will have its address translated into different addresses, depending on the destination of the communication.

  The Internet is the most used value for this field. This causes the address translation selected in the rule to be performed for all external hosts.

  Services: This field defines the services that will be part of the rule, when Services Translation type or 1-N Services Translation is selected. The window will be disabled to the remaining translation types.

Comment: It is used to write a description about a rule. It is very useful for documentation and maintenance of rules information.

The **Advanced** button, which will only be enabled when the 1-N address translation or 1-N services translation is selected, allows configuration of monitoring parameters. This monitoring will be performed by the firewall to find out if the hosts participating in the load balancing are up or not, and how the balancing will be performed. When this button is selected, the following window shows up:

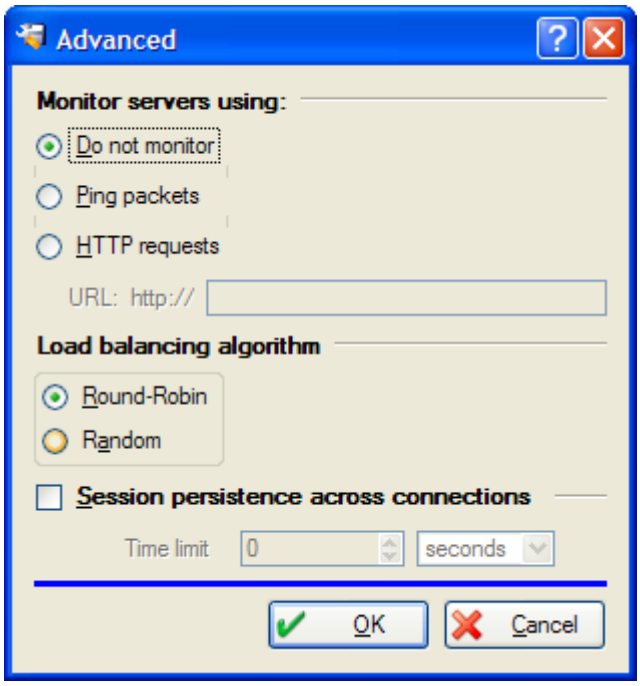
The field **Monitor servers using** defines the method used by the firewall to verify if hosts participating in the balancing (hosts defined in the *Source Entities* field) are up. It has the following options:

No monitoring: if this option is selected, the firewall will not monitor the hosts and will assume they are always up.

Ping packets: With this option selected, the firewall will monitor the hosts through ICMP packets of *Echo Request* and *Echo Reply* (also used by the PING command; hence the name).

HTTP requests: If this option is selected, the firewall will monitor hosts through HTTP requests. In this case, it is necessary to specify the URL (without the http:// prefix) that the firewall will access in each host to verify whether it's up or down.

Load balancing algorithm: This field is used to define the method used to balance requests between *Source*



Entities hosts. Its options are:

Round-Robin: If this option is on, the firewall will sequentially distribute the requests to the balancing hosts, one by one. In case the hosts have different weights, first a connection will be distributed to each host, then a connection to each machine that received a number of connections smaller than its weight, and so on. When all hosts have received a number of connections equivalent to their weight, the algorithm executes.

Random: With this option selected, the firewall randomly distributes the connections among the hosts, i.e., the probability of a connection be redirected to a specific host is equal to the ratio between its weight and the total weight of all hosts.

Session persistence across connections: It's the maximum waiting time for a new connection, after the previous one is over, for protocols or applications that use more than one connection at different times.

Observations about rules creation

It is highly recommended that translation rules be created in the following order:

1. No Translation Rules
2. Services Translation Rules
3. 1-1 Translation Rules
4. 1-N Services Translation Rules
5. 1-N Translation Rules
6. N-1 Translation Rules

To manage the firewall from an internal host that will participate in any type of translation, it is necessary to add a No Translation rule with source and destination within the same internal networks. This rule must be placed before all other translation rules.

Examples - Case 1 – Network Address Translation

Let's suppose a company has the hosts and services described below, and wants to implement NAT. The company has a dedicated Internet connection, and its provider distributed Internet valid IP addresses from 200.120.210.0 to 200.120.210.63.

In rule #1, we select the No Translation option for the company's internal networks (DMZ and Internal). This rule is important, because if any internal network host must manage the firewall, it will not have its address translated, which enables administration. It would also be correct to select No Translation option for administrator hosts (Source Entity), as well as for the interface through which the firewall will be managed (Destination Entity).

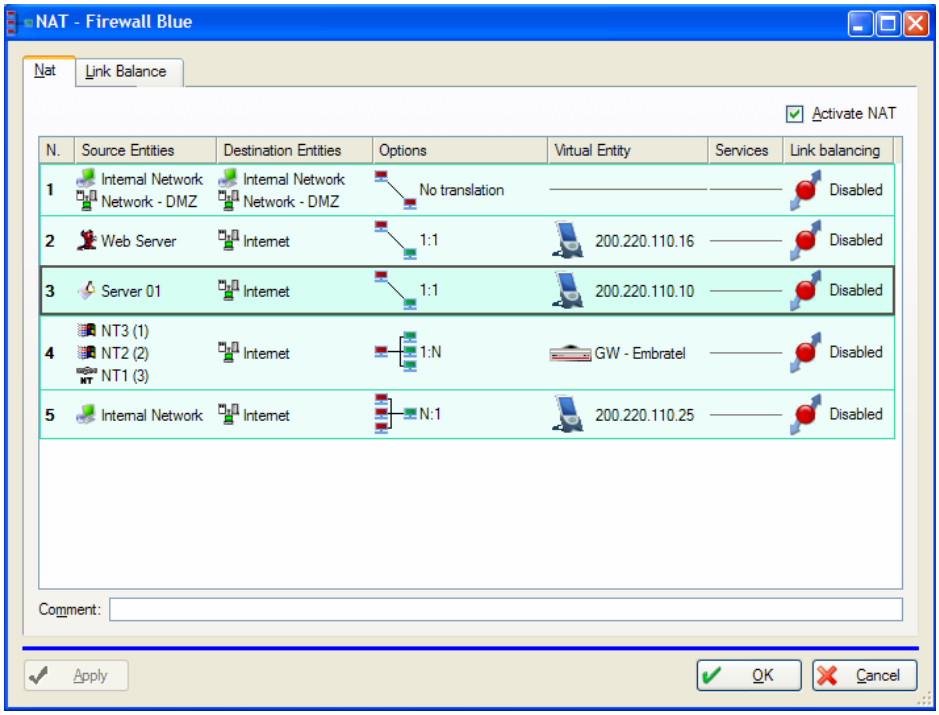
In rule #2, the server **server1** will make a 1-1 translation to the address 200.120.210.15, which means that anyone on the Internet looking for IP 200.120.210.15 will be directed to server1 (IP 10.20.0.50). The same way, if server1 originates a connection to the Internet, its IP will be 200.120.210.15.

Rule #3, by analogy, is identical to rule #2; the server server_web_aker will make a 1-1 translation to the 200.120.210.25 address.

Rule #4 exemplifies load balancing. Someone on the Internet looking for host 200.120.210.20 will be directed to NT3, NT2 or NT1, depending on the calculation made by the firewall. In the following case, the weights are different, therefore, host NT3, which has weight 4, will receive more connections. If the NT hosts have to originate Internet connections, they will have their addresses translated into 200.120.210.20 as well.

Rule #5 is of the N-1 translation type. Any Internal_Network host (10.20.0.0 with mask 255.255.255.0) will have its address translated into 200.120.210.16, when originating Internet connection. The opposite, however, does not happen. If someone from the Internet is attempting connection with IP 200.120.210.16, the firewall will not direct it to any host in the internal network. Instead, it will discard packets to this connection, for not knowing to which host the request should be sent.

It is imperative to emphasize that the order of the rules in the list is of extreme importance. Let's suppose that **rule #2** is moved to the **last position**. In this case, someone looking for host **200.120.210.15** would be directed to **server1**. However, when originating an Internet connection, **server1** would have its address translated into **200.120.210.16**, because the rule that was before in position 5 would perform the translation first.



Examples – Case 2 – Services Translation

Now, let's suppose that the company does not have a range of valid Internet IP addresses, but only **one single** valid IP. In this case, it is convenient to perform translation of services. With this type of configuration, this single IP (in this case, 200.120.210.15) can be used for several types of services.

Rule #1 was selected for the same reasons as in the previous case.

In rule #2, if someone from the Internet is looking for host 200.120.210.15 and for the server port ftp (21/TCP), the firewall will direct the connection to host server1.

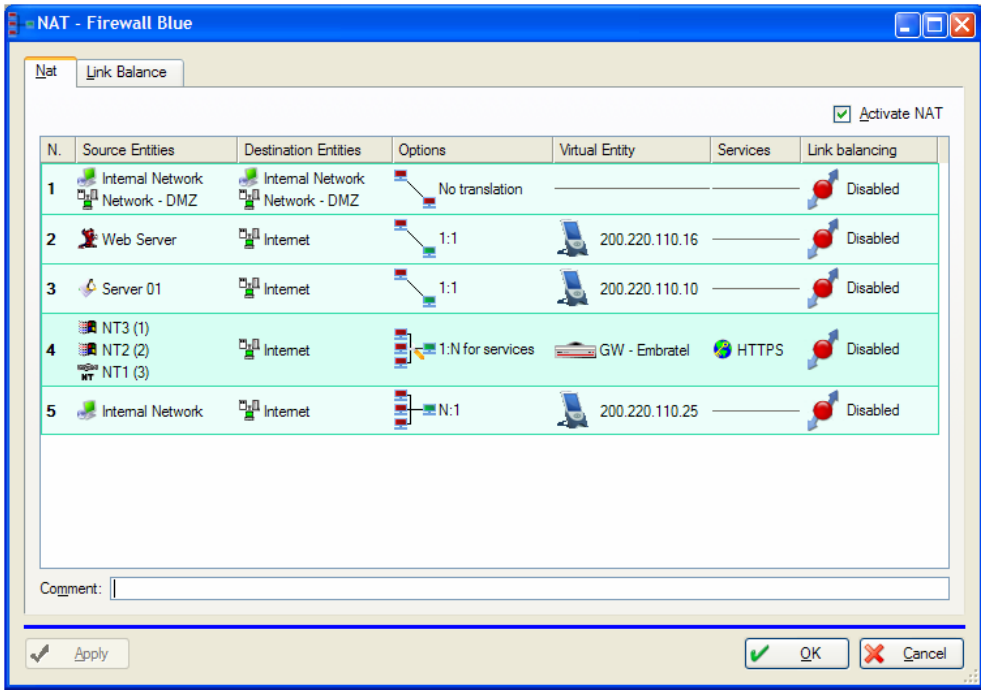
In rule #3, if someone from the Internet is looking for the same host 200.120.210.15, but at smtp port (25/TCP), the firewall will direct its connection to the Mail_SMTP entity address.

Rule #4 allows the company web server to be accessed through http port (80/TCP).

Rule #5 is an example of service port load balancing. In this case, someone on the Internet is looking for accessing IP 200.120.210.15 for secure web service (443/TCP). There are three servers available to accept this request: NT1, NT2, and NT3. The principles to attend these connections are the same explained in the previous case.

Finally, rule #6 enables any other host to originate Internet connection; in this case, the IP 200.120.210.15 will be seen at the destination.

Even though it is possible to use services translation as in case 1, Aker recommends that this configuration be used only if the company has just one valid Internet IP address.



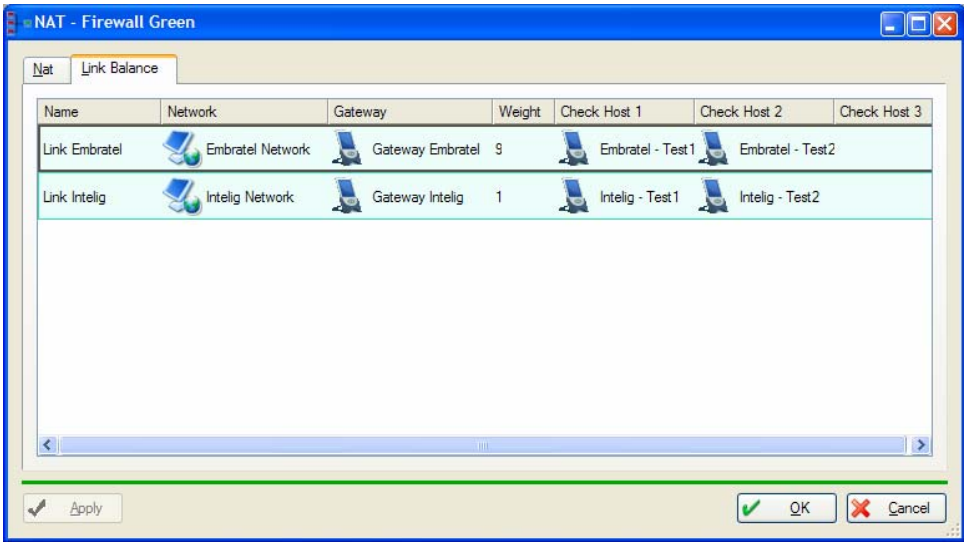
Examples – Case 3 – Link Balancing

Here, we will describe how to perform link balancing. Let's suppose the company has two Internet IP connection providers, for instance, Embratel and Intelig. In this case, each provider makes available a specific range of IP addresses to the company.

First step – Balancing Setup

The firewall administrator will set up for balancing, registering entities and providing the following information:

- **Name**: Input a name to represent the telecom operator link;
- **Network**: Register the network given by the operator;
- **Gateway**: Provide the operator's router IP address (in this case, the firewall will verify if the gateway really belongs to the operator's network);
- **Weight**: A value to be assigned to the link; higher values imply on faster links.
- **Check Host 1:** Register an entity you are sure it is adjacent to the operator router, preferably within one or two hops from your own router. The firewall will use this entity to determine whether the link is up or down. You may register an operator DNS server, or even nearby routers.
- **Check Host 2 and Check Host 3:** Verification entities also used by the firewall. It is not mandatory that all three verification entities be registered, although the more are configured, the better it is for the firewall verification system.

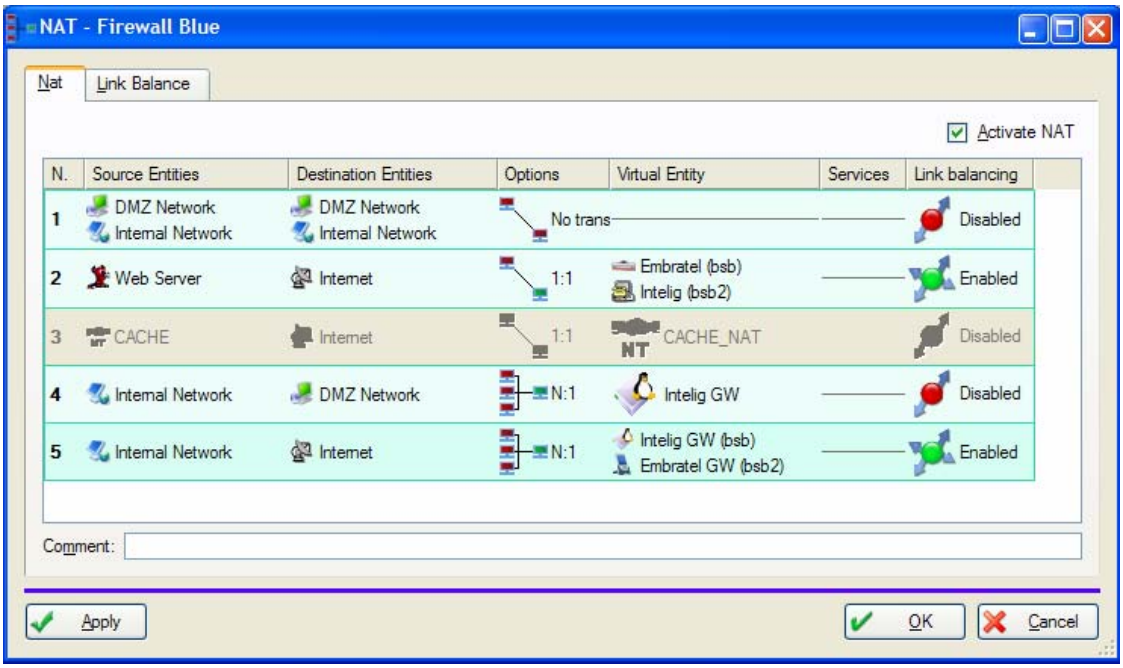


Second Step – NAT Rules Setup

The second setup step is quite simple. Just put in each translation rule two or more Virtual Entities, one with the address of a service provider.

Don't forget to enable, in the *Link balancing* column, the appropriate icon so that the service can be performed by the firewall. It is important to stress, that the firewall will also verify if the Virtual Entity actually belongs to a previously configured link.

A limitation of this approach is regarding the source of the Internet connection. The DNS must have pairs of IP addresses, and must operate in Round-Robin mode. The problem happens when an operator link is down, and the firewall has no way to redirect connections from the Internet. As a solution, the administrator could use scripts to remove, from the DNS, the IP of the non-working operator, because the firewall records this information in the event log.



7-3 Using the Command Line Interface

The NAT configuration command line interface is relatively simple, and has the same capabilities as the GUI, except for the fact that it is not possible to configure monitoring parameters.

Program location: `/etc/firewall/fwnat`

Syntax:

```
fwnat [help | show | activate | deactivate]
fwnat [enable | disable | remove] <pos>
fwnat add <pos> 1-1 <source> <destination> [ <virtual entity> |
                -bal <ve_1> <ve_2> ... ]
fwnat add <pos> n-1 <source> <destination> [ <virtual entity> |
                -bal <ve_1> <ve_2> ... ]
fwnat add <pos> services <source> <destination> [ <virtual
entity> |
                -bal <ve_1> <ve_2> ... ] <service1>...<service2>
fwnat add <pos> no_translation <source> <destination>\n"
fwnat add <pos> 1-n <source1>...<source2> <destination> <virtual
entity>
                -bal <ve_1> <ve_2> ... ] <round-robin | random>
<persist>
                <none | ping | HTTP <URL>>
```

Program help:

```
fwnat - Configures the Network Address Translation rules table
fwnat [help | show | activate | deactivate]
fwnat [enable | disable | remove] <pos>
fwnat add <pos> 1-1 <source> <destination> [ <virtual entity> |
                -bal <ve_1> <ve_2> ... ]
fwnat add <pos> n-1 <source> <destination> [ <virtual entity> |
                -bal <ve_1> <ve_2> ... ]
fwnat add <pos> services <source> <destination> [ <virtual
entity> |
                -bal <ve_1> <ve_2> ... ] <service1>...<service2>
fwnat add <pos> no_translation <source> <destination>\n"
fwnat add <pos> 1-n <source1>...<source2> <destination> <virtual
entity>
                -bal <ve_1> <ve_2> ... ] <round-robin | random>
<persist>
                <none | ping | HTTP <URL>>

       activate      = activates Network Address Translation
       deactivate    = deactivates Network Address Translation
       show          = show all NAT rules
       add           = adds a new NAT rule
       enable        = enables a disabled NAT rule
       disable       = disables an existing NAT rule
       remove        = removes an existent NAT rule
       help          = shows this message

For the add command:
       pos           = position where the new rule will be added
                       (It can be a positive integer or the word
END, to add
```

```
                        the rule at the end of the table)
       1-1           = performs a server translation. In this
case the source
                       must be an entity of the host type
       n-1           = performs a client translation
       services      = perform translation only for the supplied
services. In
                       this case the source must be an entity of
the host type
       no_translation= does not perform translation between
source and
                       destination
       1-n           = performs load balancing, that is, allows
the source
                       hosts to be accessed by the IP address
configured in
                       the virtual entity, as they were one
single host
       service1 ...  = list of service names for the new rule

For the enable / disable / remove commands:
       pos           = number of the rule to be enable, disabled
or removed
                       from the table

For the 1-n translation type:
       round-robin   = Uses the round-robin algorithm for
balancing
       random        = Uses the random algorithm for balancing
       none          = Doens't monitor the source hosts, that
is, consider
                       them to be always up
       persist       = Destination server persistence time
(mins) across
                       connections from the same client
       ping          = Monitors source hosts through pings
       HTTP          = Monitors source hosts through HTTP
connections
       URL           = Especifies the URL to be used to monitor
the source
                       hosts, in case of HTTP monitoring
```

Example 1: (Viewing the configuration)

```
#/etc/firewall/fwnat show

Global Parameters:

Network address translation: Activated

Network address translation rules:
----------------------------------

Rule 01:
--------
Type            : no_translation
Source          : Internal network
Destination     : Internal network

Rule 02:
--------
```

```
Type            : services
Source          : Server
Destination     : Internet
Virtual entity  : Firewall - external interface
Services        : MYSQL                    POP3
                  SMTP

Rule 03:
--------
Type            : 1-1
Source          : Web Server_001
Destination     : Internet
Virtual entity  : External Web server

Rule 04:
--------
Type            : 1-n
Source          : server1                    server2
                  server3
Destination     : Internet
Virtual entity  : Virtual Server
Balancing       : random         Monitoring: http
URL             : www.aker.com.br

Rule 05:
--------
Type            : n-1
Source          : Internal Network
Destination     : Internet
Virtual entity  : Firewall - external interface
```

Example 2: (Adding a 1-1 translation rule at the end of the table, mapping the *SMTP Server*, with reserved address, to the *External Server,* with a valid address, to all Internet hosts.)

```
#/etc/firewall/fwnat add end 1-1 "SMTP Server" Internet
"External Server"
Rule added at position 6
```

Example 3: (Adding a translation rule in the beginning of the table)

```
#/etc/firewall/fwnat add 1 services "Server 2" Internet
"External Server 2" Telnet FTP
Rule added at position 1
```

Example 4: (Removing rule 3)

```
#/etc/firewall/fwnat add 1 services "Server 2" Internet
"External Server 2" Telnet FTP
Rule added at position 1
```

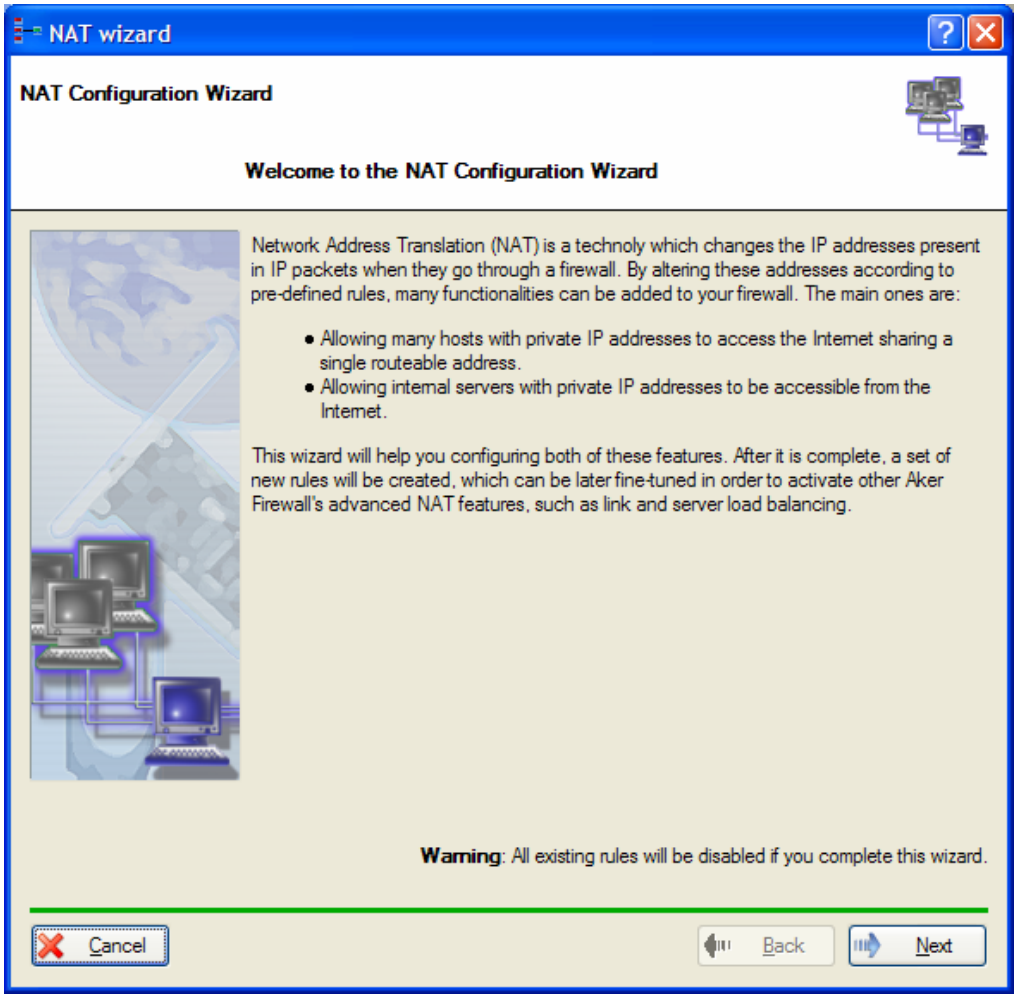
Example 5: (Adding a 1-N translation rule, load balancing, mapping servers *srv01* and *srv02* into an external host called *external_srv*, for all Internet hosts, and monitoring by ping)

```
#/etc/firewall/fwnat add 4 1-N srv01 srv02 Internet external_srv
round-robin ping
Rule added at position 4
```

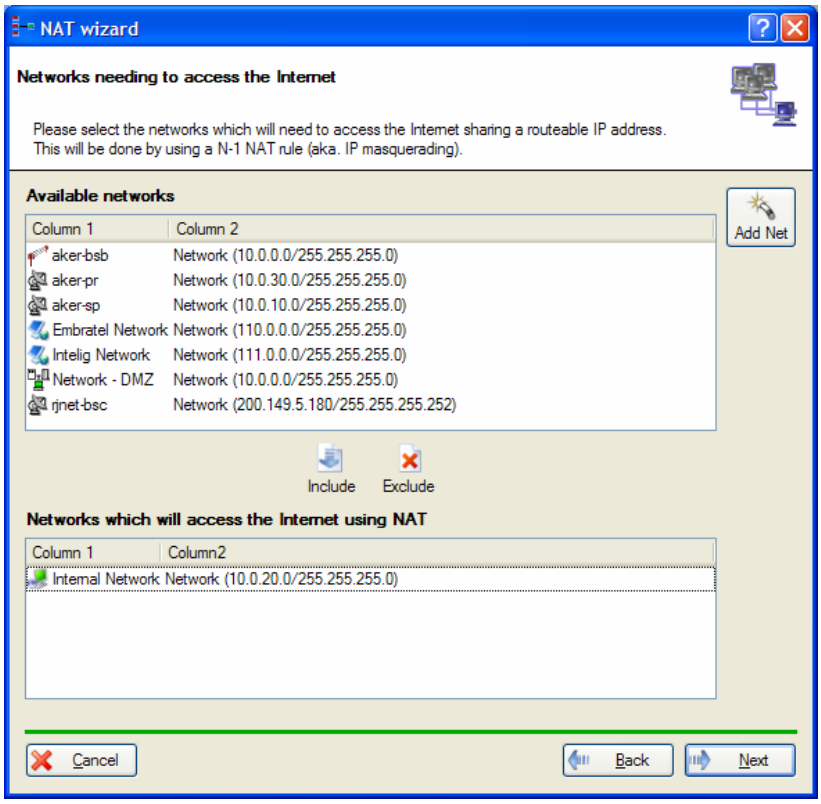
7-4 Using the NAT Configuration Wizard

The NAT Configuration Wizard can be activated either from the toolbar or the menu. The windows below prompt for information to help configuring the translation.

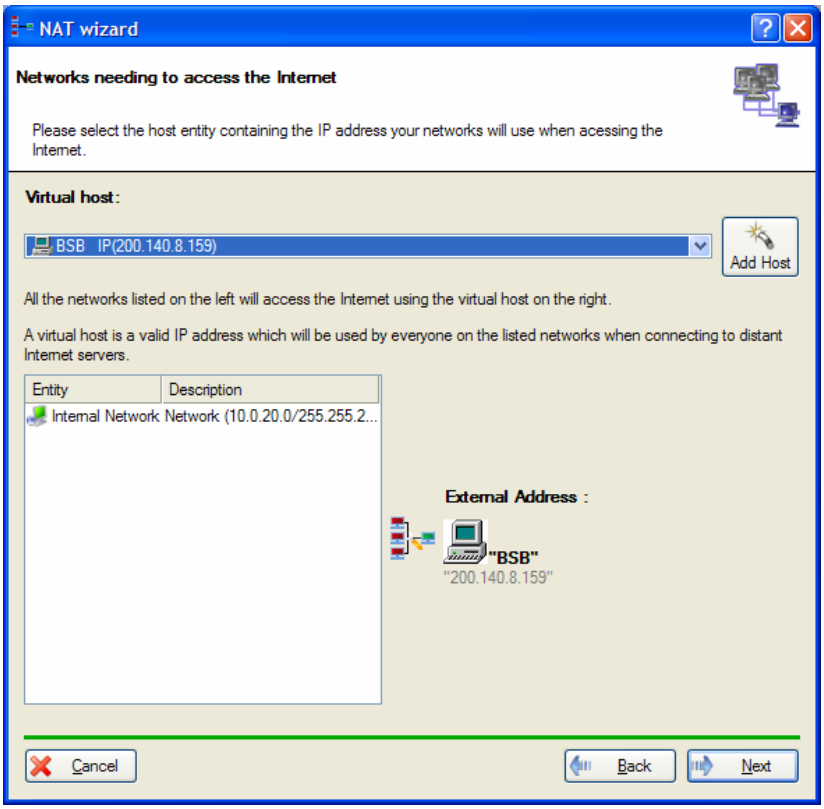
1 – The initial window gives information about NAT. Click on the Next button to proceed with the configuration.



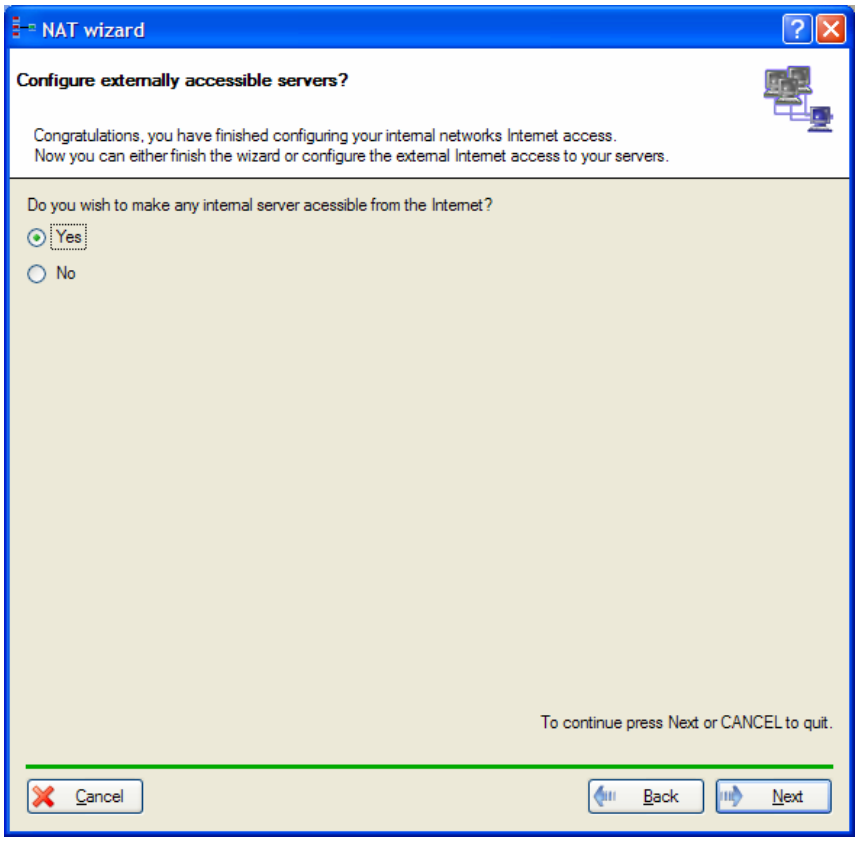
2 – Select the networks that will access the Internet.



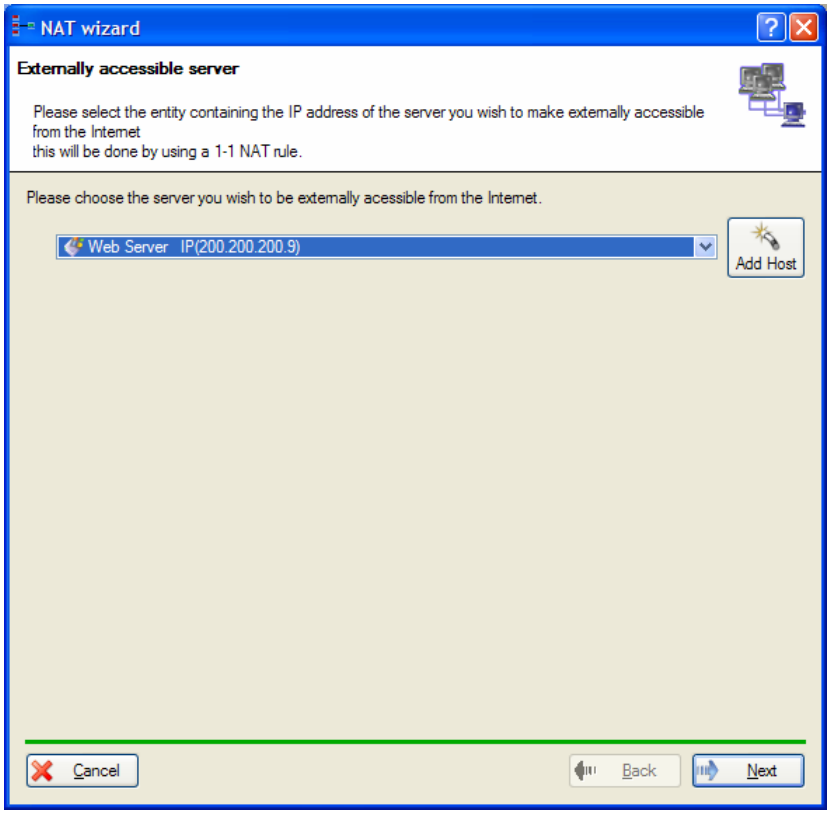
3 – Choose the IP of the virtual host to perform the N-1 translation.



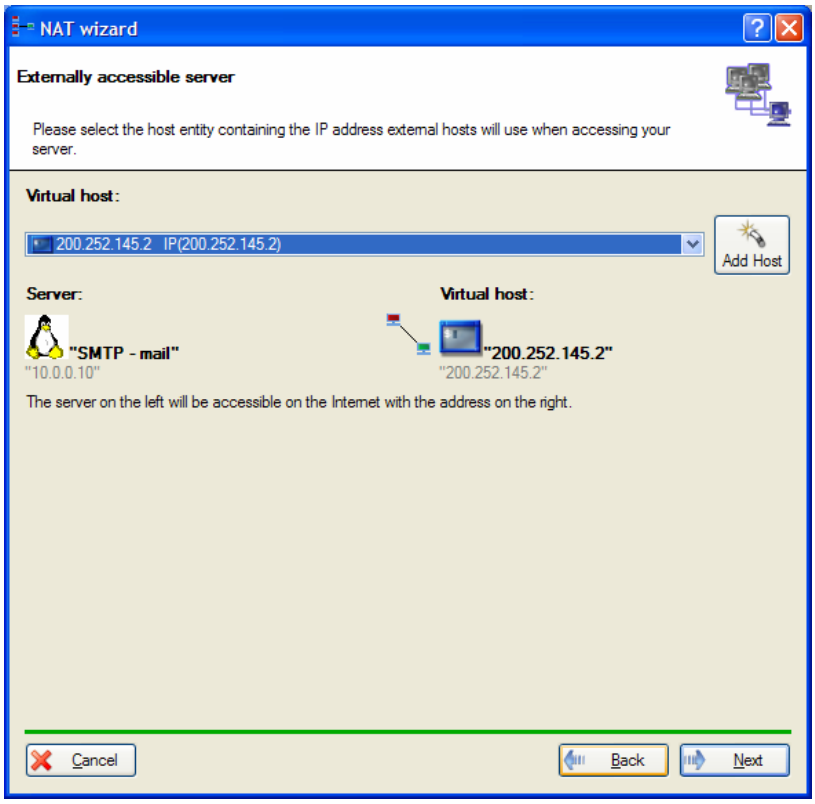
4 – Choose *Yes* if you want to configure the servers that will be exposed to the Internet.



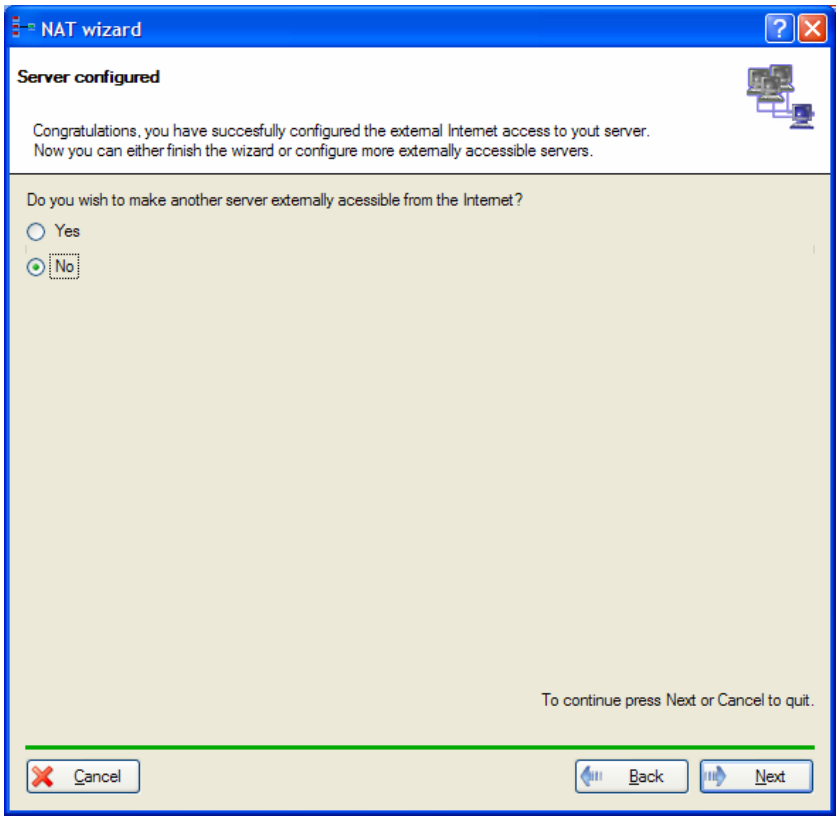
5 – Choose the entity that will be available through the Internet.



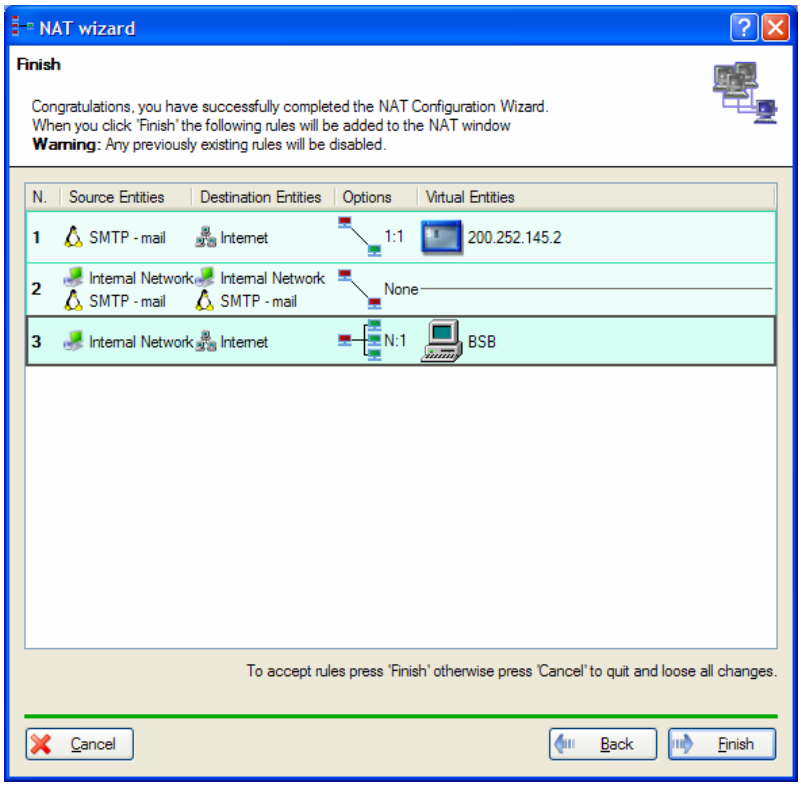
6 – Choose the IP of the virtual host that will be available to the Internet.



7 – This screen prompts for the configuration of more servers.



8 – Final NAT Wizard screen showing the rules created by it.



8-0 Creating Secure Channels

We will show here how to configure the rules that will establish secure Internet communication channels. These secure channels are used to interconnect organizations through the Internet, in such a way that the data can flow between them without the risk of being read or modified by strangers.

8-1 Planning the Installation

What is a secure data channel and what is it used for?

The Internet is a network composed of thousands of hosts spread all over the world. When two hosts are communicating, the whole traffic between them passes through several other hosts (routers, switches, etc.) from its source to its destination. Almost always, these intermediary hosts are administrated by third parties and nothing can be said about their honesty (in most cases, it is not possible to know in advance through which hosts the packets will pass until they reach their destination).

Any one of these hosts that is on the way of the packets can view their contents and/or alter any of them. This is a serious problem and its significance increases when there is the need of transmitting confidential and important data.

In order to solve this problem, a secure data channel can be used. A secure data channel can be seen as if it were a tunnel. The information is placed on one end of the tunnel and they can be read again only at the other end.

In the reality, a special treatment is given to the data that will be transmitted so that they can neither be altered during their way (authentication), nor viewed (encryption). The combination of the two techiques produces invisible and unalterable data for any host met on the way of the packets, from the source to the destination.

What is encryption?

Encryption is the combination of a key with a mathematical algorithm based on a one-way function. This algorithm is applied to the data together with the key in order to make them undecipherable for anyone who sees them. The way it is done guarantees that it is possible to obtain the original data only in case where both the algorithm and the key used are known.

If one of these two components is kept secret (in this case, the key), viewing the data by others becomes impossible.

What is authentication?

Authentication is also the combination of a key with a mathematical algorithm based on a one-way function. The difference from encryption is that this algorithm, when applied to the data, does not produce undecipherable data, but a *digital signature*. This signature is generated so that any person who is not aware of the algorithm, or the key used to generate it, is unable to calculate it.

When the digital signature is generated, it is transmitted to its destination together with the data. In case they have suffered any alterations on the way, when the recipient calculates the digital signature of the data received and compares it with the signature received, it will realize that the two are different and conclude that the data will has been altered.

The authentication is a quite fast operation compared to the encryption. However, it does not prevent the data from being read. It should be used only in the cases where reliability, but not confidentiality, is needed. If both are required, authentication is used together with encryption.

What is digital certification ?

Through the authentication process, described above, it is possible to certify the source of the messages in a comunication between two entities. However, in order to do this, it is necessary that the entities that are communicating have already exchanged some information before the actual communication can take place. This information exchange usually consists of the algorithm to be used for authentication and its key.

The problem arises when it becomes necessary to certify the source of the messages from an entity which previous communication have never existed. The only way to solve this problem is to delegate to a third entity the power to perform these certifications. This third entity is called **Certification Authority** and, in order for it to certify the source of a message, it must have already performed an information exchange with the entity which is being certified.

What is a digital certificate ?

A digital certificate is a document provided by the Certification Authority for each of the entities which will perform a communication, in order to certify their authenticity.

Types of authentication and encryption algorithms

There are several authentication and encryption algorithms nowadays. In this section, only the algorithms supported by Aker Firewall will be described.

One of the parameters to measure the resistance of an algorithm is the size of its keys. The greater the number of bits of the keys, the greater the number of possible combinations and, theoretically, the greater the resistance of the algorithm against attacks.

Authentication algorithms:

- MD5

MD5 is the acronym for *Message Digest 5*. It is an algorithm created and patented by the RSA Data Security, Inc; however, with liberated use for any applications. It is used to generate digital signatures of 128 bits for messages of any size and it is considered a quite fast and secure algorithm.

- SHA

SHA is the acronym for *Secure Hash*. It is an algorithm that generates digital signatures of 160 bits for messages of any size. It is considered more secure than the MD5, however, it has an average of 50% inferior performance in the implementation of the Aker Firewall.

The version implemented by the Aker Firewall is the SHA-1, a revision in the initial algorithm to correct a small failure. However, it will always be called SHA in this manual and in the administration interfaces.

Secret key encryption algorithms:

- The secret key algorithms are used to encrypt information streams. They have just one key, which is used to encrypt and decrypt the data.

- DES

The algorithm DES is an acronym for *Data Encryption Standard*, it was created by IBM in the 70s and it was adopted by the American government as their standard until recently. It is quite a fast algorithm in hardware implementation; however, not so fast when implemented in software. Its encryption keys have fixed length of 56 bits, which is considered insufficient for the current standards. Due to this, preference should be given to other algorithms in case of critical applications.

- Triple DES or 3DES

This algorithm consists of the application of the DES algorithm three times, using three different keys, to the same data. This is the same as using an algorithm with a key of 112 bits, what ensures much higher level of security than the one offered by DES. The problem of this algorithm is that it is twice slower than the DES, in the implementation used in Aker Firewall.

- AES

The AES algorithm was chosen, among several competing others, by NIST to replace the already insecure and ineffective DES. AES stands for Advanced Encryption Standard. The algorithm chosen in the contest was the Rijndael. It uses a 256-bit key, being much faster and more secure than the DES or even the 3DES.

Aker Firewall works with AES using keys sizes of 256 bits, which provides a very high security level. This is the recommended choice.

- Blowfish

The Blowfish algorithm was created as a possible substitution for the DES. It is a very fast algorithm (when compared to other encryption algoritms), very secure and can work with several key sizes, from 40 to 438 bits.

Aker Firewall works with Blowfish using keys sizes of 128 and 256 bits, which provides a very high security level.

Public key encryption algorithms:

The public key algorithms have a pair of associated keys, one used to encrypt and the other to decrypt the data. They are vey slow when compared to the secret key algorithms and, due to it, are normally used to perform digital signatures and to establish session keys, which will then be used in a sercret key algorithm.

- RSA

The RSA is an algorithm based in modular arithmetic, capable of working with keys of any size, however, values lower than 512 bits are considered too weak. It can be used to encrypt and decrypt data, however, due to its slowness when compared to secret key algorithms, its main use is in digital signatures and in session keys establishment.

- Diffie-Hellman

The Diffie-Hellman algorithm in fact isn't an encryption algorithm since it cannot be used to encrypt or decrypt data or perform digital signatures. Its only function is to allow session key establishments. It is also based on modular arithmetic and can work with keys of any size, however, keys with less then 512 bits are considered to weak.

Key exchange algorithms

Two basic issues when configuring a secure channel are: (a) how to set up authentication keys and encryption algorithms, as well as (b) how to perform periodic exchanges of these keys.

It is important to periodically exchange keys to decrease both, the chance of them being broken by an attacker, and the impact in case an attacker cracks any of the keys. Suppose that after trying for six months, an attacker manages to break one of the keys used by an encryption algorithm (this time period is totally hypothetical, having no relation with real situations). If a company uses the same keys during a year, for example, an attacker will be able to decode six months of its traffic. On the other hand, if the keys are exchanged daily, this same attacker, after six months trying, will decipher only the traffic of the first day, and will have to work six more months to be able to decode the traffic of another day, and so on.

Aker Firewall has four key exchange methods: IPSEC-IKE, AKER-CDP, SKIP, and manual:

- IPSEC-IKE key exchange

IPSEC This option will only be available when the entire set of IPSEC protocols is used.

The IPSEC (IP Security) is a set of standardized protocols (RFC 2401- RFC 2412) developed by IETF. IPSEC offers secure data transmission through public or private IP network. To establish an IPSEC connection three steps are required:

1. Security level negotiation.
2. Authentication and integrity.
3. Confidentiality.

To implement these three steps, IPSEC uses three mechanisms:

AH - Autentication Header
ESP - Encapsulation Security Payload
IKE - Internet Key Exchange Protocol

We strongly recommend this option to configure secure channels

- Aker-CDP key exchange

  Aker-CDP is a protocol designed by Aker Security Solutions, which enables a totally automatic configuration of secure channel parameters. It is based on the SKIP protocol, and offers all of its advantages for key exchanging described in the next paragraph. It does not need, however, manual configuration of shared secrets as SKIP does which is a big plus. Everything is done automatically.

  To ensure maximum security, all key exchanging is done through digital certificates signed by Aker itself, or by other certification authorities. These certificates use the Diffie-Hellman and RSA protocols, both with 1024 bits.

  The encryption and authentication algorithms to be used may be specified, the same way as with the SKIP protocol, or left in automatic mode, which will make the two communicating firewalls negotiate the most secure algorithm supported by both.

- SKIP key exchange

  SKIP is an acronym for *Simple Key Management for IP*. Basically, it is an algorithm that allows automatic key exchange with extremely high frequency, what makes cracking these keys nearly impossible. SKIP operation is complex and out of this manual's scope. We will only give a brief description about it.

  Basically, SKIP works with three different levels of keys:

- A secret shared by two parties who want to communicate (manually configured, in Aker Firewall case).
- A master key, recalculated at every hour, based on the shared secret.
- A random key that may be recalculated at any desired time.

Generally speaking, to establish the communication, the algorithm generates a random key and uses it to encrypt and authenticate data that will be transmitted. Then, it encrypts this random key with the master key, and sends them along with the encrypted data. After receiving the packet, the recipient decrypts the random key, using the master key it has, and uses it to decrypt the rest of the packet.

The algorithms used to authenticate and encrypt the packet, and to encrypt the key, are defined by the sender, and informed as part of the protocol. Therefore, the recipient does not need to configure these parameters.

The main advantage of using SKIP is the possibility to utilize the same shared secret for years, without any risk of an attacker breaking the keys since key exchanging is performed at very short time periods, from seconds up to one hour, depending on the traffic between the communicating networks.

- Manual key exchange

  In this case, key configuration is done manually. This means that at every key exchange, both Firewalls participating in the secure channel will have to be reconfigured simultaneously.

Types of secure channels

The Aker Firewall permits the creation of two distinct types of secure channels, called Firewall-Firewall and Client-Firewall. Each one of these channels have different objectives and limitations and usually are combined together to archive the maximum in security and flexibility.

- Firewall-Firewall secure channels

This type of secure channel is the most common and is supported by Aker Firewall since its version 1.31. It consists of the use of encryption and authentication between two firewalls, interconnected through the Internet or any other network. The channel end points are the two firewalls, which means that all encryption is done transparently by them and no additional software needs to be installed in any client host.

The only limitation of this solution is that it needs the presence of two firewalls, one in the entry point of each network, in order to allow the creation of the channel.

- Client-Firewall secure channels

These channels are supported by Aker Firewall since its version 3.10. They permit that a client host (Windows 95™, Windows 98™, Windows NT™ or Windows 2000™) establishes a secure channel directly with an Aker Firewall. To accomplish this, it is necessary the installation of a program, called Aker encryption client, in each client host.

The main advantage of this technology is to allow clients to access a coorporative network through dial-up lines with total security and transparency (transparency in the way that applications which are running in the host with the encryption client installed are not aware of its existance and continue to function normally).

This technology is very useful, however it has some disadvantages and limitations:

- It is necessary the installation of a software, the Aker encryption client, in all client hosts;
- The encryption client is not available to all platforms;
- If the encryption client is behind a firewall (accessing the network protected by another firewall, to which the secure channel will be established), the configuration of the last one must be modified to allow the routing of the secure channel traffic. In this case, the firewall directly in front of the client will not be able to control its traffic selectively, since it is encrypted. This can cause problems with some services.

Defining a firewall-firewall secure channel

In order to define a firewall-firewall secure channel we will first have to choose two groups of hosts that will exchange information in a secure way. These groups of hosts will have their packets authenticated and if desired, encrypted. A firewall at either of the channel is necessary. These firewalls will be responsible for authenticating/verifying and encrypting/decrypting the transfered data.

To define the groups of hosts, the concept of entities, shown in the chapter Registering Entities, will be used. A host, network or set can be used as entities in this definition.

In case you are not using Aker-CDP protocol, besides the entities, it is also necessary to choose the algorithm that will be used for the authentication and, if it is the case, for the encryption. It will also be necessary to configure the authentication and encryption keys.

Aker Firewall supports the existence of several simultaneous secure channels between different points. These several channels together produce a list where each entry defines the parameters of a secure channel completely. Each one of these entries receives the name *Security Association or AS*.

The planning of these secure channels should be done very carefully. The encryption is a costly operation that demands a very high processing power. This way, encrypting packets which do not really need security will be a waste of resources. Moreover, different encryption algorithms demand different amounts of processing power and, consequently, produce a higher level of security. Depending on the security level required, it is possible to choose either algorithm (each algorithm supported by Aker Firewall is described in the previous section).

The last remark on secure channels is that they are one-way. This means that in case it is desired to configure secure communication between two networks, A and B, two different channels must be configured: a channel with source in the network A and destination in the network B and another with source in the network B and destination in the network A. The packets sent from A to B will follow the configuration of the first

channel and the packets from B to A will follow the second. This will be illustrated more clearly in the examples bellow:

Examples of firewall-firewall secure channels use

Basic example of a firewall-firewall secure channel configuration

In this example it will be shown how to define a secure channel of communication between two networks, through the Internet, using two Aker Firewalls. The channel will be created so that all the communication between these two networks will be secure. The MD5 was chosen as the authentication algorithm and the DES as the encryption algorithm.

The use of an authentication algorithm is obligatory for all the channels, that is, the creation of encryption only channels is not allowed. This is necessary since without the authentication, the encryption algorithms are exposed to *cut and paste* attacks.

- **Network 1 Aker Firewall configuration**

Entities:

NETWORK1 - IP address: **A1.B1.C1.0 -** Netmask **255.255.255.0**
NETWORK2 - IP address: **A2.B2.C2.0 -** Netmask **255.255.255.0**

Secure channel 1:

Direction of the channel: **send**
Source entities: **NETWORK1**
Destination entities: **NETWORK2**
Encryption algorithm: **DES**
Authentication algorithm: **MD5**
Authentication key: **X1**
Encryption key: **X2**

Secure channel 2:

Direction of the channel: **receive**
Source entities: **NETWORK2**
Destination entities: **NETWORK1**
Encryption algorithm: **DES**
Authentication algorithm: **MD5**
Authentication key: **X3**
Encryption key: **X4**

- **Network 2 Aker Firewall configuration**

Entities:

NETWORK1 - IP address: **A1.B1.C1.0** - Netmask **255.255.255.0**
NETWORK2 - IP address: **A2.B2.C2.0** - Netmask **255.255.255.0**

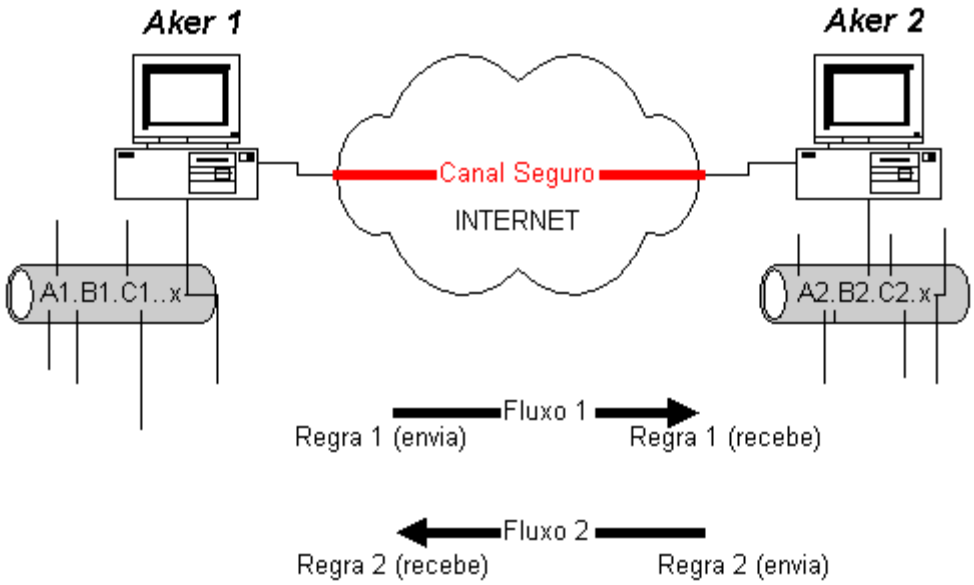
Secure channel 1:

Direction of the channel: **receive**
Source entities: **NETWORK1**
Destination entities: **NETWORK2**
Encryption algorithm: **DES**
Authentication algorithm: **MD5**
Authentication key: **X1**
Encryption key: **X2**

Secure channel 2:

Direction of the channel: **send**
Source entities: **NETWORK2**
Destination entities: **NETWORK1**
Encryption algorithm: **DES**
Authentication algorithm: **MD5**
Authentication key: **X3**
Encryption key: **X4**

Notice that the secure channel 1 of the *Aker Firewall 1* is exactly the same as the secure channel 1 of the *Aker Firewall 2*, except for the field related to the direction. The same applies to the secure channels 2.



Example of a firewall-firewall secure channel configuration for a subnet

In this example our secure channel will be defined only for a group of hosts in either of the two networks. Besides, we will define different algorithms for the channels between these groups.

Configuring different algorithms for the two directions of a secure channel can be interesting when the information of a certain direction have a greater value than the ones of the channel of opposite direction. In this case, a more secure algorithm is used in the most critical direction.

In this example, let's assume that the networks 1 and 2 have two class B addresses: A1.B1.0.0 and A2.B2.0.0, respectively.

- **Network 1 Aker Firewall configuration**

Entities:

SUBNET1 - IP address: **A1.B1.2.0 -** netmask **255.255.255.0**
SUBNET2 - IP address: **A2.B2.5.0 -** netmask **255.255.255.0**

Secure channel 1:

Direction of the channel: **send**
Source entities: **SUBNET1**
Destination entities: **SUBNET2**
Encryption algorithm: **DES**
Authentication algorithm: **MD5**
Authentication key: **X1**
Encryption key: **X2**

Secure channel 2:

Direction of the channel: **receive**
Source entities: **SUBNET2**
Destination entities: **SUBNET1**
Encryption algorithm: **3DES**
Authentication algorithm: **SHA**
Authentication key: **X3**
Encryption key: **X4**

- **Network 2 Aker Firewall configuration**

Entities:

SUBNET1 - IP address: **A1.B1.C1.0 -** netmask **255.255.255.0**
SUBNET2 - IP address: **A2.B2.C2.0 -** netmask **255.255.255.0**

Secure channel 1:

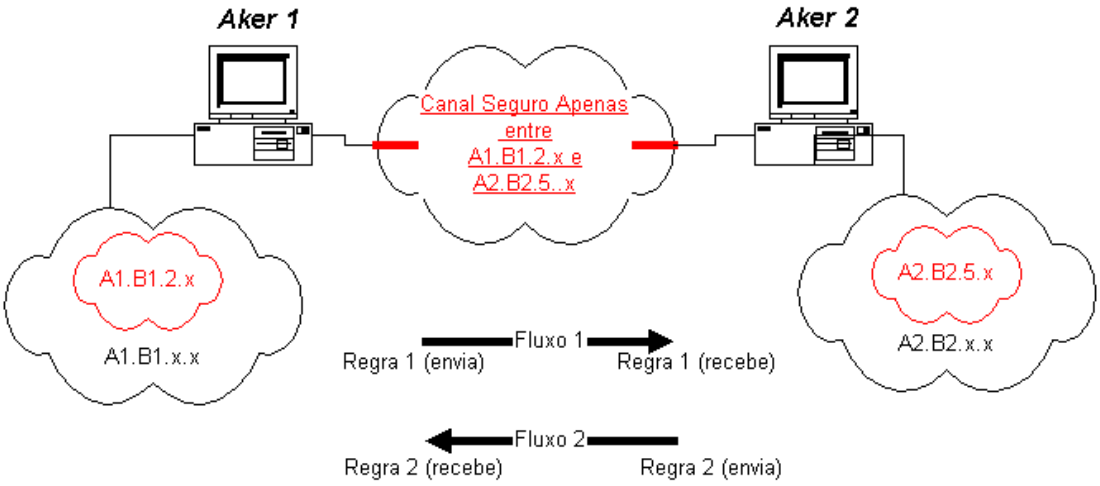
Direction of the channel: **send**
Source entities: **SUB_NETWORK2**
Destination entities: **SUB_NETWORK1**
Encryption algorithm: **3DES**
Authentication algorithm: **SHA**

Authentication key: **X3**
Encryption key: **X4**

Secure channel 2:

Direction of the channel: **receive**
Source entities: **SUBNET1**
Destination entities: **SUBNET2**
Encryption algorithm: **DES**
Authentication algorithm: **MD5**
Authentication key: **X1**
Encryption key: **X2**

Notice that in this case the secure channels appear in a different order in the two firewalls: secure channel 1 in the Firewall 1 is the same as secure channel 2 in the Firewall 2 (with inverted directions) and secure channel 2 in the Firewall 1 is the same as secure channel 1 in the Firewall 2 (again with inverted directions). In this example, the order of the rules does not make any difference (notice, however, that in some cases this cannot be true):



8-2 Aker-CDP certificates

There are four types of encryption certificates in the Aker Firewall. Each has different objectives and functions within the Aker-CDP protocol. They are:

- Local certificate

It is the negotiation certificate of the firewall being administered. Aker Security Solutions, or any other Certification Authority, issues this certificate. Only one local certificate is allowed at a time, and in case a new one is loaded, it will automatically replace the old one.

This certificate will be automatically sent to other firewalls or encryption clients, when a secure channel is being established.

- Remote certificate

These are the local certificates received by our firewall from other firewalls, when negotiating secure channels through the Aker-CDP protocol.

- Certification Authorities certificate

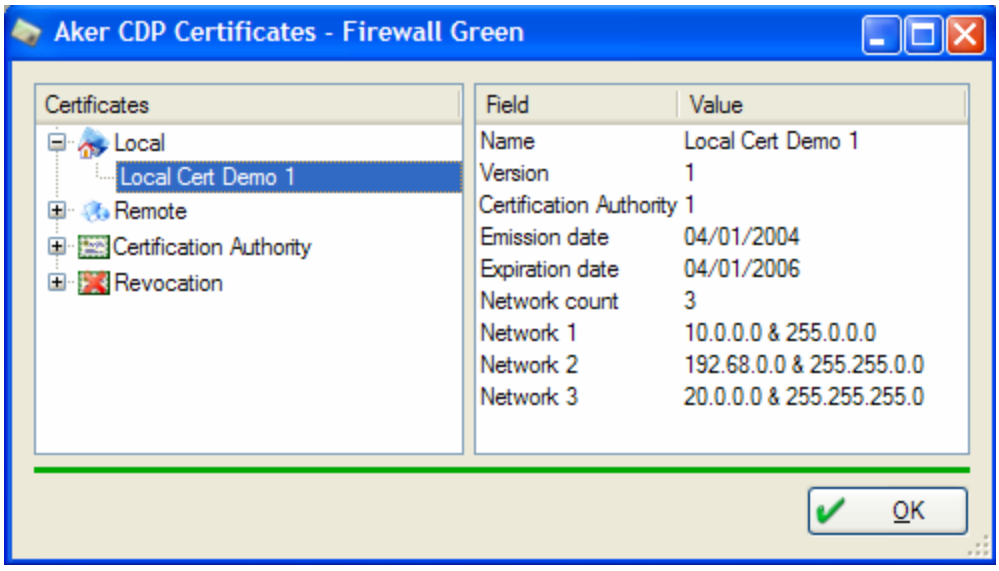
Contains the information from the institutions authorized to issue negotiation and revocation certificates. To be accepted, these certificates must be signed by a Certification Authority known by the firewall.

- Revocation certificate

These certificates are generated when any firewall negotiation certificate is compromised. Revocation certificates indicate which certificates should no longer be accepted by the firewall.
All these certificates can be viewed in the certificates window. To access it, do the following:

- Click on *Cryptography* menu in the firewall window you want to manage
- Choose *Aker CDP Certificates*

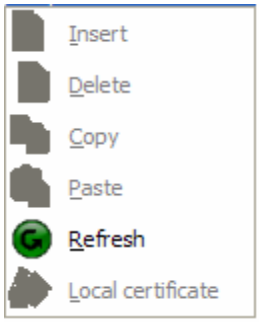
The Certificates Window



The Certificates Window displays all certificates related to Aker-CDP secure channel connections.

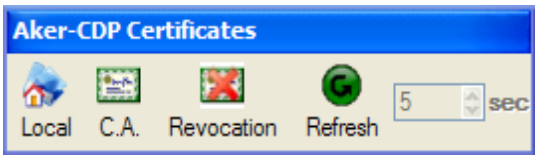
- The **OK** button closes the certificates window.
- The list to the left side of the window shows the different types of certificates..
- By clicking on a certificate, its most important fields will be displayed in the right side of the window
- The **Delete** button, located in the toolbar, removes a certification authority certificate. It will only be enabled if a certificate of this type is selected.
- The **Refresh** button, located in the toolbar, will update the displayed information. The first click activates the automatic refresh. To disable it, just click on it again. To configure the refresh time, change the value next to the button, accordingly.

When you right click on a certificate, the following window will be displayed:



Certificates fields, displayed on the right, are only for information purposes. It is not possible to alter their values

To load a new certificate, do the following:



1. Choose the type of certificate you want to load by right clicking on it, either in the Certificates Window, or in the toolbar. The available certificates are **Local**, **Certification Authority** and **Revocation**.
2. A window will show up where you can indicate the loading file name and location. Then, click on the **Open** button.

In order to use secure firewall-firewall channels using the Aker-CDP protocol, and activate the secure client-firewall channel support, it is necessary to load the local encryption certificate. Aker Security Solutions, or an authorized representative, provides this certificate at the time Aker Firewall with encryption option is purchased

8-3 IPSEC Certificates

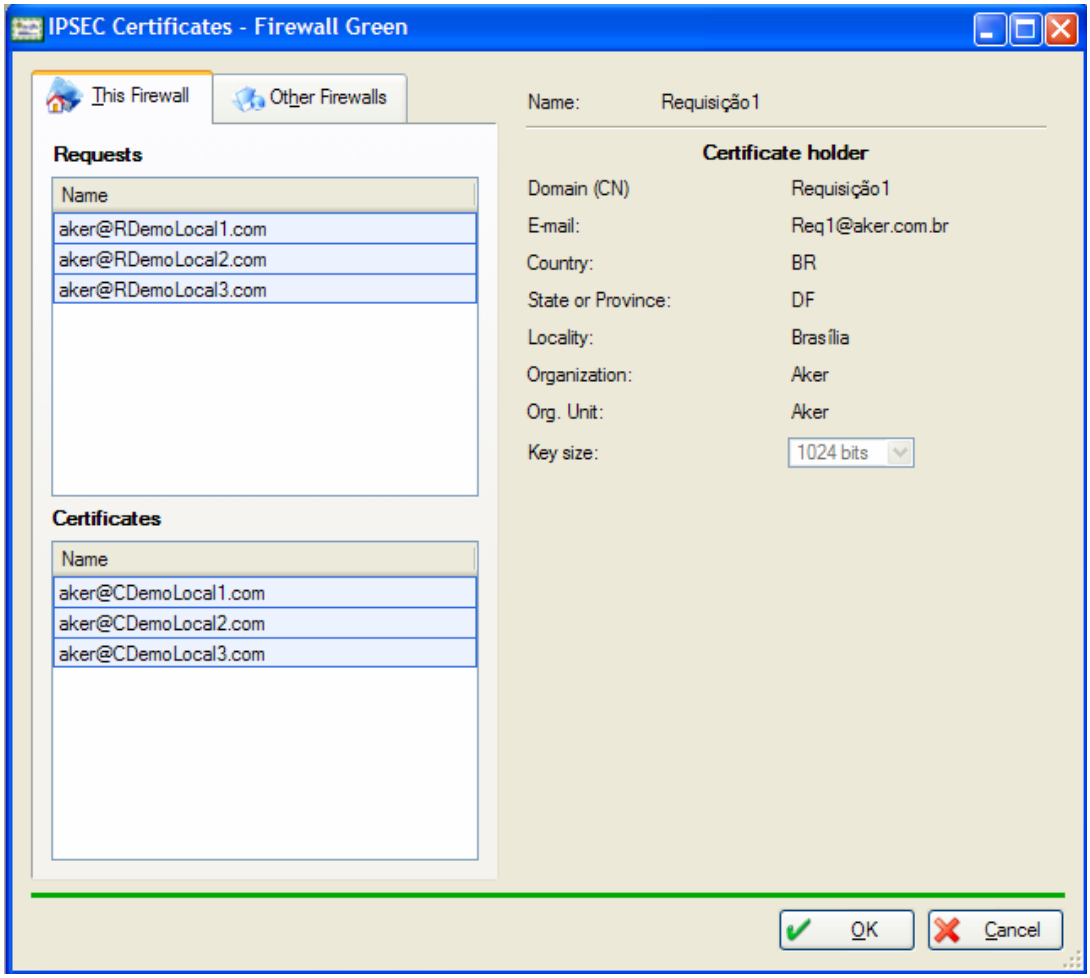
IPSEC certificates follow X.509 standard. They are used by a firewall to identify itself to another firewall, when establishing encrypted firewall-firewall channels, in IPSEC standard (see section below Configuring IPSEC tunnels). Their use, however, is not mandatory, since it is possible to establish an IPSEC tunnel by authenticating both parties using shared secrets.

To accept firewall certificates, a firewall must also have a certificate issued by the same Certification Authority.

To access the Certification Maintenance Window, do the following:

- Click on the *Cryptography* menu in the main window
- Choose *IPSEC Certificates*

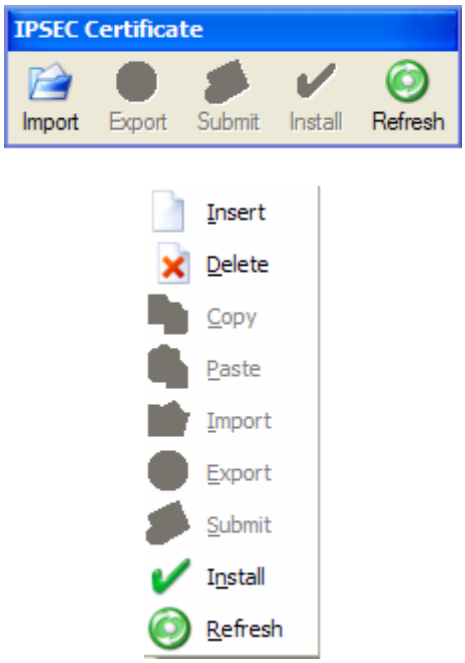
The IPSEC certificates and requests window



The IPSEC Certificates window contains Aker Firewall certificates and requests.

A request is a form to be filled with your data so that the Certification Authority can issue a certificate. A certificate is an ID card to guarantee the owner really is who he/she claims to be. When negotiating an IPSEC channel with other firewall, Aker Firewall uses these certificates to identify itself to the other firewalls. Thus, both firewalls, involved in an IPSEC firewall-firewall channel, have to generate their own certificate.

This window's operations can be found in the toolbar above the IPSEC Certificates window, or by right clicking over the desired field.



- The **Insert** button includes a new local or remote request. Local requests and certificates can be found in This Firewall window, while remote certificates and requests are found in the Other Firewalls window.
- The **Delete** button removes the selected certificate/request from the list.
- The **Export** button saves the selected certificate.
- The **Submit** button loads an exported certificate, or one according to the selected request. (This button is only active when inserting a new certificate.)
- The **OK** button will update and close the window.

Before generating a certificate, it is first necessary to generate a request in Aker Firewall. With this request, ask a Certification Authority to generate the certificate. Then, import it to the Aker Firewall.

This window is dynamically updated, i.e., it is not possible to cancel a submitted request. When inserting a new local request, local requests and certificates will be deleted. The same will happen to them, when importing a new local certificate with pair of keys (.pfx).

Therefore, the operation occurs as follows (for a local certificate):

1. Create a local request.
2. Send this request to a Certification Authority

3. Wait until the Certification Authority issues and returns the corresponding certificate
4. Load the certificate (click on Request, then on Load)

The procedure is different to create a certificate for a remote firewall:

1. Create a remote request.
2. Send this request to a Certification Authority.
3. Wait until the Certification Authority replies with the corresponding certificate.
4. Load the certificate (click on Request, then on Load)
5. Export/save the certificate to/in a PKCS#12 file (click on the remote certificate, and then, on Export)
6. Import this certificate in the remote firewall, selecting *This Firewall*, and then, right clicking on *Import*.

In the request window, there are two fields that may be confusing:

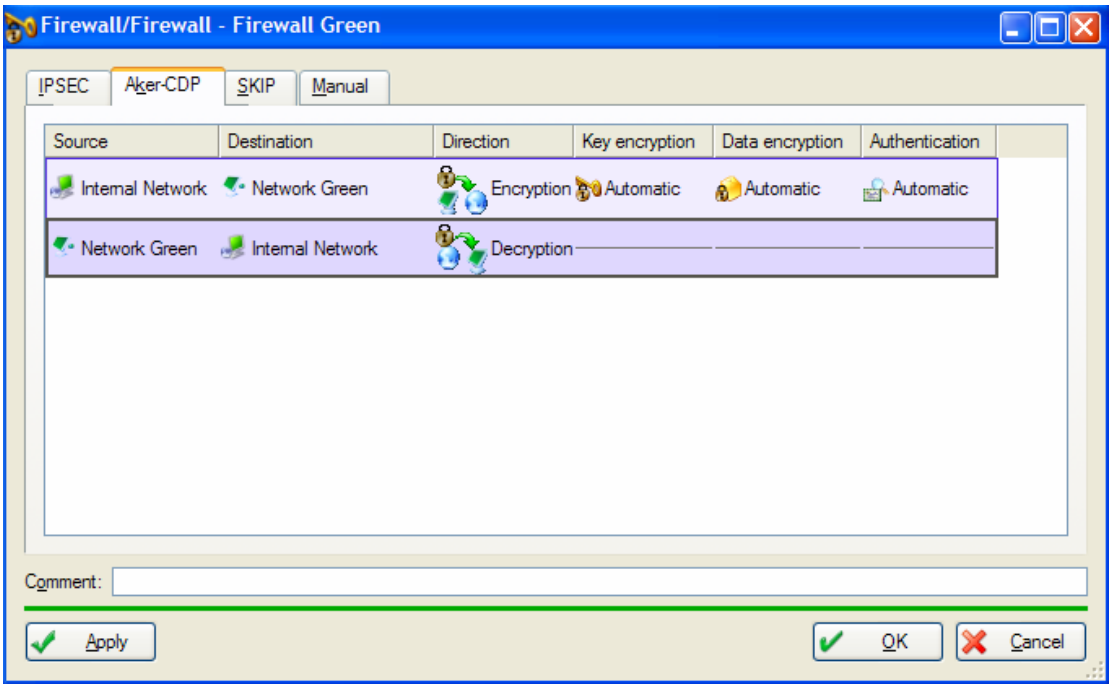
- **Domain (CN):** It is the main identifier of the request owner. This field must be filled with the *common name*.
- **Key size:** If the certificate is remote, or local with the creation of a new key, this field will store the key size in bits. Otherwise (additional local certificate), this field may not be modified, once the existing key will be used.

8-4 Configuring Firewall-Firewall channels

To access the Firewall-Firewall channel configuration window, do the following:

- Click on the *Cryptography* menu in the main window
- Choose *Firewall-Firewall*

The Firewall-Firewall cryptography window

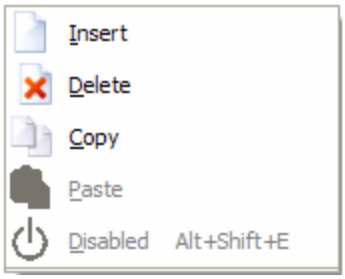


The cryptography window has the definition of all Aker Firewall encryption flows. Each flow is displayed on a separate line, made out of several cells. Selected flows will be shown in a different color. The window is composed of four tabs, where each one is used to configure encryption flows using a different key exchange mechanism.

- The **OK** button will update the flow set, which will start operating immediately.
- The **Cancel** button will discard any alteration and close the window.
- The **Apply** button sends all alterations to the firewall, and keeps the window open.

- Use the scroll bar on the right side to view flows that don't fit the window.
- Comments associated to selected flows will be displayed on the bottom part of the window.

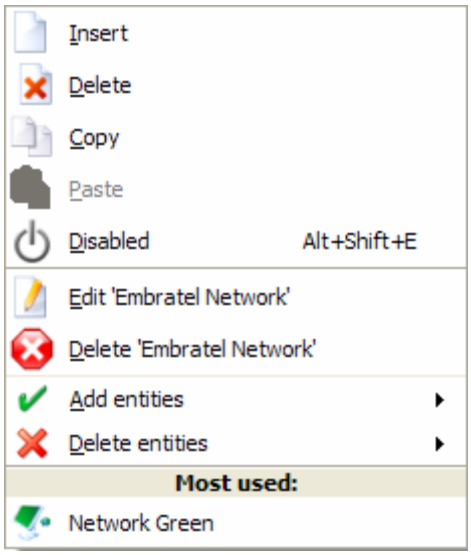
Hint: A rule position may be modified by drag and dropping it in a new position. Note that the cursor will change into a hand holding a stick.
To execute any operation on a specific flow, just right click on it. The menu below will show up. (This menu will come up any time the right mouse button is pressed, even if no flow is selected.) In this case, only the *Insert* and *Paste* options are enabled.



- **Insert:** adds a new flow to the list. If any flow is selected, the new one will be inserted in its position, pushing it down.
- **Delete:** This option erases the selected flow from the list.
- **Copy:** copies selected flow to a temporary area.
- **Paste:** copies the flow from the temporary area to the list. If a flow on the list is selected, the new one will be copied onto its position, pushing it down. Otherwise, it will be copied to the end of the list.
- **Disable/Enable:** disables or enables the selected flow.

Hint: All these options may be executed from the toolbar in the top part of the window. In this case, first select the flow with the left mouse button, and then click on the desired option in the toolbar.

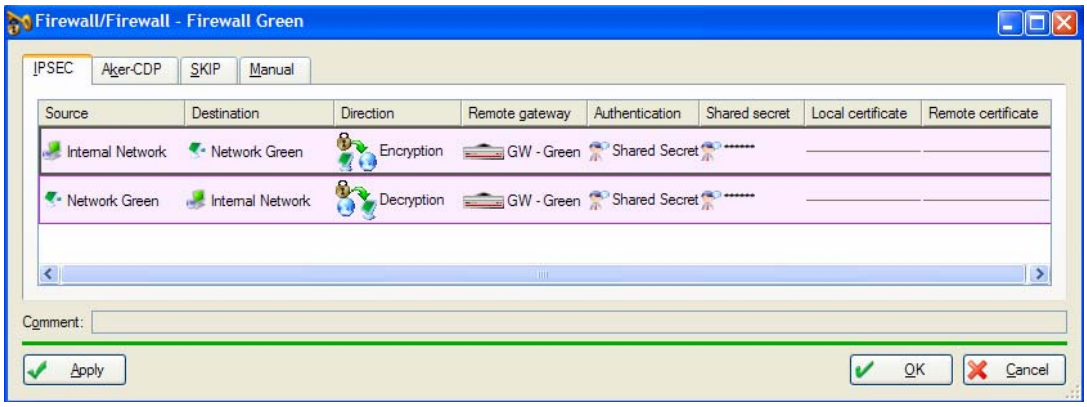
There are two ways to add or edit flows: drag entities to the desired flow, or right click over the desired field. In this case, the following options will be available: add, delete, or edit entities, as shown below:



Configuring IPSEC tunnels

IPSEC tunnels are used to create a VPN between two networks. The word ‘tunnel’ is applied to differentiate it from common VPNs. Because it effectively creates a virtual channel between involved firewalls, enabling, for example, that networks with invalid addresses communicate securely through the Internet.

To configure IPSEC channels, select the IPSEC tab in the Firewall-Firewall window. This will change the window and display the fields necessary for configuration.



Configuration fields:

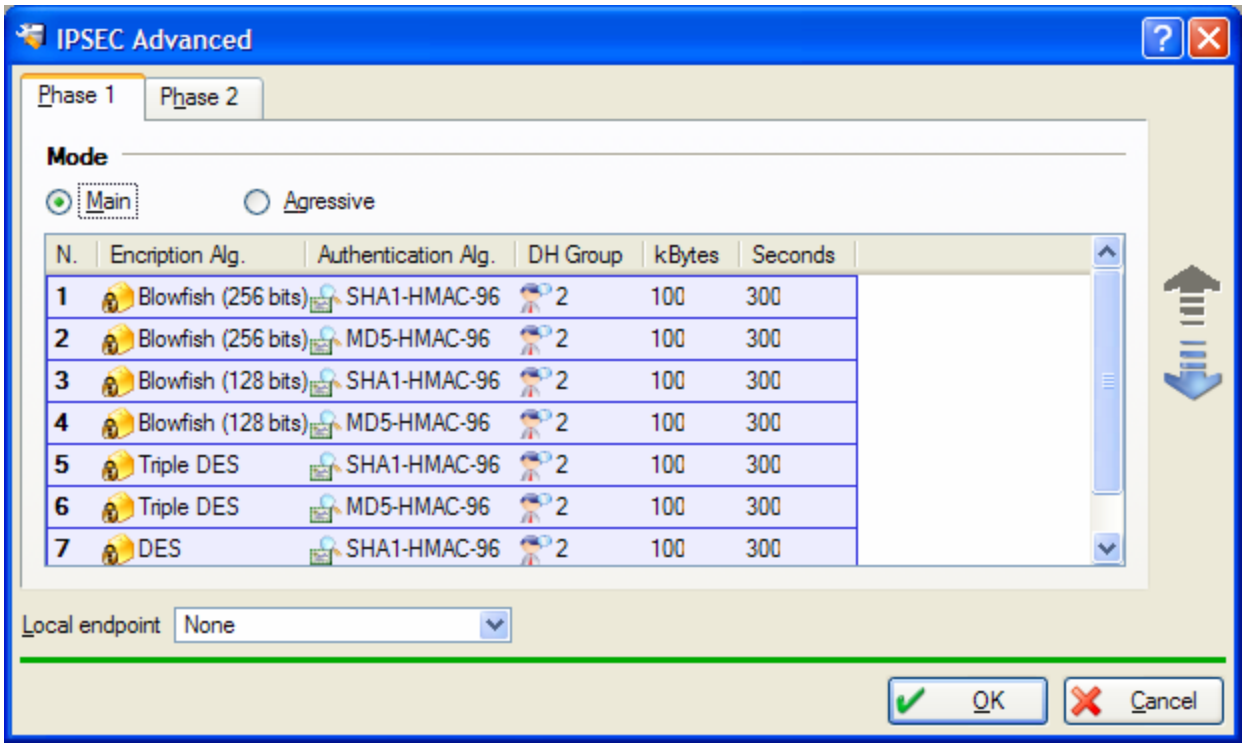
> **Remote Gateway:** Defines the entity of the host type that will be the remote gateway, i.e., the other end of the IPSEC tunnel.

Both firewalls in the tunnel need to be sure about the other's identity, to avoid falsification attacks. There are two selectable ways of accomplishing this:

> **Shared Secret:** a character string that works as a password, and must be equal in both sides of the tunnel..
>
> **Certificate:** Uses X.509 standard certificates with a system of public keys to identify firewalls. This is the same system used by Internet secure sites, for example.
>
> The following must be specified:
>
> - the **local** certificate to be presented to the other end of the tunnel (Remote Gateway), and
> - the identification information required by the **remote** firewall. This information will be an e-mail address, for certificates created with the USER-FQDN option and a host name (*Fully Qualified Domain Dame*), if the option is FQDN..

Advanced

> The Advanced window is used to define preferred encryption and authentication algorithms and the ones that are allowed by the firewall, during IKE key negotiation. The fields come pre-filled with default algorithms, which may be modified. More information on RFC 2401 to RFC 2412.
>
> The Advanced window, now, includes a choice of the local endpoint, for those cases of invalid intermediary network between the firewall and the router.

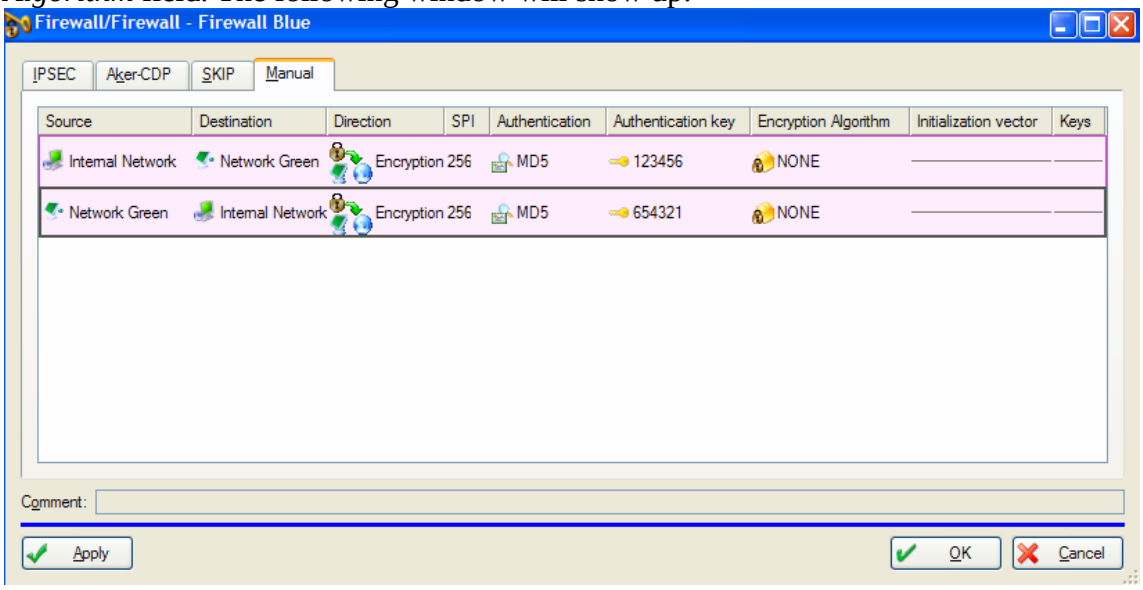


Using manual key exchange

To use the manual key exchange, select the *Manual* tab in the *Firewall/Firewall* window. The window will change and the fields needed for this type of configuration will be displayed.

Authentication only

To use flows with authentication only, select the option *None* in the *Encryption Algorithm* field. The following window will show up:



Source: Defines the entities which addresses will be compared to the source address of the IP packets that will make up the flow

Destination: Defines the entities which addresses will be compared to the destination address of the IP packets that will make up the flow.

Comment: Reserved to write down a comment about the flow. Very useful for documentation purposes.

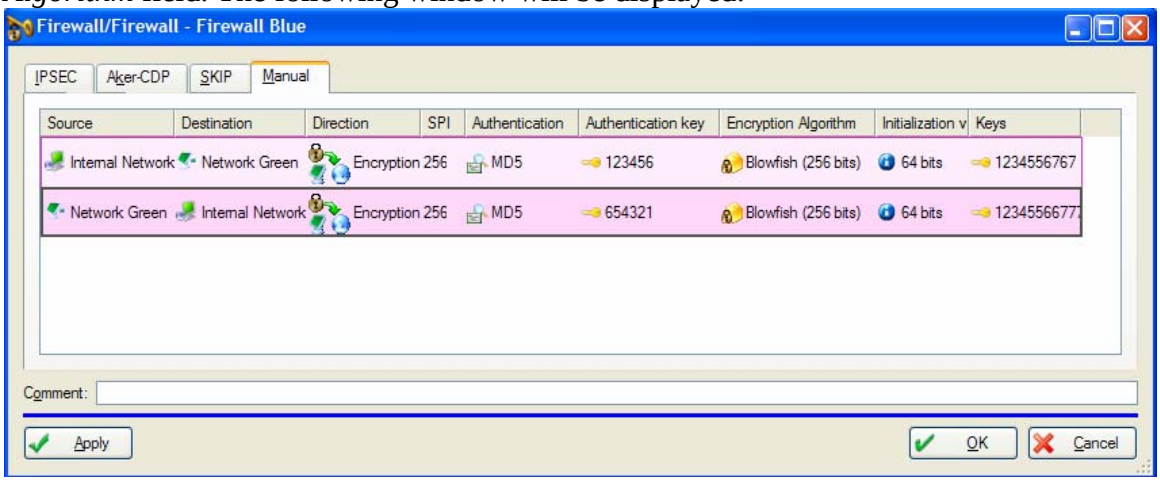
Direction: Defines the direction of the flow. There are only two possible options: either the packet is being *encrypted*, prior to a sending operation, or it is being *decrypted* following a receiving one. (For more details, see Planning the Installation.)

SPI (*Security Parameter Index*): This is a single number, used by the recipient, to identify a specific flow. It is mandatory and must be equal or higher than 256, and must be different for each flow going to the same recipient.

Authentication Key: Key used in the authentication process. This key must be typed in hexadecimal numbering system. Its maximum length varies according to the algorithm used: 32 digits for MD5, and 40 for SHA. It is recommended that you use the maximum number of characters allowed..

Authentication: Defines which authentication algorithm will be used. Possible values are: MD5 or SHA

Authentication with encryption using DES or Blowfish
To encrypt flows/channels with DES, Blowfish with 128-bit keys, or Blowfish with 256-bit keys encryption algorithms, select the corresponding option in the *Encryption Algorithm* field. The following window will be displayed:



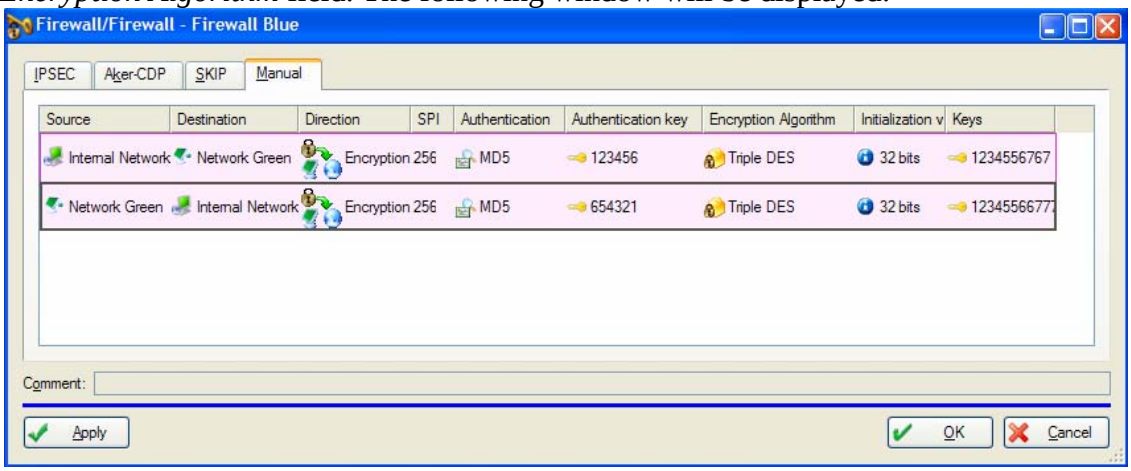
This window is exactly the same as the previous item one, except for two new fields:

Initialization Vector: It is the size, in bits, of the initialization vector to be used in the encryption algorithm. This vector is automatically generated by the system to each transmitted packet. The 64-bit option is recommended.

Keys: It is the key that will be applied to encrypt the packet. It must be a hexadecimal number, of 16, 32 and 64 digits, to be used respectively with DES, Blowfish (128 bits), and Blowfish (256 bits) algorithms.

Authentication with encryption using Triple DES (3DES)

To encrypt flows/channels with the Triple DES algorithm, select the *3DES* option in the *Encryption Algorithm* field. The following window will be displayed:



The window shown here is exactly the same as the one in the **Authentication with Encryption using DES** item. The only difference is in the **Key** field, that had just one insertion field and now has three:

Key 1: It is the key used in the first DES application. It must be a hexadecimal number made of 16 digits (mandatory).

Key 2: It is the key used in the second DES application. It must be a hexadecimal number made of 16 digits (mandatory).

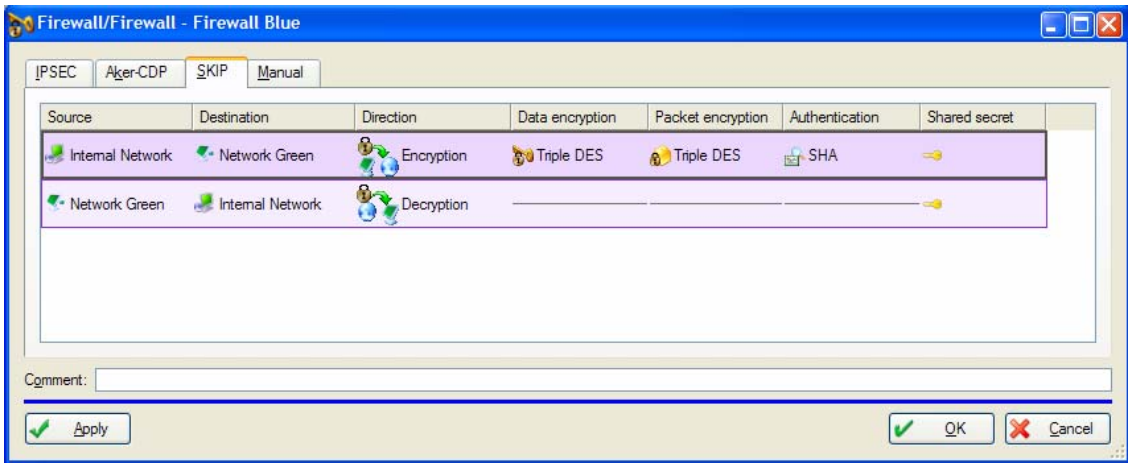
Key 3: It is the key used in the third DES application. It must be a hexadecimal number made of 16 digits (mandatory).

Using SKIP key exchange

Select the *SKIP* tab in the *Firewall-Firewall* window. The window will change and show the fields necessary to this configuration.

In the SKIP protocol, all encryption and authentication algorithms are configured only in the host that sends the packets. The host receiving the packets just needs to configure the source and destination entities, as well as the shared secret.

In both cases, the following window will show up: (receiving hosts unnecessary fields will be disabled)



Source: Defines the entities which addresses will be compared to the source address of the IP packets that will make up the flow.

Destination: Defines the entities which addresses will be compared to the destination address of the IP packets that will make up the flow.

Direction: Defines the direction of the flow. There are only two possible options: either the packet is being *encrypted*, prior to transmission, or it is being *decrypted*, following arrival (For more details, see Planning the Installation).

Data Encryption: It is the algorithm used to encrypt the session key, sent in the packet. The Blowfish (256 bits) is recommended in this case.

Packet encryption: It is the algorithm that will be used to encrypt the data in the packet. You can choose *None* (in case you want to use authentication only), *DES, 3DES, Blowfish (128 bits) or Blowfish (256 bits).*

Authentication: Defines the algorithm that will be used in the authentication. Possible values are: MD5 or SHA.

Shared Secret: It is the secret that will be used to generate master keys (For more information, see Planning the Installation). The secret must be the same in both firewalls, at both ends of the channel. It is mandatory to be a hexadecimal number of 64 digits.

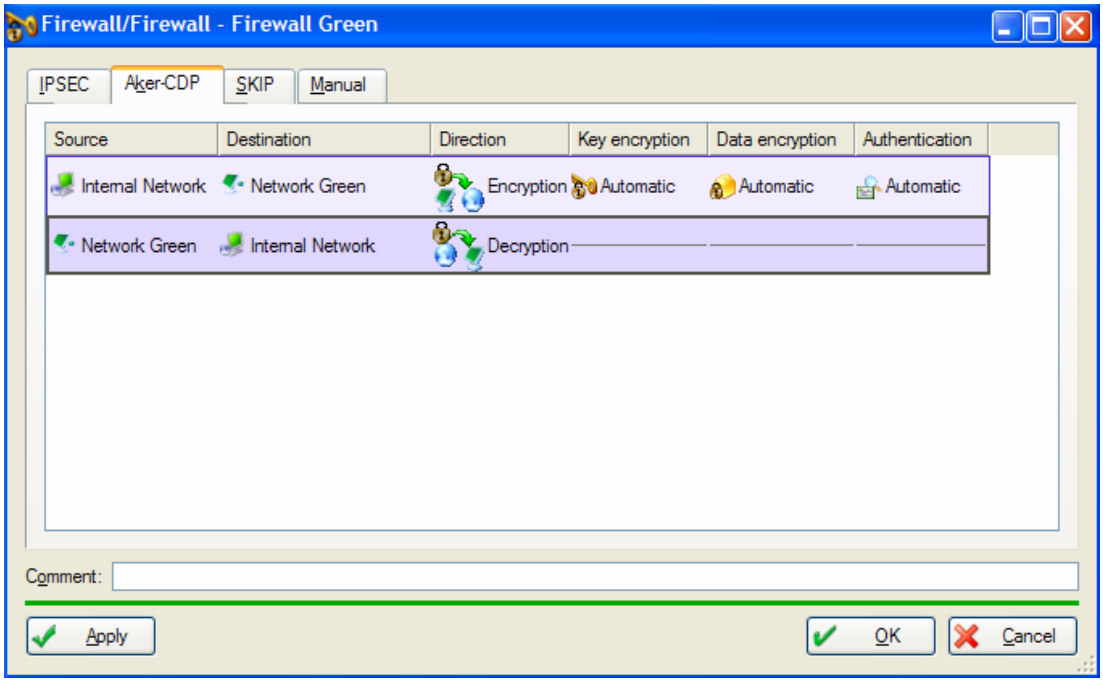
Besides those fields, there is an option to easy the configuration of equal secrets on both firewalls responsible for the sending and receiving of the encryption flow:

Load key from file: This option allows the *Shared Secret* field to be read from a file. This file must have only one line with the 64 digits of the secret.

When this option is selected, a window will show up asking for the name of the file where the secret will be retrieved from..

Using Aker-CDP key exchange

Select *Aker-CDP* tab from the *Firewall-Firewall* window. The window will change and bring up the fields needed for this type of configuration. The window will look like this:



The Aker-CDP key exchange parameters configuration is identical to that of SKIP, explained previously, except for two things: it is not necessary to specify a shared secret, and all algorithms can be set in the *Automatic* option. Thus, firewalls participating in the channel will negotiate the most secure algorithm, supported by both.

8-5 Using the command line interface

It is possible to perform all the above configurations using the command line interface. Each configuration is described in a separate section.

Loading IPSEC certificates

The command line interface for IPSEC certificate configuration is simple to use, and has the same capabilities as the graphical user interface.
Program Location: `/etc/firewall/fwipseccert`

Syntax:

```
     fwipseccert show [request | certificate]
     fwipseccert remove [request | certificate] <number>
     fwipseccert export <certificate> <file PKCS12> <password>
     fwipseccert request <local | remote> <1024 | 2048> <email>
<country>
                 <state> <city> <organization> <org unit> <domain>
[use_email]
                 [print]
     fwipseccert install <local | remote> <certificate>
     fwipseccert import <file PKCS12> <password>
```

Program help::

```
Aker Firewall - Version 5.0
fwipseccert – Creation and management of requests and x.509
certificates.
Usage: fwipseccert help
       fwipseccert show [request | certificate]
       fwipseccert remove [request | certificate] <number>
       fwipseccert request <local | remote> <1024 | 2048> <email>
<country>
                  <state> <city> <organization> <org unit> <domain>
[use_email]
                  [print]
       fwipseccert install <local | remote> <certificate>
       fwipseccert export <certificate> <file PKCS12> <password>
       fwipseccert import <file PKCS12> <password>

       help       = displays this message
       show       = displays a list of pending requests or installed
certificates
       remove     = removes a request or certificate according to its
number
       request    = creates a pair of public and private keys along
with a x.509
                    certificate request
       install    = installs a x.509 certificate, which pair of keys
must have been
                    previously created by the system, through the
request command
       export     = exports the certificate and its corresponding pair
of keys to a
                    file in the pkcs12 format
       import     = obtains a certificate and its pair of keys, from
the pkcs12 file,
```

```
                  and installs it as the local certificate (see
below)

For the request command, we have the following:
       local      = the local certificate is used in the firewall's
own identification;
                    it is possible to create several local
certificates, however, all
                    of them will use the same pair of keys, generated
the first time
                    a local request is generated
       remote     = remote certificates are used to identify other
network entities
       1024/2048  = the two possible key lengths
       use_email  = the certificate will have the <email> value as its
                    subject alternative name; the <domain> will be the
default value
       print      = after the request generation, it will be printed
on the screen

       email, country, state, city, organization, org unit, and domain
fields are
              used to identify the certificate user. The field
<country> must hold a
              maximum of two digits.  The <org unit> field stands for
organization
              unit, and refers to the organization department or
division to which
              the certificate user belongs.
```

Loading certificates

The command line interface of the encryption certificates configuration is simple to use and has the same capacities as the graphic user interface.

Program location: `/etc/firewall/fwcert`

Sintax:

```
fwcert help
fwcert show [local | ca | negociation | revogation]
fwcert load [local | ca] <file> [-f]
fwcert load revogation <file>
fwcert remove <code> [-f]
```

Program help:

```
Aker Firewall - Version 5.0
fwcert - Configures the secure channels certificates
Usage: fwcert help
       fwcert show [local | ca | negociation | revogation]
       fwcert load [local | ca] <file> [-f]
       fwcert load revogation <file>
       fwcert remove <code> [-f]

       help        = shows this message
       show        = shows the especified certificates
       load        = loads a new certificate in the firewall
```

```
       remove      = removes a certification authority certificate

For the show command:
       local       = shows the local negociation certificate
       ca          = shows the certification authority certifications
       negociation = shows the negociation certificates of other
firewalls
                     that have been received through the network
       revogation  = shows the revogation certificates that have been
loaded
                     locally or received through the network

For the load command:
       local       = loads the local negociation certificate (if there
is a
                     certificate already loaded it will be replaced)
       ca          = loads a certification authority certificate which
will be
                     used to validate the received negociation
certificates
       revogation  = loads a revogation certificate which will be used
to
                     invalidate a compromised negociation certificate
       file        = file name which the certificate will be loaded
from
       -f          = if present, will cause the program not to confirm
when
                     replacing a certificate

For the remove command:
       code        = code of the certification authority to be removed
       -f          = if present, will cause the program not to confirm
when
                     removing a certificate
```

Example 1: (loading the local certificate)

```
#/etc/firewall/fwcert load local /tmp/firewall.crt
Loading certificate...OK
```

Example 2: (viewing the certification authorities certificates)

```
#/etc/firewall/fwcert show ca
Name: Aker Security Solutions
Code: 1

Name: Authorized Certification Authority
Code: 2
```

Example 3: (loading a new certification authority certificate)

```
#/etc/firewall/fwcert load ca /tmp/new_ca.ca
Certificate added
```

Example 4: (removing a certification authority certificate, without confirmation)

```
#/etc/firewall/fwcert remove 2 -f
Certification authority removed
```

Configuring Firewall-Firewall channels

The use of the command line interface in the configuration of the secure channels creates a difficulty caused by the great number of arguments that should be passed through the command line.

This command line interface has the same capacities of the graphic interface except that it is not possible to assign comments for the secure channels, to specify more than one entity for the source or destination of the secure channels, nor to specify algorithms for the Aker-CDP key exchange through this interface (when using Aker-CDP, all algorithms will always be set to automatic) . It will neither be possible to configure algorithms to be used by IPSEC-IKE (Advanced window); they will always have default values.

Program location: `/etc/firewall/fwcripto`

Syntax:

```
fwcripto [show | help]
fwcripto remove <pos>
fwcripto add <pos> <source> <destination> <send | receive>
         ipsec <gateway> <<ss <secret> | cert <local> <remote>>
fwcripto add <pos> <source> <destination> <send | receive>
         manual <spi> [MD5 | SHA] <authentication key> NONE
fwcripto add <pos> <source> <destination> <send | receive>
         manual <spi> [MD5 | SHA] <authentication key>
         [DES | BFISH128 | BFISH256] <iv size> <encryption key>
fwcripto add <pos> <source> <destination> <send | receive>
         manual <spi> [MD5 | SHA] <authentication key>
         3DES <iv size> <key1> <key2> <key3>
fwcripto add <pos> <source> <destination> send
         skip [DES | 3DES | BFISH256] [MD5 | SHA]
         [NONE | DES | 3DES | BFISH128 | BFISH256] <secret>
fwcripto add <pos> <source> <destination> receive
         skip <secret>
fwcripto add <pos> <source> <destination> <send | receive> aker-cdp
```

Program help:

```
Aker Firewall - Version 5.0
fwcripto - Configures the secure channels table
Usage: fwcripto [show | help]
       fwcripto remove <pos>
       fwcripto add <pos> <source> <destination> <send | receive>
                 ipsec <gateway> <<ss <secret> | cert <local> <remote>>
       fwcripto add <pos> <source> <destination> <send | receive>
                 manual <spi> [MD5 | SHA] <authentication key> NONE
       fwcripto add <pos> <source> <destination> <send | receive>
                 manual <spi> [MD5 | SHA] <authentication key>
                 [DES | BFISH128 | BFISH256] <iv size> <encryption key>
       fwcripto add <pos> <source> <destination> <send | receive>
                 manual <spi> [MD5 | SHA] <authentication key>
                 3DES <iv size> <key1> <key2> <key3>
       fwcripto add <pos> <source> <destination> send
                 skip [DES | 3DES | BFISH256] [MD5 | SHA]
                 [NONE | DES | 3DES | BFISH128 | BFISH256] <secret>
```

```
       fwcripto add <pos> <source> <destination> receive
                skip <secret>
       fwcripto add <pos> <source> <destination> <send | receive>
aker-cdp

       show      = shows all entries in the secure channels table
       add       = adds a new entry to the table
       remove    = removes an existing entry from the table
       help      = shows this message

For the add command:
       pos       = position where the new entry will be added
                   (It can be a positive integer or the word END, to
add the
                    new entry at the end of the table)
       send      = this entry will be used when sending packets
       receive   = this entry will be used when receiving packets
       ipsec     = uses IPSEC key exchange protocol
       gateway   = the entity representing the remote end of the IPSEC
tunnel
       ss        = uses Shared Secret for authentication
       secret    = the string to be used  as the shared secret
       cert      = uses X.509 certificates for authentication
       local     = the domain name in the local certificate to present
       remote    = the domain name in the remote certificate to expect
       manual    = uses manual key exchange
       skip      = uses SKIP for automatic key exchange
       aker-cdp  = uses Aker-CDP for automatic key exchange
       spi       = Security Parameter Index
                   (It is an integer that identifies the security
association
                    between the source and destination hosts. This
number must
                    be greater than 255)
       MD5       = uses the MD5 as the authentication algorithm
       SHA       = uses the SHA-1 as the authentication algorithm
       DES       = uses the DES as the encryption algorithm
       3DES      = uses the triple DES as the encryption algorithm
       BFISH128  = uses the Blowfish with 128 bits keys as the
encryption
                   algorithm
       BFISH256  = uses the Blowfish with 256 bits keys as the
encryption
                   algorithm
       NONE      = doesn't use encryption, only authentication
                   (for the skip, the first selected algorithm
corresponds
                    to the key encryption algorithm and the second one
to the
                    packet encryption)
       iv_size   = initialization vector size, in bits, for the
encryption
                   algoritm. It value must be either 32 or 64.

       The authentication key, encryption key(s) and the skip secret
       must be typed as hexadecimal digits.
       For the 3DES, 3 keys separated by spaces must be typed

For the remove command:
       pos       = position to be removed from the table
```

```
                    (the position is the value shown on the left of
each entry
                     when the show command is invoked)
```

Example 1: (viewing the secure channels table)

```
#/etc/firewall/fwcripto show
Entry 01:
--------
Source       : NETWORK1
Destination  : AKER
Direction    : Receive  Keys: SKIP
Secret       :
5ab53faefc7c9845acbe223148065dabe3279819ab01c39654effacbef087022

Entry 02:
--------
Source       : AKER
Destination  : NETWORK1
Direction    : Send     Keys: SKIP            Algorithms: 3DES MD5 DES
Secret       :
5ab53faefc7c9845acbe223148065dabe3279819ab01c39654effacbef087021

Entry 03:
--------
Source       : Internal Network
Destination  : External Network 1
Direction    : Send     Keys: Manual          Algorithms: SHA DES
SPI          : 999      Authentication: 0c234da5677ab5
Encryption   : 9a34ac7890ab67ef
IV: 64 bits

Entry 04:
--------
Source       : External Network 1
Destination  : Internal Network
Direction    : Receive  Keys: Manual           Algorithms: SHA DES
SPI          : 999      Authentication: 0c234da5677ab5
Encryption   : 9a3456ac90ab67ef
IV: 64 bits

Entry 05:
--------
Source       : Aker Network 1
Destination  : Aker Network 2
Direction    : Receive  Keys: Aker-CDP         Algorithms: Auto Auto
Auto

Entry 06:
--------
Source       : Aker Network 2
Destination  : Aker Network 1
Direction    : Send    Keys: Aker-CDP          Algorithms: Auto Auto
Auto
```

Example 2: (removing the third entry)

```
#/etc/firewall/fwcripto remove 3
Entry 3 removed
```

Example 3: (adding an entry with manual key exchange and DES encryption at the end of the table)

```
#/etc/firewall/fwcripto add end NETWORK1 NETWORK2 send manual 7436 MD5
c234da5677ab5 DES 64 4234ad70cba32c6ef
Entry added at position 7
```

Example 4: (adding an entry with SKIP key exchange in the beginning of the table)

```
#/etc/firewall/fwcripto add 1 NETWORK1 NETWORK2 send skip 3DES SHA DES
5ab53faefc7c9845acbe223148065dabe3279819ab01c39654effacbef087022
Entry added at position 1
```

Example 5: (adding an entry with Aker-CDP key exchange at position 2 of the table)

```
#/etc/firewall/fwcripto add 2 "Aker Network 3" "Aker Network 1"
receive aker-cdp
Entry added at position 2
```

9-0 Configuring Client-Firewall Secure Channels

We will show here how to configure the Aker Encryption Client and the firewall, to establish secure channels between client machines and a Firewall Aker.

9-1 Planning the installation

What is a secure Client-Firewall channel?

As detailed in the previous chapter, a secure client-firewall channel is established directly between a client host and a Firewall Aker. This is possible through the installation of the Aker Encryption Client in client hosts.
A Client-Firewall encryption channel uses the same encryption, authentication, and key exchange technologies as secure firewall-firewall channels do, with the difference that everything is automatically negotiated by the communicating entities. Manually, the administrator can only disable certain algorithms, to ensure they won't be used.
Another fundamental difference between secure firewall-firewall and client-firewall channels regards their implementation in the Firewall Aker. While firewall-firewall is always done in IP packets level, where each packet is individually encrypted, with client-firewall it is done in the data flow level, where only the information the packet is carrying is encrypted (and not other IP packet data).

Requirements for creating Client-Firewall secure channels

To establish secure channels between clients and a firewall, the following conditions must be satisfied:

1. The Aker Encryption Client must be installed in every host that will establish secure channels with the firewall.
2. The firewall local certificate must be loaded (for more information on certificates, see chapter Creating Secure Channels).
3. The firewall configuration must allow that encryption clients establish secure sessions.
4. The clients must be configured to establish encryption channels with the networks protected by the firewall.

The Encryption Client will use port 2473/UDP (Aker-CDP protocol) to establish a secure channel with the firewall. No firewall or any other control mechanism should exist between the client and the firewall, blocking packets passage to this port; otherwise it will not be possible to establish secure channels.

The Encryption Client only encrypts data sent through the Winsock. It does not encrypt any type of NetBIOS communication.

Defining a client-firewall secure channel

A client-firewall secure channel configuration is much simpler than that of a firewall-firewall channel. It is only necessary to define, in the firewall, which hosts will establish client secure channels, and whether user authentication will be performed. All other procedures are done automatically, when the client initiates the secure channel negotiation.

9-2 Configuring the Firewall using the graphic user interface

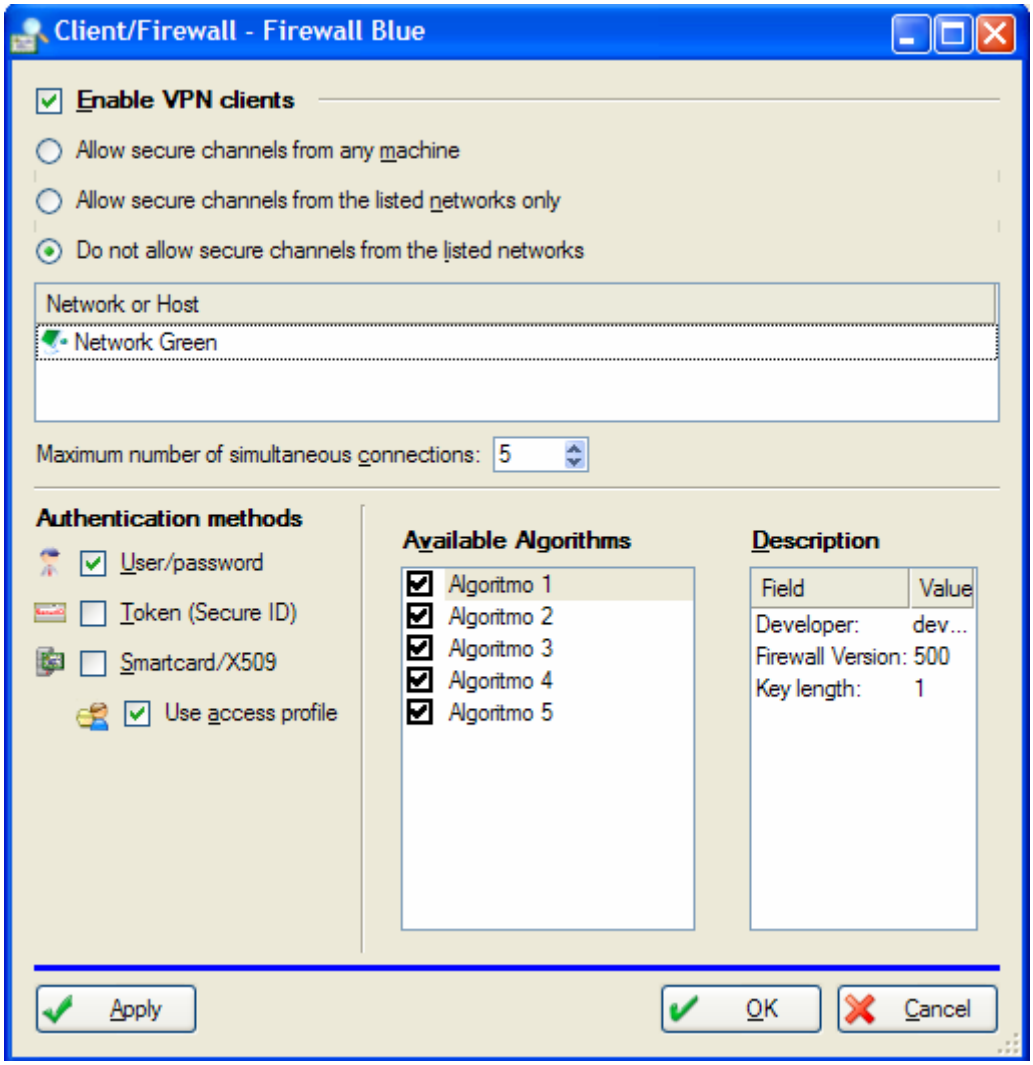
Client-Firewall channel configuration is very simple, once both the client and the firewall do most procedures automatically. The administrator just needs to define which clients can establish a secure channel, and whether user authentication will be performed.

All these configurations are set in the Client Secure Channels Window. To access it, do the following:

- Click on *Cryptography* menu in the main window
- Choose *Client/Firewall* item

A configuração dos canais cliente-firewall é bastante simples, uma vez que todo o procedimento é feito automaticamente pelo cliente e pelo firewall. Ao administrador cabe apenas definir quais clientes podem estabelecer um canal seguro e se será realizada autenticação de usuários.

The Client-Firewall Encryption Window



The client channel configuration parameters are made of the following fields:

Enable VPN clients: This option must be checked to activate firewall support for secure clients channels. When this support is disabled, the configuration is kept stored, but may not be altered.
Allow secure channels from any machine: allows any Internet machine to establish a secure channel with the Firewall.

Allow secure channels from the listed networks only: This option requires that any entity wanting to establish a secure channel must be included in the list below.

Do not allow secure channels from the listed networks: This option is the opposite of the previous one. It requires that entities wishing to establish the secure channel should not be included in the list just below it.

Maximum number of simultaneous connections: This parameter configures the maximum number of client secure channels that may be active at the same time. It may

range between 0 and the maximum number of acquired Encryption Client licenses. If is set to 0, no user will be allowed to establish secure channels.

Authentication Methods

The available options, which may be independently checked, are:

- User/password

The user must be authenticated through a combination of username and password. These data are redirected to one or more authentication servers, to be validated. This is the least secure option, although it does not require any additional hardware.

- Token (Secure ID)

User authentication is done through a combination of username, PIN and a Token Secure ID code, which is modified at every minute. These data are redirected to the authenticator Token, registered in the firewall, to be validated. This option is much more secure than the previous one, although it requires that each user have a Token.

- Smartcard/X509

User is authenticated through X509 certificates, stored in smart cards, and issued by one of the Certification Authorities registered in the firewall. This is the most secure authentication method of the three, however it requires that each user have a smart card, as well as that each computer, used with the Encryption Client, have a smart card reader.

If any option is checked in *Authentication Methods*, it is possible to determine whether a user, validated in the Encryption Client, will have or not an associated access profile. If the option **Use Access Profile** is checked, after being validated in the Encryption Client, the user will have the same rights it would have if it had also been authenticated through the authentication client. If this option is not checked, however, the user will establish a secure channel without an associated access profile (as in Firewall Aker versions 3.52 and prior).

 It is possible to use the Aker Authentication Client together with the Encryption Client. This way, if the authentication method being used is username/password, then the user will not have to be authenticated again to the firewall. For more information about authentication client refer to chapter Aker authentication client.

Adding and removing entities from the entities list:

To add an entity to the entity list, do the following:

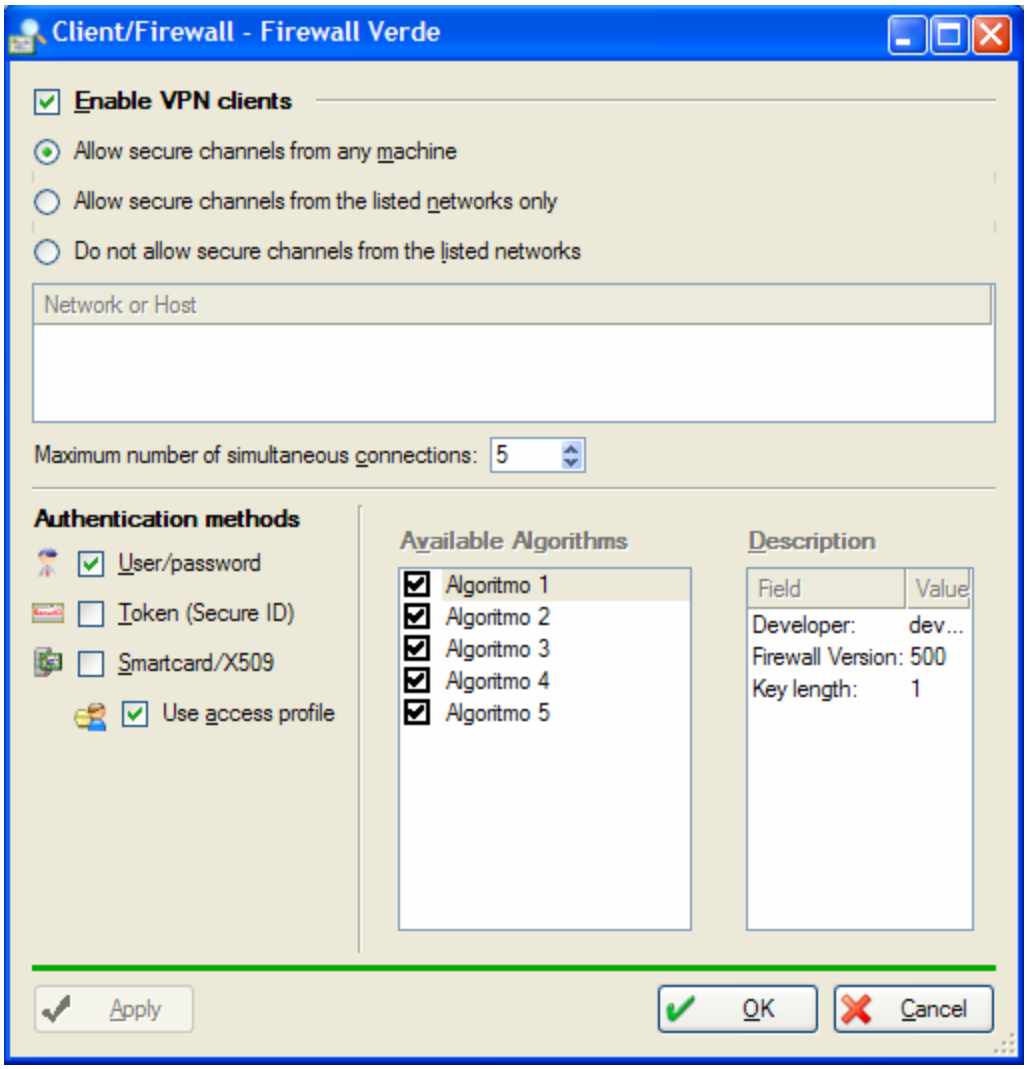
1. Right click on the field where the entity is to be inserted, or select and drag the entity from the entities field, in the bottom left, to the desired field.

To remove an entity from the entities list, do the following:

1. Right click on the field from where the entity will be removed

Enabling and disabling encryption algorithms

The administrator can disable encryption algorithms to block their usage in client/firewall secure channels. This is done by removing check marks from the corresponding algorithm box, in the **Available Algorithms** section, located in the bottom part of the Client/Firewall Encryption Window.



9-3 Configuring the Firewall using the command line interface

The command line interface for Client-Firewall secure channels configuration is of simple use and has the same capacities of the graphic user interface.

Program location: `/etc/firewall/fwclient`

Syntax:

```
fwclient [activate | deactivate | show | help]
fwclient [add | remove] <name>
fwclient [enable | disable] <algorithm>
fwclient max_clients <value>
fwclient authentication none
fwclient authentication [password | card | token] <yes | no>
fwclient allow [all | listed | others]
fwclient profile <yes | no>
```

Program help:

```
fwclient - Configures the client secure channels parameters
Usage: fwclient [activate | deactivate | show | help]
       fwclient [add | remove] <name>
       fwclient [enable | disable] <algorithm>
       fwclient max_clients <value>
       fwclient authentication none
       fwclient authentication [password | card | token] <yes | no>
       fwclient allow [all | listed | others]
       fwclient profile <yes | no>

       activate       = activates support to client secure channels
       deactivate     = deactivates support to client secure channels
       show           = shows the active configuration
       add            = adds a new entity to the list of entities
       remove         = removes a entity from the list of entities
       enable         = enables the use of the specified algorithm
       disable        = disables the use of the specified algorithm
       max_clients    = sets the maximum number of simultaneous
clients
       authentication = deactivates or selects the types of user
authentication
                        that will be demanded to client hosts to
establish
                        secure channels
       allow          = indicates which entities will be allowed to
establish
                        secure channels with the firewall
       profile        = Enables the use of access profiles for users
validated
                        using the encryption client
       help           = shows this message

For the add / remove commands:
       name         = name of the entity to be added to or removed
from the
                      entities list

For the max_clients command:
```

```
       value        = maximum number of simultaneous clients (must be
an
                      integer number between 0 and 1000)

For the authentication command:
       none           = does not demand user authentication
       password       = accepts or not user/password authentication
       card           = accepts or not smart card authentication
       token          = accepts or not token based authentication

For the allow command:
       all          = allows any host in the Internet to establish a
secure
                      channel with the firewall
      listed        = allows only the hosts, networks and sets listed
to
                      establish a secure channel with the firewall
      others        = allows all hosts in the Internet, except the
hosts,
                      networks ou sets listed to establish a secure
channel
                      with the firewall
```

Example 1: (viewing the configuration)

```
#/etc/firewall/fwclient show
Configuration parameters:
---------------------------------
Support to client secure channels: activated
Maximum number of simultaneos channels: 25
Uses access profiles: yes
User authentication: none

DO NOT allow secure channels only from the entities below:
-----------------------------------------------------------
hacker1                                          (Host)
test network                                     (Network)

Loaded algorithms:
------------------
DES                                              (enabled)
3-DES                                            (enabled)
Blowfish-128                                     (enabled)
Blowfish-256                                     (enabled)
```

Example 2: (activating the user authentication by username/password and viewing the new configuration)

```
#/etc/firewall/fwclient authentication password yes
#/etc/firewall/fwclient show
Configuration parameters:
---------------------------------
Support to client secure channels: activated
Maximum number of simultaneos channels: 25
Uses access profiles: yes
User authentication:
   User/password: yes
   Smart card   : no
   Token        : no
```

```
DO NOT allow secure channels only from the entities below:
-----------------------------------------------------------
hacker1                                          (Host)
test network                                     (Network)

Loaded algorithms:
------------------
DES                                              (enabled)
3-DES                                            (enabled)
Blowfish-128                                     (enabled)
Blowfish-256                                     (enabled)
```

Example 3: (allowing the establishment of secure channels from any host and viewing the configuration)

```
#/etc/firewall/fwclient allow all
#/etc/firewall/fwclient show
Configuration parameters:
---------------------------------
Support to client secure channels: activated
Maximum number of simultaneos channels: 25
Uses access profiles: yes
User authentication:
   User/password: yes
   Smart card   : no
   Token        : no

Allows secure channels from any host in the Internet

Loaded algorithms:
------------------
DES                                              (enabled)
3-DES                                            (enabled)
Blowfish-128                                     (enabled)
Blowfish-256                                     (enabled)
```

Example 4: (disabling the DES algorithm and viewing the configuration)

```
#/etc/firewall/fwclient disable des
#/etc/firewall/fwclient show
Configuration parameters:
---------------------------------
Support to client secure channels: activated
Maximum number of simultaneos channels: 25
Uses access profiles: yes
User authentication:
   User/password: yes
   Smart card   : no
   Token        : no

Allows secure channels from any host in the Internet

Loaded algorithms:
------------------
DES                                              (disabled)
3-DES                                            (enabled)
Blowfish-128                                     (enabled)
Blowfish-256                                     (enabled)
```

9-4 Installing Aker Encryption Client

Aker Encryption Client runs on Windows 95/98/NT/2000 platforms. Its installation is so simple that it's not even necessary to restart the machine in which it's being installed.

To install the Encryption Client, load the CD-ROM and select **Install Encryption Client**, inside the **Firewall** menu. If the autorun option is disabled, then the following steps will be necessary:

1. Click on the **Start** menu
2. Select **Run**
3. Type **`D:\en\firewall\criptoc\setup`**. (If your CD-ROM drive uses a letter other than D, replace it accordingly.)

The installation window will be displayed. To proceed, follow the instructions on the screen.

When the installation is completed, a new group called **Aker Firewall** will have been created under the **Start** menu. Inside this group, there will be a subgroup called **Encryption Client**. And inside this one, there will be an **Encryption Client** option, which must be selected, in order to run the program.

Installing the client through scripts

To make it easier to install Aker Encryption Client in a large number of hosts, it is possible to perform an automatic and non-interactive installation. This way, it is possible to write a logon script, for example, that installs the client if it is not installed already.

The automatic installation is invoked through another program, called **`Setupbat`**, located in the same directory of the installation program, described above. It receives the installation options through command line and the following options are available:

`-a`	Performs an automatic installation
`-i`	Adds the client to the **Start** menu
`-d` ***`directory`***	Especifies the installation directory
`-f`	Installs the client even if a previous installation is detected
`-c`	Starts the client after installing it

If the **`-d directory`** option is not specified, the client will be installed in **`C:\Program Files\aker\aker_crypt`**

Distributing a default configuration in client installation

In addition to automatically installing the Client, it is also possible to distribute a default configuration, which will be used in both the automatic and the interactive installation. Consequently, a firewall administrator can leave the entire Aker Encryption Client configuration ready, so that the user won't need to perform any type of configuration.

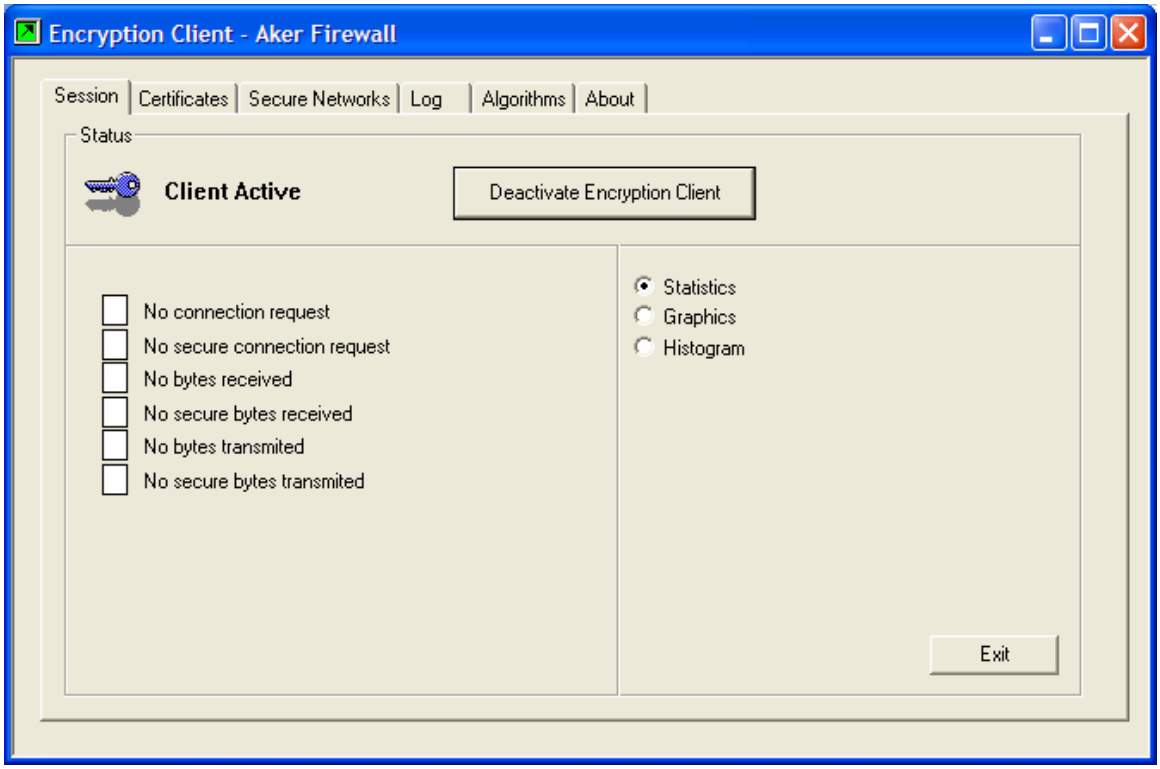
To install the Client with a default configuration, just configure it in a machine, in the desired way. Afterwards, copy specific files to the directory where the default versions will be installed. The following files can be copied:

nets.cla	Configuration of secure networks and the option of using Aker Authentication Client for logon
algorithms.cla	List of enabled algorithms
certs.cla	Certification authorities and revogation certificates

9-5 Configuring the Encryption Client

While the Encryption Client is running, an icon is displayed in the taskbar next to the clock. To configure the Client, click once on this icon. The Client Configuration and Monitoring Window will show up. This window has six tabs, each one responsible for a part of the configuration:

Session

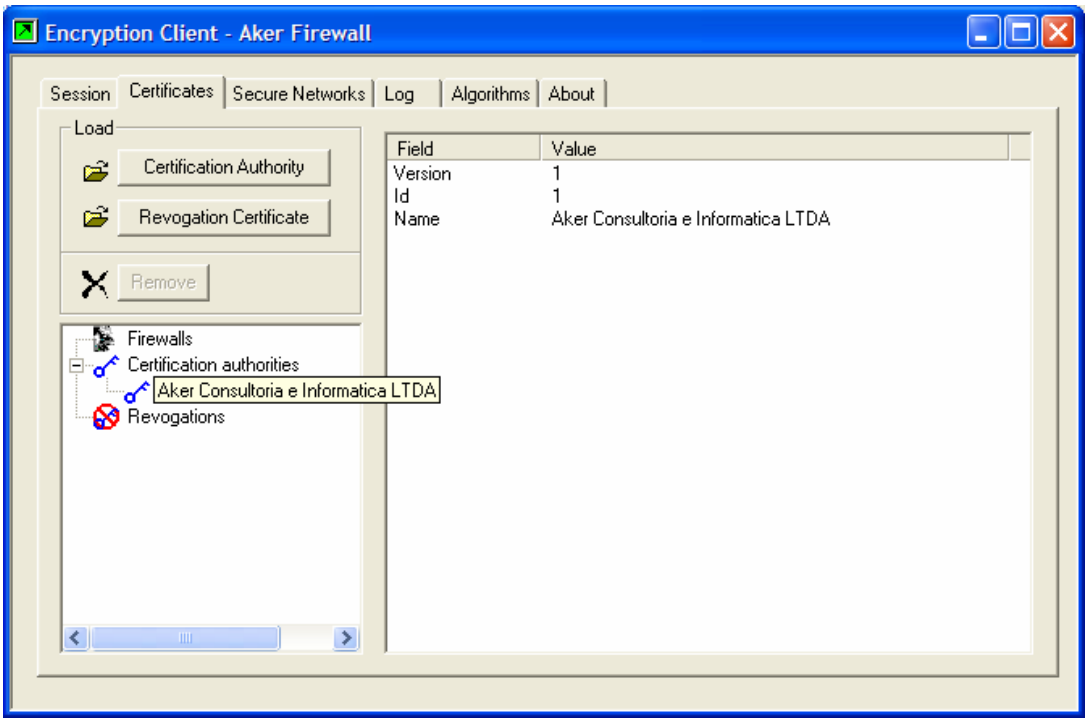


The Session tab shows a summary of the Client activity. It indicates whether the Client is active, and the amount of bytes and connections (secure and insecure) that have passed through it in the current session.

Secure connections are the ones being encrypted, and the insecure are unencrypted.

There is a button, in the top part of the tab, that activates or deactivates the Client. If the Client is deactivated, no connection will be encrypted..

Certificates



This tab has its functioning equal to the firewall certificates window, with the only difference that there is no local certificate.

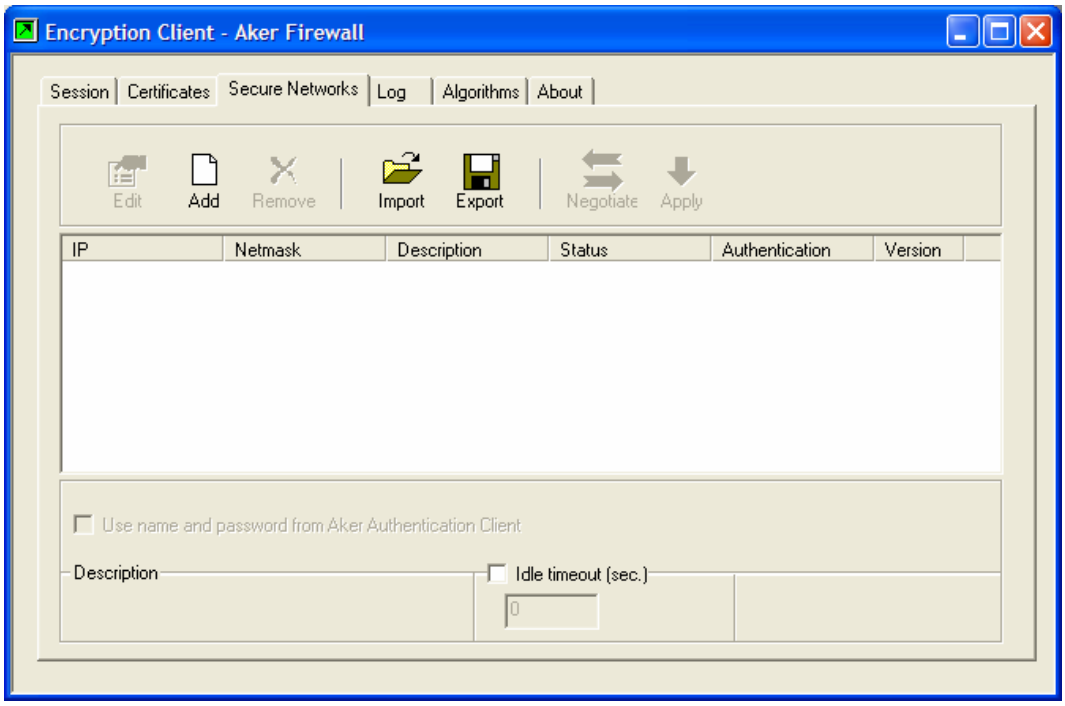
It has two lists: the left list shows negotiation, revocation, and Certification Authorities certificates. The right list shows the fields of a selected certificate. If no certificate is selected, this list will remain blank.

Certificates fields displayed on the right are for information purposes only. None of those values may be altered.

To load a new certificate, do the following:

1. In the Load group, click on the **Certification Authority** or the **Revocation Certificate** button, to select the certificate type to be loaded.
2. Specify the name and location of the file to be loaded, in the window that will show up. Then click **Open**.

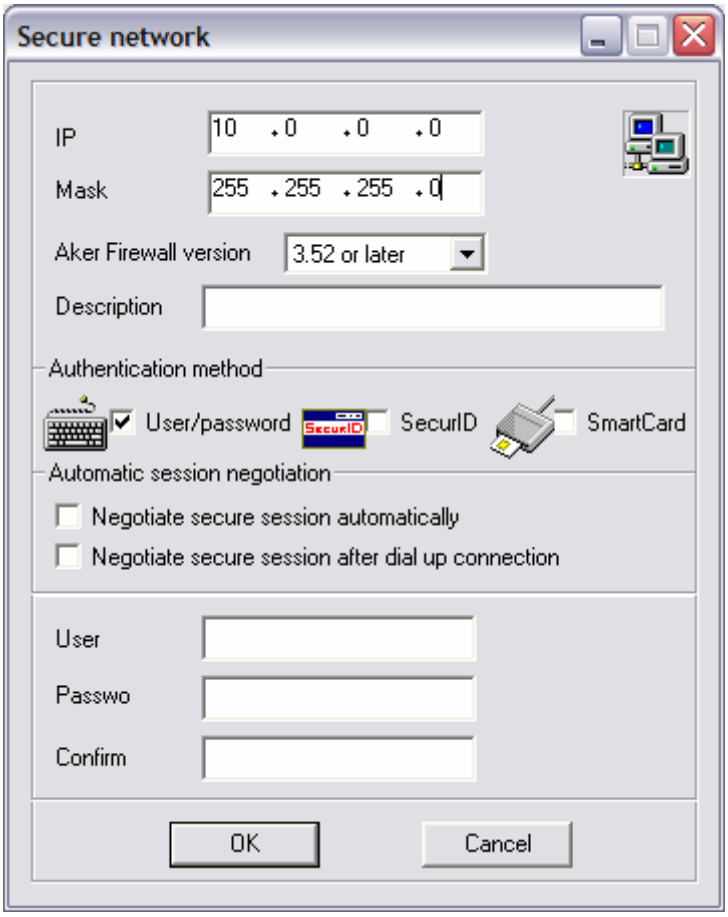
Secure Networks



This is the main Client configuration tab. It shows a list of all networks to which the communication will be encrypted. Each network has a status column indicating if it's active or not.

To add a new entry to the list, just click on the **Add** button, in the toolbar. To delete or edit a secure network, select it, and click on the desired option in the toolbar.

Selecting *Add* or *Edit* will display the window below:



IP: It is the network IP address to which the communication will be encrypted.

Netmask: It is the netmask of the network to which the communication will be encrypted.

Description: It is a free text field, used only for documentation purposes.

It is possible to export the current configuration to a file and import it lately in the same or in another host. For these purposes, there are the **Import** and **Export** buttons, located in the toolbar. The **Export** button saves the current secure networks list in a file and the **Import** button loads the networks list from a file and adds them to the present list (the new entries will be added in the end of the present list).

The **Negotiate** button allows the immediate negotiation of a secure channel to the selected network. If the session to the selected network is already established or no entry is selected, then this button will be disabled.

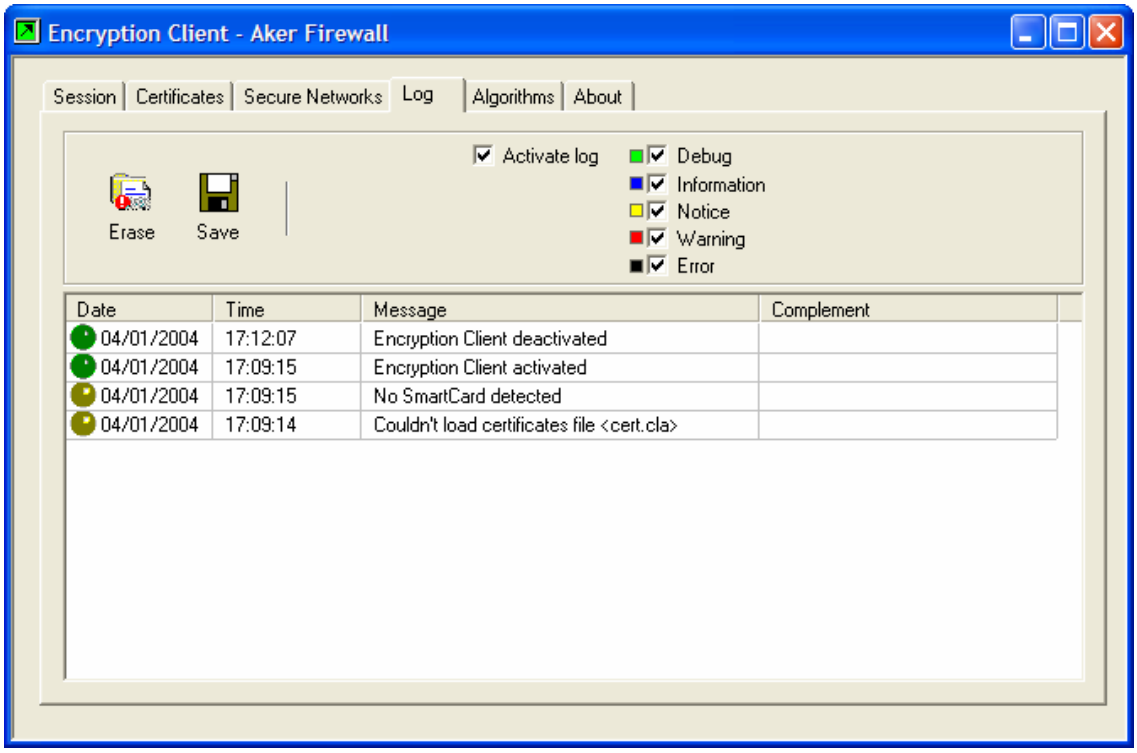
The **Apply** button makes the recently made modifications permanent. When it is clicked, all active sessions will be finished.

The **Use name and password from Aker Authentication Client** option, if checked, causes the encryption client to use the username and password used in the network logon to establish secure sessions, if they demand user authentication. If this option is not checked and the firewall is configured to demand user authentication, a window

asking for an username and a password will be shown every time a new encryption session is established.

If the Aker Authentication Client is not active, the **Use name and password from Aker Authentication Client** option will be disabled.

Log



This is a very useful tab to accompany the Encryption Client operation. It has a list with several messages in chronological order. A colored icon, next to each message, symbolizes its priority. The colors mean the following:

Green	Debug
Blue	Information
Yellow	Notice
Red	Warning
Black	Error

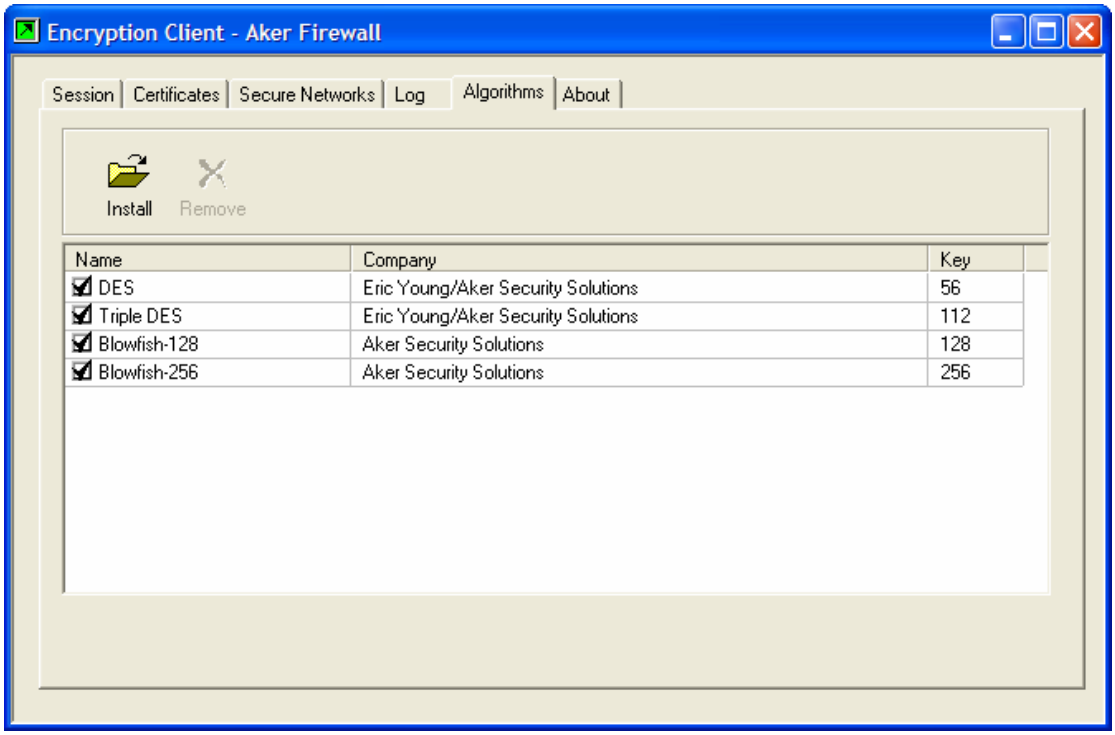
The **Erase** button, located in the toolbar allows the erasing of all existing log entries.

The **Save** button, located in the toolbar, allows to save the log in a text file. When it is clicked, a window asking for the filename to save the log will be displayed.

The **Activate Log** option, if unchecked, will produce no more log messages from the encryption client.

The Aker Encryption Client log is stored only during client execution time. If it is closed, all log information will be discarded.

Algorithms



The Algorithms tab allows for disabling algorithms, blocking their utilization for the establishment of secure channels. In this tab, it is also possible to load new algorithms, and to remove previously loaded ones. It has a list of each algorithm, its name, company or person who implemented it, and its key length in bits.

To disable an algorithm, click on the box to the left of its name. A new click will enable it again.

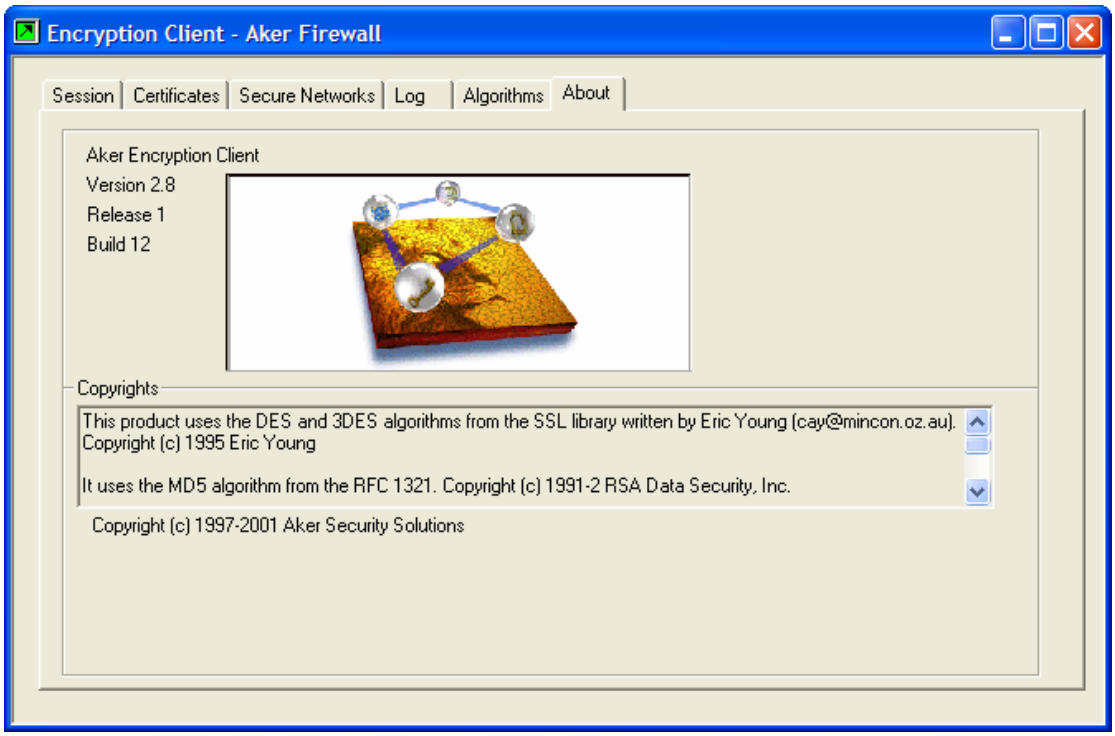
To add a new algorithm to the Encryption Client, click on the **Install** button, located in the toolbar. A window asking for the .DLL filename, supplied by the algorithm developer, will be shown.

To remove an algorithm, click on its name, then click on the **Erase** button, located in the toolbar. This procedure will remove the .DLL file installed as shown in the previous example.

To perform any algorithm operation, the Encryption Client must be inactive.

It is not possible to remove the default encryption client algorithms. It is only possible to disable them.

About



This tab supplies useful information about the Aker Encryption Client, such as its version and release.

10-0 Integration of the Firewall modules

In this chapter, the relationship of the three large Aker Firewall modules will be shown: the packet filter, the network address translator and the encryption and authentication module. The path through which the packets gofrom the moment they are received by the Firewall until the moment they are accepted or rejected will also be shown.

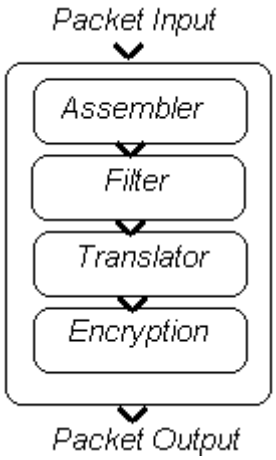
10-1 The flow of packets in Aker Firewall

In the previous chapters of this manual, the three large Aker Firewall modules were shown separately and all the details pertinent to the configuration of each one. Now, it will be shown how a packet goes through them and which alterations it can undergo in each one of them.

Basically, there are two different flows: one for packets that are generated in the internal network and have an external host as destination (inside-outside flow) or packets that are generated in the external network and have a host on the internal network as destination (outside-inside flow).

The inside-outside flow

When any packet from the internal network reaches the firewall, it goes through the modules in the following order: assembler module, packet filter, network address translator and encryption module.



- **The assembler module**

The assembler module is responsible for storing all fragments of the received IP packets until they can be reassembled and converted into a complete packet. This packet will be then passed to the other modules.

- **The packet filter**

The packet filter has the basic function of validating a packet in accordance with the rules defined by the administrator, and its stateful table, and deciding whether it should be allowed to pass through the firewall. If it decides that the packet can pass, it will be passed to the other modules, otherwise, it will be discarded and the flow will end.

- **The network address translator**

The network address translator receives an authorized packet and verifies, according to its configuration, if it should have the source address translated. In case of positive answer, it translates it, otherwise, the packet suffer no other alterations.

Afterwards, the packet will be passed to the encryption module.

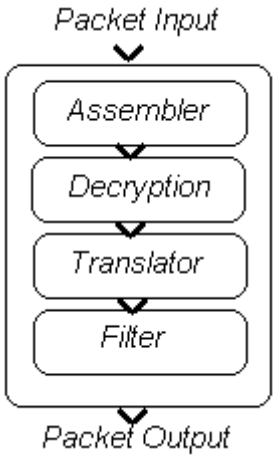
- **The encryption module**

The encryption module receives a valid packet, with translated addresses, and decides, based on its configuration, if this packet should be encrypted or authenticated before being sent to the destination. In case of positive answer, the packet will be authenticated, encrypted, and some specific headers will be added to it.

Afterwards, the packet will be sent through the network.

The outside-inside flow

When any packet coming from the external network, in direction towards the internal network, reaches the firewall, it goes through the modules in the following order: assembler module, decryption module, network address translator and packet filter.



- **The assembler module**

The assembler module is responsible for storing all fragments of the received IP packets until they can be reassembled and converted into a complete packet. This packet will be then passed to the other modules.

- **The decryption module**

The decryption module removes the headers added by the encryption module, verifying the packet authentication signature and decrypting it. In case either the authentication or the decryption presents an error, the packet will be discarded.

The other function of this module is to make sure that all the packets that arrive from a network to which there is a secure channel come encrypted. In case a packet comes from a network to which there is an encryption or authentication channel and this packet is not either authenticated or encrypted, it will be discarded.

If the packet has been validated successfully, it will be passed to the network address translator.

- **The network address translator**

The network address translator receives a packet and checks if the destination address of this packet is one of the virtual IP addresses. In case of positive answer, this address is translated to a real address.

Afterwards, the packet will be passed to the packet filter.

- **The packet filter**

The packet filter is the last module of the outside-inside flow. It has the basic function of validating the received packet according to the rules defined by the administrator, and its stateful table, and deciding whether it should be allowed to pass through the firewall. If it decides that the packet can pass, it will be sent to the destination host, otherwise, it will be discarded.

10-2 Integration of the filter and the network address translation

When configuring filtering rules to be used with hosts whose addresses will be translated, the following doubt arises: should the real hosts addresses be used or the virtual ones ?

This question can be easily answered while analyzing the packet flow:

- In the inside-outside flow, the packets go through the filter first and then have their addresses translated (if it is the case), that means, the filter receives the real addresses from the hosts.
- In the outside-inside flow, the packets go through the network addresses translator first, which translates the destination addresses of the virtual IP addresses into the real ones. After this, the packets are sent to the packet filter, this means, the packet filter receives the packets with the real addresses again.

In both cases, the filter is not aware of the existence of the virtual addresses, what leads us to the following statement:

 When filtering rules are created, the network addresses translation must be ignored. The rules must be configured as if the source and destination hosts were communicating directly, without using any kind of addresses translation.

10-3 Integration of the filter with the network address translation and the encryption

In the previous section, we have shown how to configure the filtering rules to hosts whose addresses would be translated. The conclusion was that you should work only with the real addresses, ignoring the address translation. Now, one more question arises: when secure channels are configured to hosts that will go through the network address translation, should the real addresses of these hosts be used or the virtual ones ?

In order to answer this question, the packet flow should be analyzed again:

- In the inside-outside flow, the packets go through the filter first, have their addresses translated (if it is the case) and, at last, they are passed to the encryption module. Due to this fact, the encryption module receives the packets as if they were originated in the virtual addresses.
- In the outside-inside flow, the packets go through the decryption module and are decrypted (if it is the case). Then, they are sent to the network addresses translator, which translates the destination addresses of the virtual IP addresses into real addresses, and, at last, they are sent to the packet filter. The decryption module receives the packets before they have had their addresses translated and, consequently, with the virtual addresses.

In both cases, the encryption and decryption modules receive the packets as if they had their origin or destination in the virtual IP addresses, what leads us to the following statement:

 When secure channels are created, you should pay attention to the network addresses translation. The source and destination addresses must be set as if the channel had the virtual IP addresses as its origin or destination.

11-0 Configuring the Security

We will show here how to configure attack protection in the Aker Firewall security module.

11-1 Protection against SYN Flood

What is a SYN Flood attack?

SYN Flood is one of the most popular denial of service attacks. The purpose of these attacks is to deny the functioning of a host or a specific service. In case of the SYN flood, it is possible to make any TCP based service unusable.

In order to understand this attack, it is first necessary to understand the functioning of the TCP protocol related to connection establishment.

The TCP protocol uses a 3-way handshake to establish a connection:

1. The client host sends a packet to the server with a special flag called the SYN flag. This flag indicates that the client wants to establish a connection.
2. The server responds with a packet containing both the SYN and ACK flags, which means that the server has accepted the request for the connection and that it is waiting for a confirmation from the client in order to have the connection established.
3. The client, right after receiving the packet with the SYN and ACK, responds with a packet containing only the ACK flag, which indicates to the server that the connection has been successfully established.

All connection requests received by a server are stored in a special queue which has a predetermined size, dependent on the operating system. They are kept stored until the server is informed by the client that the connection has been established. In case the server receives a connection request packet and the pending connections queue is full, this packet is discarded.

Basically, the attack consists of sending a large number of packets of connection request to a specific server. These packets are sent with a source address forged to an inexistent host (reserved addresses described in the chapter about the network address translation are often used in this circumstance). The server, right after receiving these packets, sends a response packet and waits for a confirmation from the client host. As the source address of the packets is false, this confirmation will never reach the server.

What happens is that during a specific moment, the server pending connections queue is found completely full. From this point on, all the requests for connections establishment are discarded, and the service is invalidated. Such invalidation persists for few seconds, for the server, when discovering that the confirmation is taking too long, removes the pending connection from the queue. However, if the attacker keeps on sending packets continuously, the service will be kept invalidated for as long as he wishes.

Not all machines are vulnerable to SYN Flood attacks. Newer implementations of the TCP protocol have mechanisms to cancel out these types of attacks.

How does the Aker Firewall SYN Flood protection work?

Aker Firewall has a mechanism whose purpose is to avoid SYN Flood attacks. Its functioning is based on the following steps:

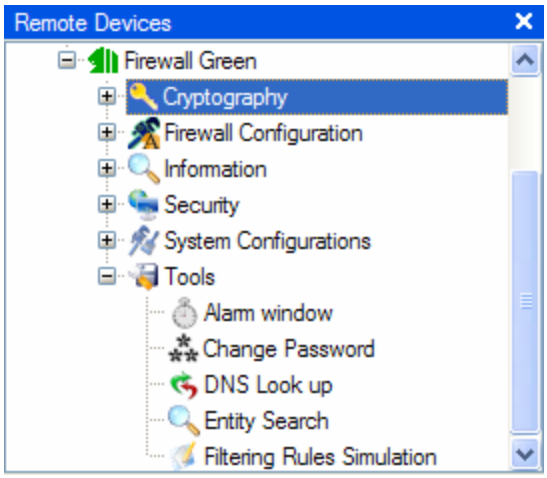
1. When a connection request packet (packet with the SYN flag, described in the previous topic) is sent to a server to be protected, the firewall registers it in a table and allows the packet to pass (evidently, the packet will only be allowed to pass if this has been authorized by the filtering rules configured by the administrator. For further details, refer to the chapter The Stateful Filter).
2. When the server response arrives informing that the connection has been accepted (packet with the SYN and ACK flags), the firewall will immediately send a packet to the server confirming the connection, and it will also allow the response packet to pass towards the client. From this point on, an internal clock will be activated in the firewall. This clock will mark the time during which the confirmation packet from the client must arrive.
3. If the connection request is a regular one, within a period of time shorter than the maximum allowed, the client will respond with a packet confirming the establishment of the connection. This packet will make the firewall validate the connection request and shut down the internal clock.
4. In case the client does not respond within the maximum time allowed, the firewall will send a special packet to the server which will drop the connection.

With all these procedures, the firewall prevents the pending connection queue in the server to overfill. This is possible since all the pending connections will be established as soon as the response packets reach the firewall. The SYN flood attack, then, will not take place.

It is important to emphasize that the functioning of this protection is based on the timeout for the clients confirmation packets. If the timeout is too short, valid connections may be refused. If the timeout is too long, the server, in the case of an attack, will keep a large number of established connections, which may cause even more serious problems.

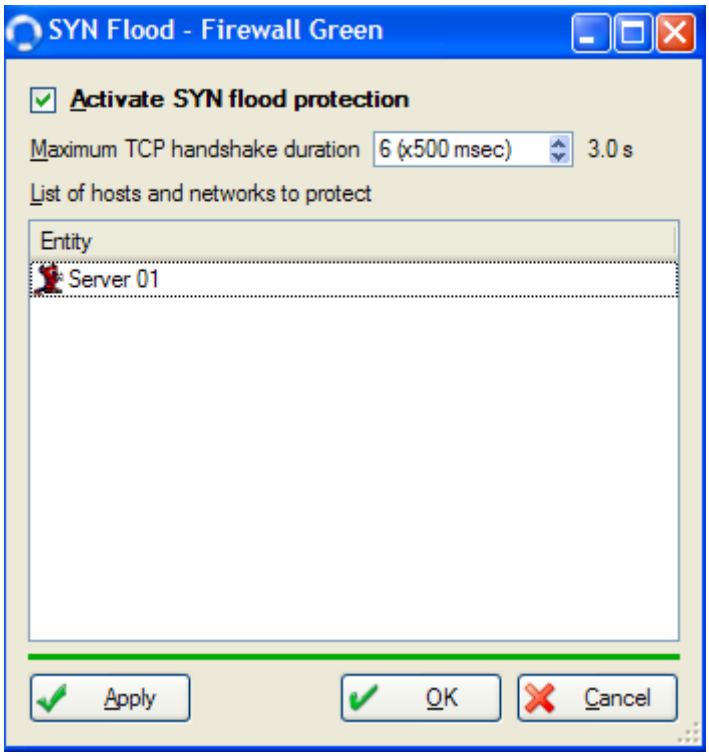
11-2 Configuring SYN Flood protection through the GUI

To access the SYN Flood protection parameters configuration window, do the following:



- Click on the *Security* menu in the Firewall window you want to manage
- Choose *SYN Flood*

The SYN Flood protection configuration window



- The **OK** button updates configuration parameters and closes the window
- **Cancel** discards all modifications and closes the window.

- The **Apply** button sends all modifications to the firewall and keeps the window open

Field meaning:SYN flood Fields:

Activate SYN Flood protection: This option must be checked to activate the protection against SYN Flood, and unchecked to deactivate it. (When SYN Flood protection is disabled, old configurations are kept stored but cannot be modified.)

Maximum TCP handshake duration: Defines the maximum time period, in 500ms units, a firewall will wait for a client connection confirmation. If this time is reached, a packet will be sent to the server host, dropping the connection.

 The ideal value for this field may vary for each installation. However, values from 3 to 10 are suggested, corresponding to time periods between 1,5 and 5 seconds.

List of hosts and networks to protect

This list includes the hosts, networks or sets that will be protected by the firewall.

To add a new entity to the protection list, do one of the following:

- Drag and drop an entity from the hosts, networks or set branches, in the Entities window, straight to the list.
- Right click on the list of hosts and network to protect to open the context-sensitive menu. Select **Add Entities**. Click on the entity to be added. Click **Add**.

To delete an entity from the list, select it and press delete on your keyboard, or right click on it, and choose the **Delete** option in the context-sensitive menu.

 All TCP servers, with service that can be used by external clients, should be included in the list of entities to be protected. The firewall address should not be added to this list, since FreeBSD and Linux operating systems are not susceptible to SYN Flood attacks.

11-3 Flood Protection

What is a Flood attack?

Flood attacks are characterized by the high number of open and established connections to web, ftp, and smtp, among other servers, from Internet hosts that were invaded and are being controlled and used to spread Denial of Service (DoS) attacks to other machines.

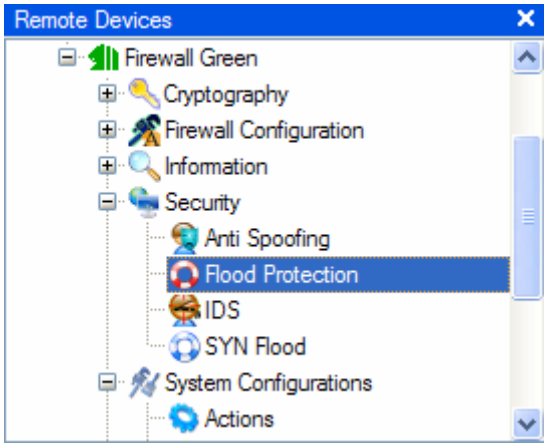
The protection is also useful to avoid service overuse (download sites, for example), as well as to prevent more serious damages caused by virus, such as NIMDA, which caused that each infected host opened hundreds of connections simultaneously.

How does Aker Firewall Flood Protection work?

Aker Firewall has a mechanism to frustrate flood attacks. Its operation is based on limitting the number of connections that may be simultaneously opened from a same host, to a protected entity.

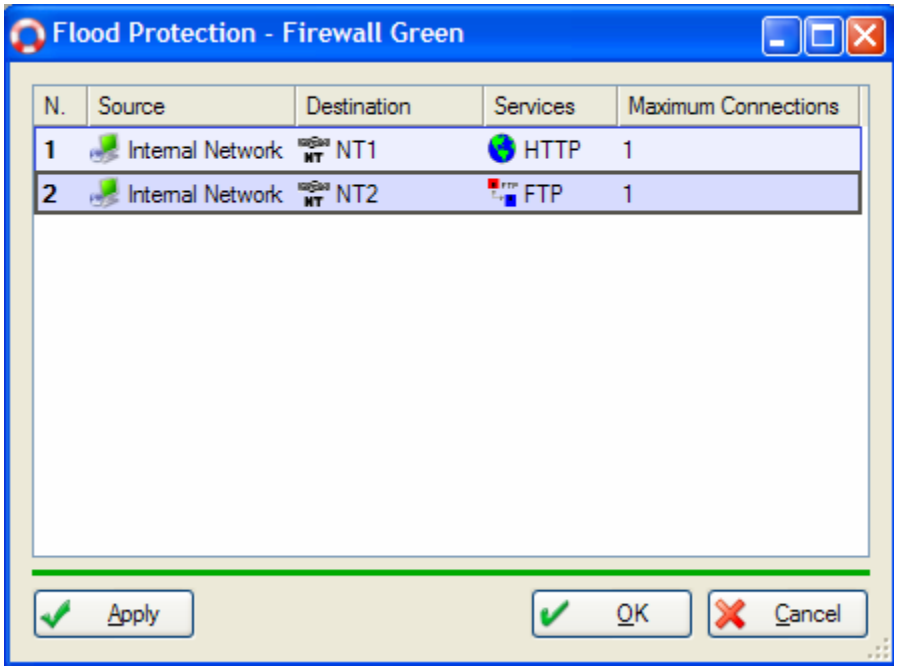
The firewall administrator must estimate this limit according to daily operation pattern of each server or network to being protected.

11-4 Configuring Flood protection through the GUI



- Click on the *Security* menu in the Firewall window you want to manage
- Choose *Flood Protection*

The Flood Protection configuration window



- The **OK** button updates configuration parameters and closes the window.
- **Cancel** discards all alterations and closes the window.
- **Apply** sends all alterations to the firewall and keeps the window open.

Field meaning:
Number: Corresponds to the Protection Flood rule number.

Source: A network or host that can be the source of DDoS attacks (usually the Internet)

Destination: Hosts or networks to be protected.

Services: Service to be protected. More than one entity may be included in this field.

Maximum Connections: Numeric field where the maximum number of simultaneous connections an entity can hold, from the same source, must be informed.

11-5 Anti-Spoofing Protection

What is a Spoofing?

IP spoofing involves the supply of false information about a person, or about a host identity, to obtain non-authorized access to systems and/or to the services they provide. Spoofing interferes in the way a client and a server establish a connection. Despite the fact that spoofing is possible with several protocols, the most known of the spoofing attacks is the IP spoofing.

The first step in a spoofing attack is the identification of two destination hosts, which we will call A and B. In most cases, one host (A) will have a trusting relationship with the other (B). It is indeed this relationship that the spoofing attack will try to exploit. Once the destination systems (A and B) have been identified, the attacker will try to establish a connection with B, in such a way that B believes it has a connection coming from A. The real connection request is from the attacker's host, which we will call X. This spoofing is done with X creating and sending a false message (created on X, but with A's source address) requesting a connection with B. When receives this message, B responds generating a similar message, recognizing the request, and establishing sequence code numbers.

Under usual circumstances, this message generated by B would be combined with a third message recognizing the sequence issued by B and sent to the client host. Thus, the handshake would be completed, and the connection could go on. However, since B believes it's communicating with A, B sends its response to A, and not to X. Therefore, to continue acting like A, X will have to respond to B, as if it were A, without knowing the sequence numbers generated by B. So, to successfully represent A, X must guess precisely the sequence numbers B will use to confirm the connection. In certain situations, this is much easier than we can imagine.

Furthermore, besides guessing the sequence number, the intruder X must also ensure that the initial response message from B never gets to A. If A were to receive such message, it would deny to B having requested the connection, and the spoofing attack would fail. To archieve its objective, i.e., to block B-to-A messages, the attacker X usually sends several connection request packets to A, to exhaust its capacity to receive requests, thus preventing it from responding to B. This technique is known as "port violation". When this operation comes to an end, the invader will be able to conclude the fake connection.

IP spoofing, as described above, is a clumsy and tedious strategy. However, a recent analysis revealed the existence of tools capable of executing a spoofing attack in less than 20 seconds. IP spoofing is a dangerous threat, but luckily, it is relatively easy to create protection mechanisms against it. The best defense against spoofing is to configure routers to reject any packet, which alleged source is from an internal network. This simple precaution will prevent external machines to take advantage of reliable relationships within internal networks.

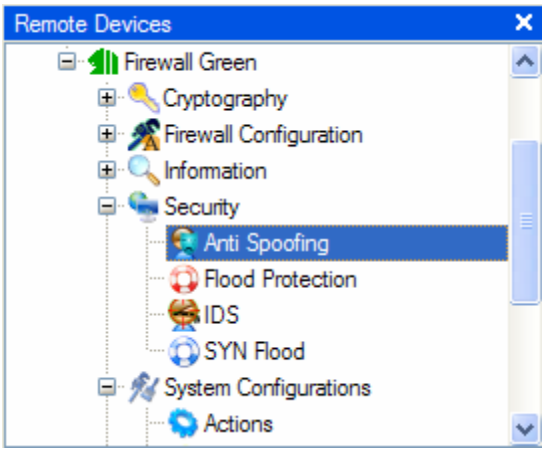
How does Aker Firewall Spoofing Protection work?

Aker Firewall has a mechanism to frustrate Spoofing attacks. It’s based on registering firewall-protected newtorks, i.e., networks behind each firewall network interface.

Only packets from registered entities will be accepted in the internal networks. And, from the external networks, only packets which originating IP addresses do not match any internal network addresses..

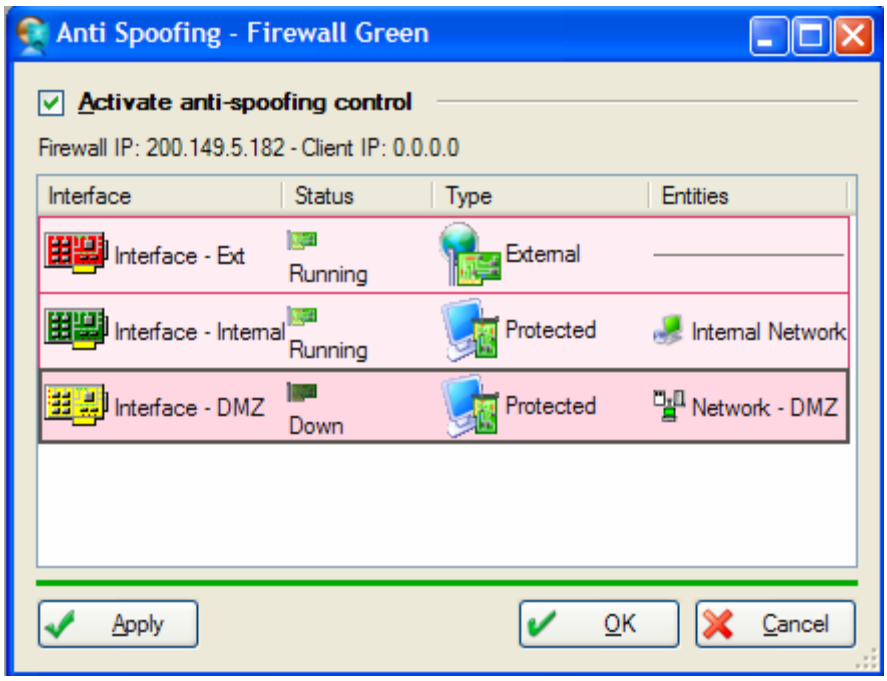
The firewall administrator must evaluate these networks, define corresponding entities, and utilize the graphical user interface to build the protection.

11-6 Configuring Anti-Spoofing protection through the GUI



- Click on the *Security* menu in the Firewall window you want to manage
- Choose *Anti-Spoofing*

The Anti-Spoofing configuration window



- The OK button will update the configuration parameters and close the window.
- Cancel will discard all alterations and close the window.
- Apply will send all alterations to the firewall and keep the window open.

Field meaning:
Activate anti-spoofing control: When this option is checked, it activates the Anti-Spoofing protection.
Interface: Corresponds to the interface entity registered in the firewall by the administrator.

Status: Shows the interface status; whether it is up or down. This field cannot be edited.

Type: By default, this field is set as *External*. It can be changed to *Protected* by right clicking on it. By doing this, it becomes possible to edit the *Entities* field next to it.

Protected means that the interface is connected to an internal network and only packets whose source IP addresses are present in any of the entities specified in the rule will be accepted. *External* means that the interface is connected to the Internet and thus incoming packets with any source addresses will be accepted, except those that belong to any entity listed in any rule of an interface marked as *Protected*.

Entities: When an entity is defined as *Protected*, it is necessary to include in this field a list of all networks and/or hosts that are connected to this interface.

11-7 Intrusion Detection System (IDS)

What is an intrusion detection system (IDS) ?

Intrusion detection systems are designed with the purpose of identifying accesses to systems or networks that are not according with the security policy of an organization. This identification is performed based on pattern matching, packet data or system information that can correspond to attacks or hacking attempts on a network.

The IDS are software or hardware solutions dedicated to the task of identifying and responding automatically to activities considered suspicious (usually known attack patterns or actions previously defined and configured as non authorized). A IDS recognize activities not considered normal and can be programmed to reconfigure the firewall dynamically (blocking attacks at real-time), send alerts to the administrator, save a log file or even close the connection.

How the support for IDS agents works ?

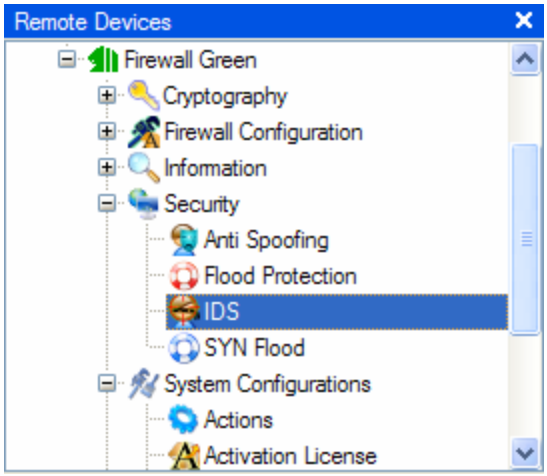
The intrusion detection agent interacts directly with the firewall adding blocking rules when it detects a suspicious behaviour. For example, let's suppose an agent monitoring a web server is configured to not allow more than 20 simultaneously connections from a same host in the Internet. If this configuration is violated, the agent automatically adds a rule in the firewall blocking the access from the host where the connections are coming from. This rule can be valid for a period of time, after this period it is automatically removed, or valid until the next firewall reboot.

Aker Firewall has specific plugins for Real Secure™, NFR™, Dragon™ and Snort products, allowing their immediate and transparent integration with the firewall. In this case the plugin must be installed on the host where the IDS agent is installed and then configured to add blocking rules in the firewall. The firewall must be configured to support IDS agents, as described in the next section. It is possible to use other IDS agents, however their integration must be made through the use of scripts. In this case, the section describing the command line interface should be written.

The IDS blocking rules will only be removed when they expire, by an administrator action or by a firewall reboot. In the last two cases all blocking rules will be removed (that is, it is not possible to remove a specific rule after it is added).

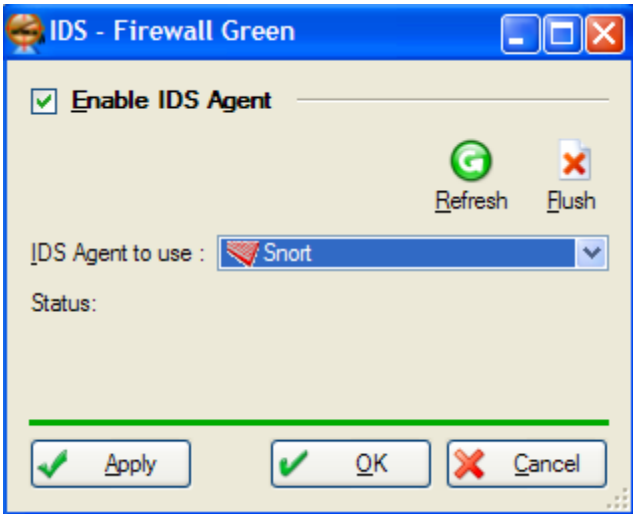
11-8 Configuring support for the Intrusion Detection Agent

To access the Instrusion Detection window, just do the following:



- Click on the *Security* menu on the firewall window you want to manage
- Select *IDS*

The Intrusion Detection window



This window configures all parameters that allow IDS agents to add blocking rules to the firewall..

- The **OK** button will close the IDS agent configuration window, and save all modifications.
- The **Cancel** button will close the window but will not apply any modification.
- **Apply** will send all alterations to the firewall, and will keep the window open.

Parameter meaning

Enable IDS Agent: This option must be checked to activate IDS agent support, and unchecked to deactivate it. (When IDS agent support is disabled, old configurations remain stored, but cannot be altered).

IDS Agent to use: Indicates the IDS agent enabled to add blocking rules to the firewall. This agent must have been previously registered in the firewall. For more information, see the Registering Entities chapter.

Status: Allows the administrator to verify the status of the connection to the IDS agent. A green value, with the word *Connected*, indicates that the firewall was successfully authenticated and the communication with the agent was established.

The **Apply** button will refresh the connection status.

The **Flush** button will exclude from the firewall all rules registered by the IDS agent. .

11-9 Installing the Plugin for IDS agents on Windows NT

IDS plugin installation is very simple. Insert Aker Firewall CD-ROM in the destination host, or copy the content of the agent installation directory, from the CD-ROM to any temporary directory in this host.

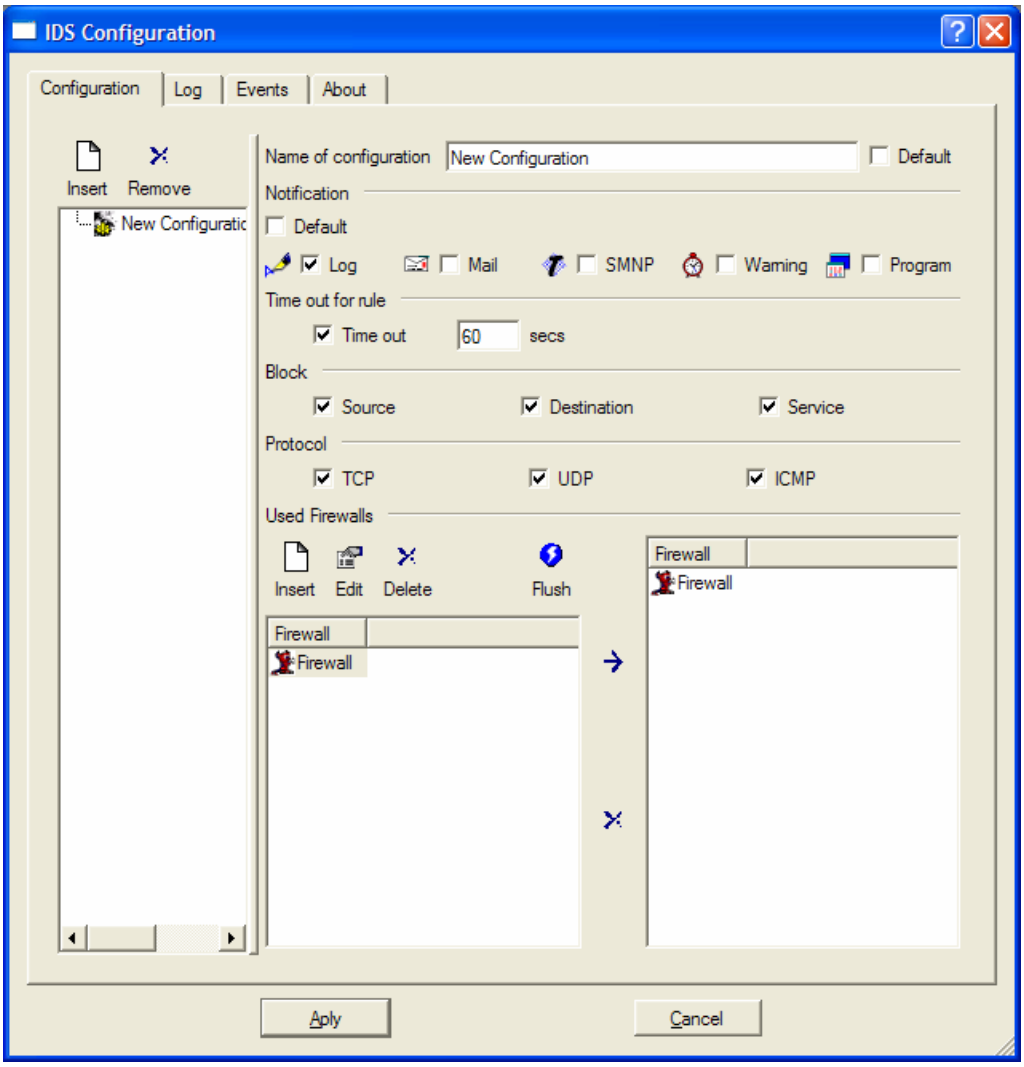
Then, click on the **Start** menu, select **Run**, and type in the following command: **D:\en\firewall\ids** (If your CD-ROM drive uses a letter other than D, replace it accordingly in the command). After that, select the appropriate file to your plataform and double click on it.

The program will display an initial window asking for a confirmation in order to continue with the installation. Click on the **Continue** button to proceed. Next, a window with the product licensewill be shown, asking for a confirmation to continue. Click on the **I Agree** button.

Aker Firewall IDS plugin configuration

After the plugin installation, it is necessary to configure it. This configuration allows registration of all firewalls that will be notified, as well as the definition of the rules that will be added.

To access the configuration program, click on the *Start* menu, and select the *Aker Firewall* group. Inside it, select the *Intrusion Detection* group, and then, the *Intrusion Detection* option. The following window will be displayed:



This window has 4 tabs. In the first one, shown above, is where the plugin configuration is done. It has a list with the names of the several configurations created by the administrator, and that will later be shown as action options in the Real Secure administration console. It is possibleto specify a configuration name when an event is being executed, or to use the **Default** button to specify a configuration that will be executed by default, i.e., when no configuration name is specified.

To create a new configuration, click on the **Insert** button, located in the top left side of the window. A blank configurationwill be created. To edit a configuration parameter, click on its name, and modify the desired parameters..

Parameter meaning

Configuration Name: The name that will be displayed in the administration consoles of Real SecureTM, NFRTM, Enterasys Dragon, and Snort. When selected, it will execute the actions defined by the administrator.

Notification: This field allows definition of the actions that will be executed by the firewall, when a blocking rule is added through the execution of aconfiguration. If the **Default** option is selected, the actions associated to the message “IDS blocking rule

added" will be executed. Otherwise, it is possible to specify exactly the actions to be taken. For more information on action configuration, see the Configuring System Actions chapter.

Block: This field is used to define the type of blocking that will be performed when the configuration is executed. There are three possible options that may be independently selected (when more than one option is selected, the rule will block packets that match all, and not just some, checked options):

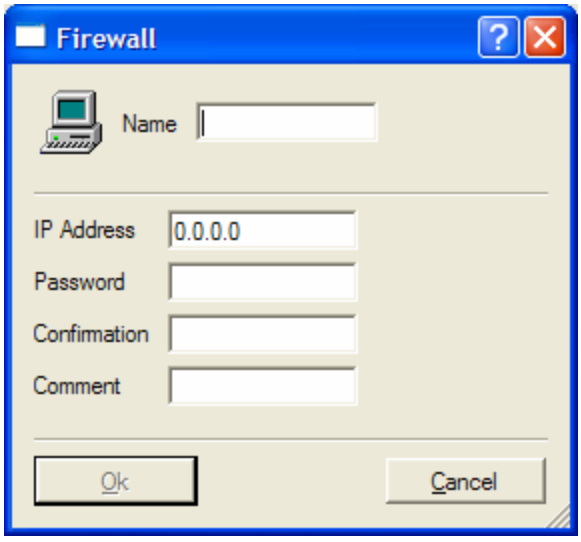
Source: Packets with source addresses equal to the rule's will be blocked

Destination: Packets with destination addresses equal to the rule's will be blocked

Service: Packets using the same service as the rule will be blocked. If this option is checked, the protocols that will be associated to theservice, must be selected in the **Protocol** field. This is necessary because Real SecureTM has a limitation. It does not supply the protocol of a service, only its number. Since NFR only inspects TCP traffic, this protocol must be selected when this IDS is being used.

Rule activation time: This field is used to define how long the rules added by the configuration will remain active. If the option **Activation Time** is checked, this must be specified, in seconds. If this option is unchecked, the rule will remain active untilnext time the firewall is restarted

Used Firewalls: In this field, we define to which firewalls the temporary rules will be added. An access password and IP address must be configured for each firewall. The access password must be the same configured in the definition of the IDS agent entity (for more information, see the Registering Entities chapter). When the Insert or Edit buttons are pressed, the following window will show up:

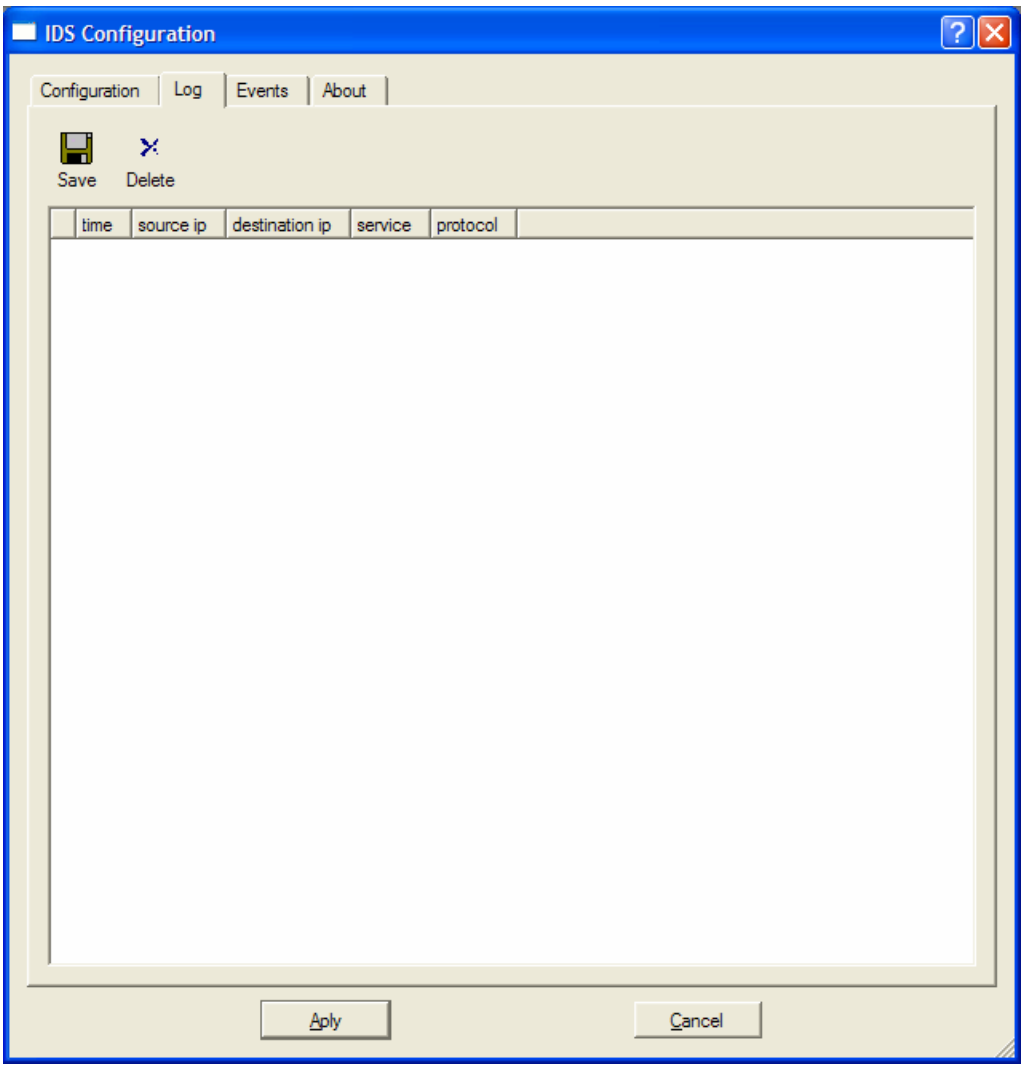


The firewalls defined above, must be added to the configuration through the following steps: Select the required firewalls; press the arrow button so that the selected firewalls will show up on the right list of the window.

The **Flush** button deletes the dynamic rules added to the selected firewalls by the IDS.

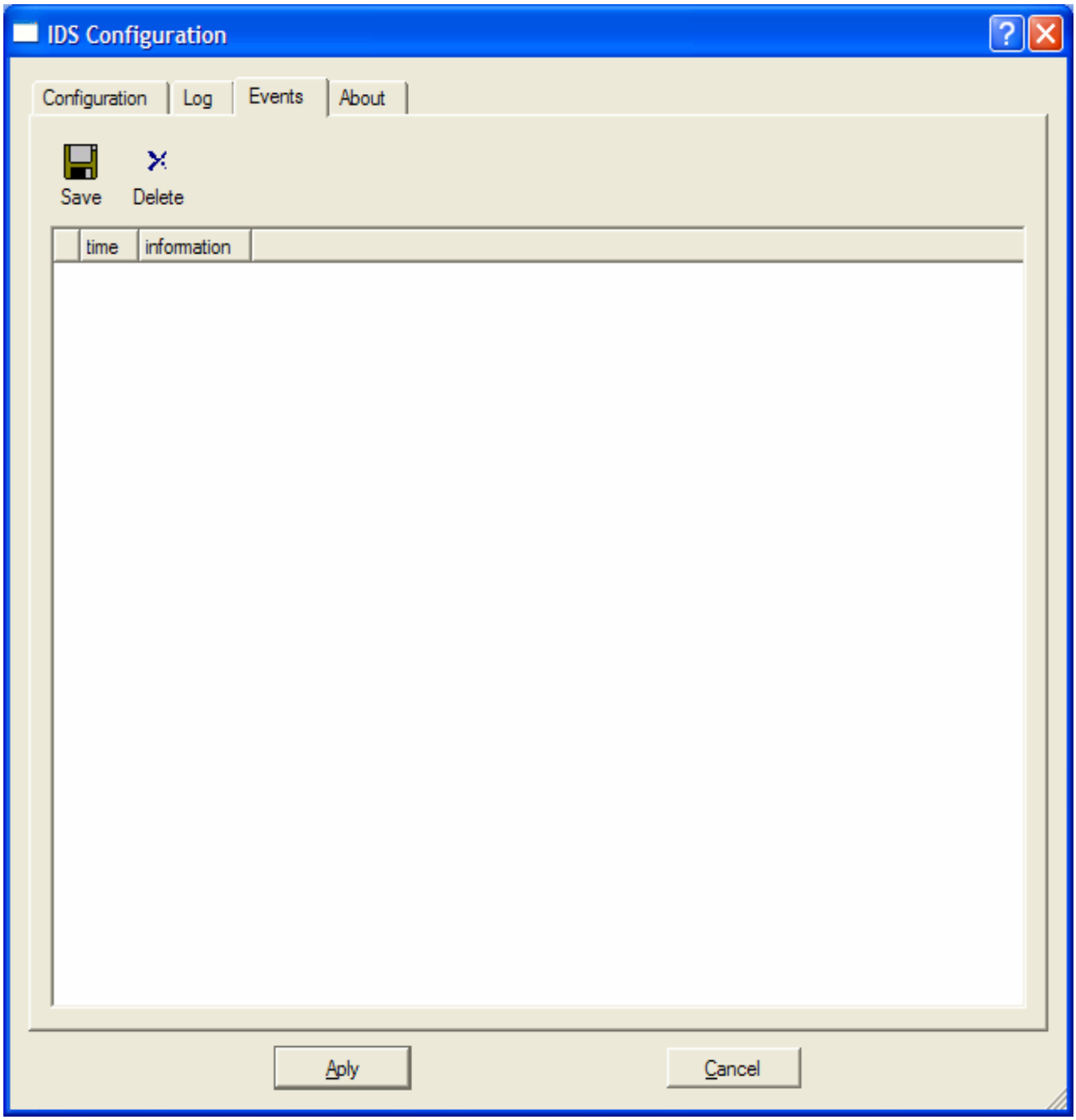
After all modifications are done, click on the **Apply** button. If the Real Secure is being used, a window will show up saying that the Real Secure Global Responses will be modified, and asking for a confirmation to continue. Click on the **Yes** button, to save the new configuration.

Log



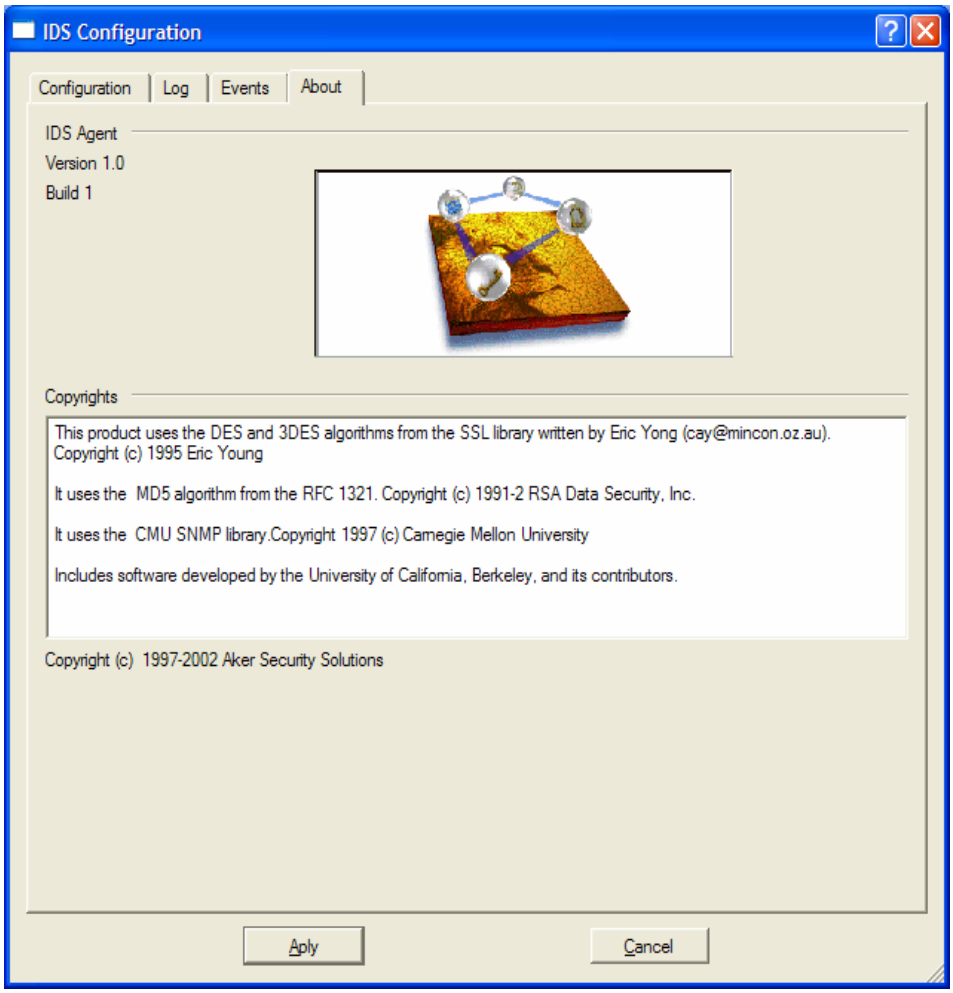
All the blocks sends for the IDS will be registred in this window.

Events



This is a very useful tab to trackagent operation. It has a list of several messages in chronological order. Next to each message, there's a colored icon symbolizing its priority.

About



General informations of product.

11-10 Using the command line interface – Syn Flood

The command line interface of the SYN flood protection is quite simple to be used, and it holds the same capacities of the graphic user interface.

Program location: `/etc/firewall/fwflood`

Syntax:

```
fwflood [activate | deactivate | show | help]
fwflood [add | remove] <name>
fwflood timeout <value>
```

Program help:

```
Aker Firewall - Version 5.0
fwflood - Configures the SYN Flood protection parameters
Usage: fwflood [activate | deactivate | show | help]
       fwflood [add | remove] <name>
       fwflood timeout <value>

       active      = activates the SYN Flood protection
       deactivate  = deactivates the SYN Flood protection
       show        = shows the active configuration
       add         = adds a new entry to be protected
       remove      = removes one entity to be protected
       timeout     = sets the connection establishment timeout
       help        = shows this message

For the add / remove commands:
       name        = name of the entity to be protected or removed
from
                     the protection list

For the timeout command:
       value       = maximum timeout in 500 ms units
```

Example 1: (viewing the configuration)

```
#/etc/firewall/fwflood show
Configuration parameters:
---------------------------------
SYN Flood protection: activated
Timeout             : 6 (x 500 ms)

List of entities to be protected:
---------------------------------
Aker                                          (Network)
Mail Server                                   (Host)
NT_01                                         (Host)
```

Example 2: (deactivating the SYN flood protection and viewing the configuration)

```
#/etc/firewall/fwflood deactivate
#/etc/firewall/fwflood show
Configuration parameters:
---------------------------------
```

```
SYN Flood protection: deactivated
Timeout             : 6 (x 500 ms)

List of entities to be protected:
---------------------------------
Aker                                              (Network)
Mail Server                                       (Host)
NT_01                                             (Host)
```

Example 3: (removing the host NT_01 from the list of entities to be protected and viewing the configuration)

```
#/etc/firewall/fwflood remove NT_01
#/etc/firewall/fwflood show
Configuration parameters:
---------------------------------
SYN Flood protection: deactivated
Timeout             : 6 (x 500 ms)

List of entities to be protected:
---------------------------------
Aker                                              (Network)
Mail Server                                       (Host)
```

Example 4: (including the host Server_01 in the list of entities to be protected and viewing the configuration)

```
#/etc/firewall/fwflood add Server_01
#/etc/firewall/fwflood show
Configuration parameters:
---------------------------------
SYN Flood protection: deactivated
Timeout             : 6 (x 500 ms)

List of entities to be protected:
---------------------------------
Aker                                              (Network)
Mail Server                                       (Host)
Server_01                                         (Host)
```

11-11 Using the command line interface – Flood Protection

Program Location: `/etc/firewall/fwmaxconn`

Program Help:

```
Aker Firewall - Version 5.0
Usage: fwmaxconn help
     fwmaxconn show
     fwmaxconn add <pos> <source> <destination> <service> <n_conns>
     fwmaxconn remove <pos>
     fwmaxconn <enable | disable> <pos>
the parameters are:
        pos     : rule position in the table
        source  : host/networkwhere connections originate
        destination: host/network to where the connections are going
        service : network service for which there is a connection
        n_conns : maximum number of simultaneous connections from the
same source
```

Example 1: (viewing the configuration)

```
#/etc/firewall/fwmaxconn show
Rule 01
--------
Source       : Network_Internet
Destination  : NT1
Services     : HTTP
Connections  : 5000
Rule 02
--------
Source       : Network_Internet
Destination  : NT3
Services     : FTP
Connections  : 10000
Rule 03
--------
Source       : Network_Internet
Destination  : Internal_Network
Services     : Gopher
Connections  : 100
```

11-12 Using the command line interface – Anti-Spoofing

Program location: /etc/firewall/fwifnet
Aker Firewall - Version 5.0
Usage: fwifnet [help | show]
fwifnet add interface <name_if> [external]
fwifnet add network <name_if> <network> [network1] [network2] ...
fwifnet remove [-f] interface <name_if>
fwifnet remove network <name_if> <IP_address> <netmask>

Program Help:

```
Usage: fwifnet [help | show]
       fwifnet add interface <name_if> [external]
       fwifnet add network <name_if> <network> [network1] [network2]
...
       fwifnet remove [-f] interface <name_if>
       fwifnet remove network <name_if> <IP_address> <netmask>

For the add / remove commands, we have the following:
     interface  : the network interface name to be controlled
     external   : this word makes the firewall consider that the
interface is
                  external
     network    : an allowed network in a non-external interface
```

Example 1: (viewing the configuration)

```
#/etc/firewall/fwifnet show
Aker Firewall - Version 5.0
Anti-Spoofing module status: enabled
Registered interface: DMZ_Interf
     Allowed network: DMZ_network
Registered interface: External_Interf (external)
Registered interface: Internal_interf
     Allowed network: Internal_network
```

11-13 Using the command line interface - IDS

It is very simple to use the command line interface to configure. Intrusion Detection Systems / ou the support for intrusion detection. In addition, this interface has the same resources as the graphical user interface.

Program location: /etc/firewall/fwids

Sintaxe:

```
fwids [enable | disable | show | clear??? | help]
fwids agent <entity>
fwids block [source <source ip>] [destination <destination ip>]
                [service <service/protocol>] [time]
```

Program Help::

```
Aker Firewall - Version 5.0
fwids – Configures IDS external agent parameters
Usage: fwids [enable | disable | show | clear | help]
    fwids agent <entity>
fwids block [source <source ip>] [destination <destination ip>]
                [service <service/protocol>] [time]

     enable       = enables IDS external agents operation
     disable      = disables IDS external agents operation
     show         = shows current configuration
     block        = adds a temporary blocking rule
     clear        = removes all temporary blocking rules
     agent        = specifies name of entity with agent data
     help         = displays this message

For the block command, we have:
     source       = indicates that connections originating in the
specified IP address must be blocked
     destination  = indicates that connections going to the specified
IP address must be blocked
     service      = indicates that connections using specified service
must be blocked.  In this case, the following must be done:
                    specify the service as the port  for TCP and UDP
protocols;
                    specify the type of service for ICMP;
                    or the protocol number for other protocols (ex:
23/tcp, 53/udp, 57/other)
     time         = time, in seconds, during which the rule will
remain active. If not specified, the rule will be active untilnext
time the firewall is started.
```

Example 1: (Enabling support for intrusion detection)

```
#/etc/firewall/fwids enable
```

Example 2: (Defining IDS agent)

```
#/etc/firewall/fwids agent IDS_Agent
```

The entity IDS_Agent must have been previously registered in the system. For more information on how to register entities in Aker Firewall, go to chapter Registering Entities.

Example 3: (Viewing current configuration)

```
#/etc/firewall/fwids show
Configuration parameters::
---------------------------
External IDS agent: enabled
Agent: IDS_Agent
```

Example 4: (Adding a blocking rule from host 192.168.0.25 to host 10.0.0.38, in the WWW service, port 80 of TCP protocol, for one hour)

```
#/etc/firewall/fwids block source 192.168.0.25 destination 10.0.0.38
service 80/tcp 3600
```

12-0 Configuring the System Actions

This chapter shows how to configure the system automatic responses for previously determined situations.

What are the system actions ?

Aker Firewall has a mechanism that allows the creation of automatic responses for specific situations. These automatic responses are configured by the administrator in a series of possible independent actions that will be performed when a pre-determined situation occur.

What are the system actions for?

The actions purpose is to make a high interaction degree between the firewall and the administrator possible. Its use allows, for example, the execution of a program capable of paging the administrator when the firewall detects an attack. Therefore, the administrator will be capable of taking an immediate action, even if he is not monitoring the firewall at the moment.

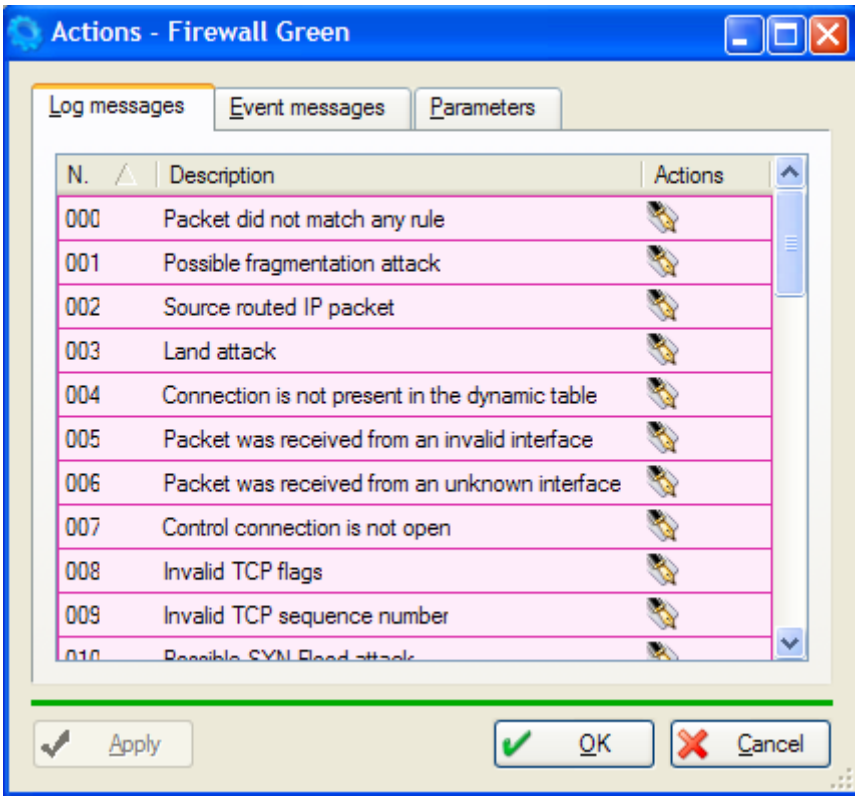
12-1 Using the graphic user interface

To access the action configuration window, the following must be done:

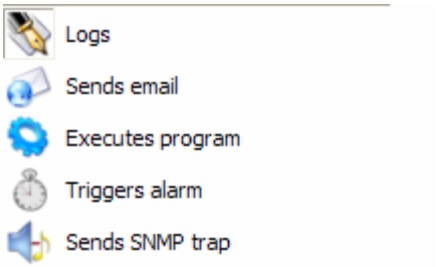
- Click on the menu *System Configurations* in the main window menu.
- Choose the *Actions* item

The actions configuration window

When this option is selected, the window that allows the configuration of actions to be taken by the system will be shown. For each log and event message and for the packets which do not match any rule it is possible to set independent actions. The window shown will have this format:



To select the actions to be performed for the messages shown in the window, right click on the messages. For each selected action, a corresponding icon will be displayed.



For each message that has the icon of an action, the correspondent action will be taken by the firewall when the message occurs. The following actions are allowed:

- **Logs**: If this option is active, every time the corresponding message occurs, it will be logged by the firewall.
- **Sends Mail**: If this option is active, an e-mail will be sent when the corresponding message occurs (the e-mail address configuration will be shown in the next section).
- **Executes Program**: If this option is active, a program defined by the administrator will be executed every time the corresponding message occurs (the configuration of the path of the program to be executed will be shown in the next section).
- **Triggers alarm**: If this option is active, the firewall will show an alert window every time the corresponding message occurs. This alert window will be shown on the machine where the remote graphic user interface is running and, if the host allows, a warning sound will also be produced. If the graphic user interface

is not active, no messages will be shown and this option will be ignored (this action is particularly useful to call the administrator's attention when an important message occurs).

- **Sends SNMP trap**: If this option is active, an SNMP Trap will be sent to the SNMP manager every time the corresponding message occurs (the configuration of the parameters to send traps will be shown in the next section).

It is not possible to change the actions for the firewall initialization event message (message number 43). This message will always have only the Log option as configured actions.

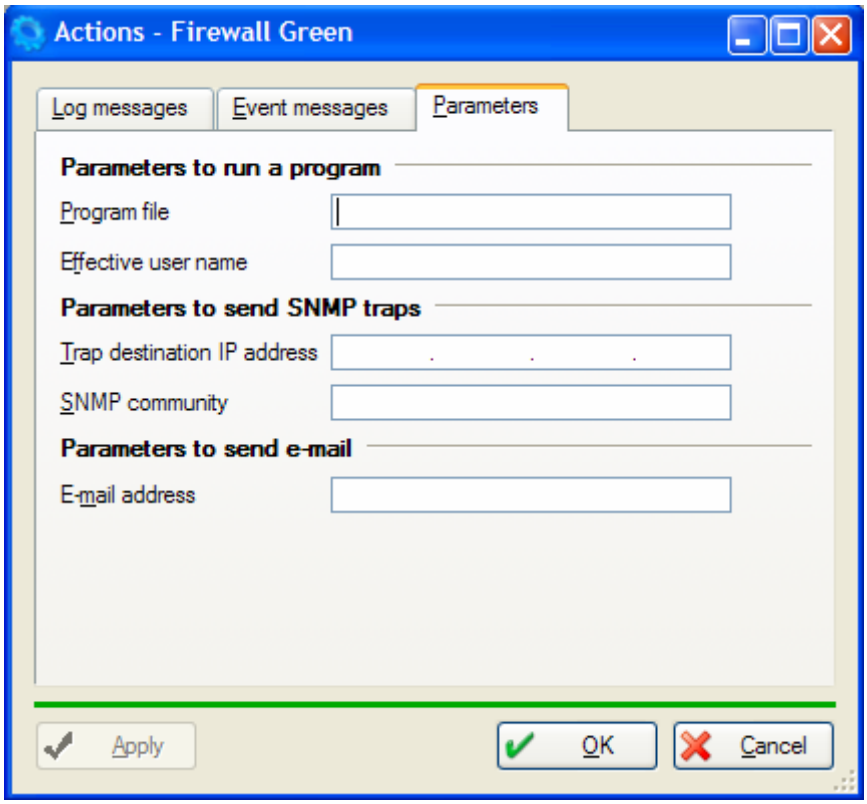
Meaning of the actions window buttons

- The **OK** button will close the actions window and apply the changes done.
- The **Cancel** button will close the window and discard the changes done.
- The **Apply** button will apply the changes but kept the window open.

The parameters configuration window

In order to get the system to take the actions, it is necessary to configure certain parameters (for example, for the firewall to send an e-mail, it is necessary to configure the address). These parameters are configured through the parameters configuration in the actions window.

This window is shown when the **Parameters** tab in the messages window is clicked . It has the following format:



Meaning of the parameters:

- **Parameters to run a program**

Program file: This parameter configures the name of the program to be run by the system, when an action with the option *Program* occurs. The full path name of the program must be typed. It is necessary to attempt to the fact that the program and all the directories on the path must have execution permission for the user who will execute it (which is configured in the next option).

The program will receive the following parameters by the command line (in the same order as shown):

1. Name of the program being run (this is a standard for the unix operating system).
2. Type of message (**1** - for log or **2** - for event).
3. Priority (**7** - debug, **6** - information, **5** - notice, **4** - warning or **3** - error).
4. Number of the message that caused the execution of the program or **0** to indicate the cause was not a message. (in this case, the execution of the program was initiated by a rule)
5. ASCII string with the complete text of the message (this string may have the line feed characters in it).

 In the UNIX operating system , the slash "/" is used to specify the path of a program. It may confuse those who are used to the DOS/Windows environment, where the backslash is "\" is used.

Effective user name: This parameter indicates the identity of which the external program will be executed. The program will have the same privileges of this user.

 This user must be a valid user, registered in the FreeBSD or Linux. It is necessary not to confuse him with the Aker Firewall users, which are useful only for the Firewall administration.

- **Parameters to send SNMP traps**

Trap destination IP address: This parameter configures the IP address of the SNMP manager to which the firewall must send the traps.

SNMP community: This parameter configures the name of the SNMP community that will be sent in the traps.

The sent SNMP traps will have the generic type **6** (*enterprise specific*) and the specific type **1** for log or **2** for events. They will be sent with the enterprise number **2549**, which is the number assigned by the IANA to the Aker Consultancy and Informatics.

There is a file called **/etc/firewall/mibs/AKER-MIB.TXT,** which brings information about Aker Consultancy and Informatics sub-tree in the global tree. This file is written on the ASN.1 notation.

- **Parameters to send e-mail**

E-mail address: This parameter configures the e-mail address of the user the email will be sent to. This user can be an user from the firewall itself or not (in this situation, it is necessary to write the complete address, for example user@aker.com.br).

If it is desired to send e-mails to several users, a list can be created and the name of the list can be inserted in this field.

 It is important to notice that, if any of these fields are blank, the corresponding action will not be taken, even if it is active.

12-2 Using the command line interface

The command line interface used to configure the actions has the same capacity of the graphic user interface and it is easy to use.

Program location: `/etc/firewall/fwaction`

Syntax:

```
fwaction help
fwaction show
fwaction assign <number> [log] [mail] [trap] [program] [alert]
fwaction <program | user | community> [name]
fwaction ip [IP address]
fwaction email [address]
```

Program help:

```
fwaction - Command line interface for configuring system actions
Usage: fwaction help
       fwaction show
       fwaction assign <number> [log] [mail] [trap] [program] [alert]
       fwaction <program | user  | community> [name]
       fwaction ip [IP address]
       fwaction e-mail [address]

       help      = shows this message
       show      = lists the messages and the actions assigned to each
of them
       assign    = assigns actions for a specific message
       program   = defines the name of the program to be run
       user      = defines the name of the user that will run the
program
       community = defines the name of the SNMP community for trap
generation
       ip        = defines the IP address of the SNMP server that will
receive
                   the traps
       e-mail    = defines the name of the user that will receive the
e-mails

For the assign command:
       number    = number of the message which the action will be
assigned to
                   (the number of each message is shown on the left
when
                    the option show is selected)
       log       = Logs each message generated
       mail      = Sends an e-mail for each message generated
       trap      = Sends a SNMP trap for each message generated
       program   = Executes program for each message generated
       alert     = Open an alert window for each message generated
```

Example 1: (configuring the parameters for e-mails sending and program execution)

```
#fwacao e-mail root
#fwacao program /etc/pager
#fwacao user nobody
```

Example 2: (showing the complete configuration of the actions of the system)

```
#fwacao show
General Conditions:

00 - Packet did not match any rule
>>>> Log

Log messages:

01 - Possible fragmentation attack
>>>> Log
02 - Source routed IP packet
>>>> Log
03 - Land attack
>>>> Log
04 - Connection is not present in the dynamic table
>>>> Log
05 - Packet was received from an invalid interface
>>>> Log
06 - Packet was received from an unknown interface
>>>> Log
07 - Control connection is not open
>>>> Log

(...)

231 - Host did not answer and was marked as down
>>>> Log
232 - Link was marked as up
>>>> Log
233 - Link was marked as down
>>>> Log

Configuration parameters:

program   : /etc/pager
user      : nobody
e-mail    : root
community :
ip        :
```

Attention: Due to a large number of messages, only the first and the last ones are shown. The real program will show all of them when executed.

Example 3: (assigning actions to the *Packet did not match any rule* message and showing the messages)

```
#fwacao assign 0 log mail alert
#fwacao show
General Conditions:

00 - Packet did not match any rule
>>>> Log Mail Alert

Log messages:

01 - Possible fragmentation attack
>>>> Log
```

```
02 - Source routed IP packet
>>>> Log
03 - Land attack
>>>> Log
04 - Connection is not present in the dynamic table
>>>> Log
05 - Packet was received from an invalid interface
>>>> Log
06 - Packet was received from an unknown interface
>>>> Log
07 - Control connection is not open
>>>> Log

(...)

231 - Host did not answer and was marked as down
>>>> Log
232 - Link was marked as up
>>>> Log
233 - Link was marked as down
>>>> Log

Configuration parameters:

program   : /etc/pager
user      : nobody
e-mail    : root
community :
ip        :
```

Attention: Due to a large number of messages, only the first and the last ones are shown. The real program will show all of them when executed.

Example 4: (canceling all the actions for the *Source routed IP packet* message and showing the messages)

```
#fwacao assign 2
#fwacao show
General Conditions:

00 - Packet did not match any rule
>>>> Log Mail Alert

Log messages:

01 - Possible fragmentation attack
>>>> Log Mail
02 - Source routed IP packet
>>>>
03 - Land attack
>>>> Log
04 - Connection is not present in the dynamic table
>>>> Log
05 - Packet was received from an invalid interface
>>>> Log
06 - Packet was received from an unknown interface
>>>> Log
07 - Control connection is not open
>>>> Log
```

```
(...)

231 - Host did not answer and was marked as down
>>>> Log
232 - Link was marked as up
>>>> Log
233 - Link was marked as down
>>>> Log

Configuration parameters:

program   : /etc/pager
user      : nobody
e-mail    : root
community :
ip        :
```

Attention: Due to a large number of messages, only the first and the last ones are shown. The real program will show all of them when executed.

13-0 Viewing the System Log

In this chapter, we will show how to view the system log, an essential resource for attack detection, firewall tracking and monitoring, and during the system configuration phase.

What is the system log?

The log is where the firewall stores all information about packets received. It may contain records generated by any of the three main modules: packet filter, network address translation, and encryption/authentication. The type of information stored in the log depends on the firewall configuration, but basically, it includes information about accepted, rejected and discarded packets, packet errors, and network address translation information.

Among all the data stored in the log, information about discarded and rejected packets is, possibly, the most important. Because it is through the analysis of these data that we may determine eventual attempts of invasion, unauthorized service use, and configuration errors, among others.

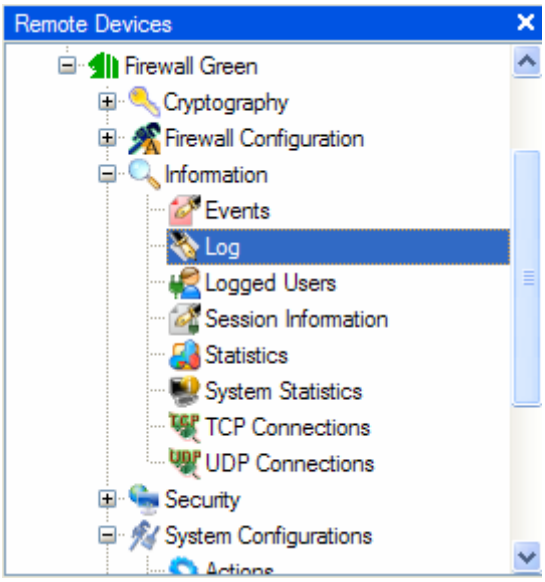
What is a log filter?

Even though the system is configured to record all kinds of information, sometimes a specific type of information is of more interest (for example, the rejected attempts to use the POP3 service of a specific machine, on a given day, or still, the attempts that were indeed accepted). The log filter is a mechanism offered by Aker Firewall, to create different views of the whole set of log records, making it easier to obtain the desired information.

The filter only shows information previously registered in the log. If specific information is targeted, the log system must be configured to register it first, and then, a filter is used to view it.

13-1 Using the graphic user interface

To access the Log window, do the following:



- Click on the *Information* menu of the firewall you want to view the log
- Select *Log*

The Log toolbar

Every time the Log option is selected, the Log bar comes up automatically. Located next to other bars, the log bar may be dragged and left floating anywhere over the Log information. It looks like shown below:

Legend:

 Opens the firewall Log Filter window.

 This icon will only show up when the firewall is performing a search in the Log. It allows interruption of the search.

 Exports the Log to several file formats.

 Erases the firewall Log.

 Performs a reverse resolution of the IP shown by the Log.

 The log screen is refreshed at every specified period of time, defined in the field next to it (described below).

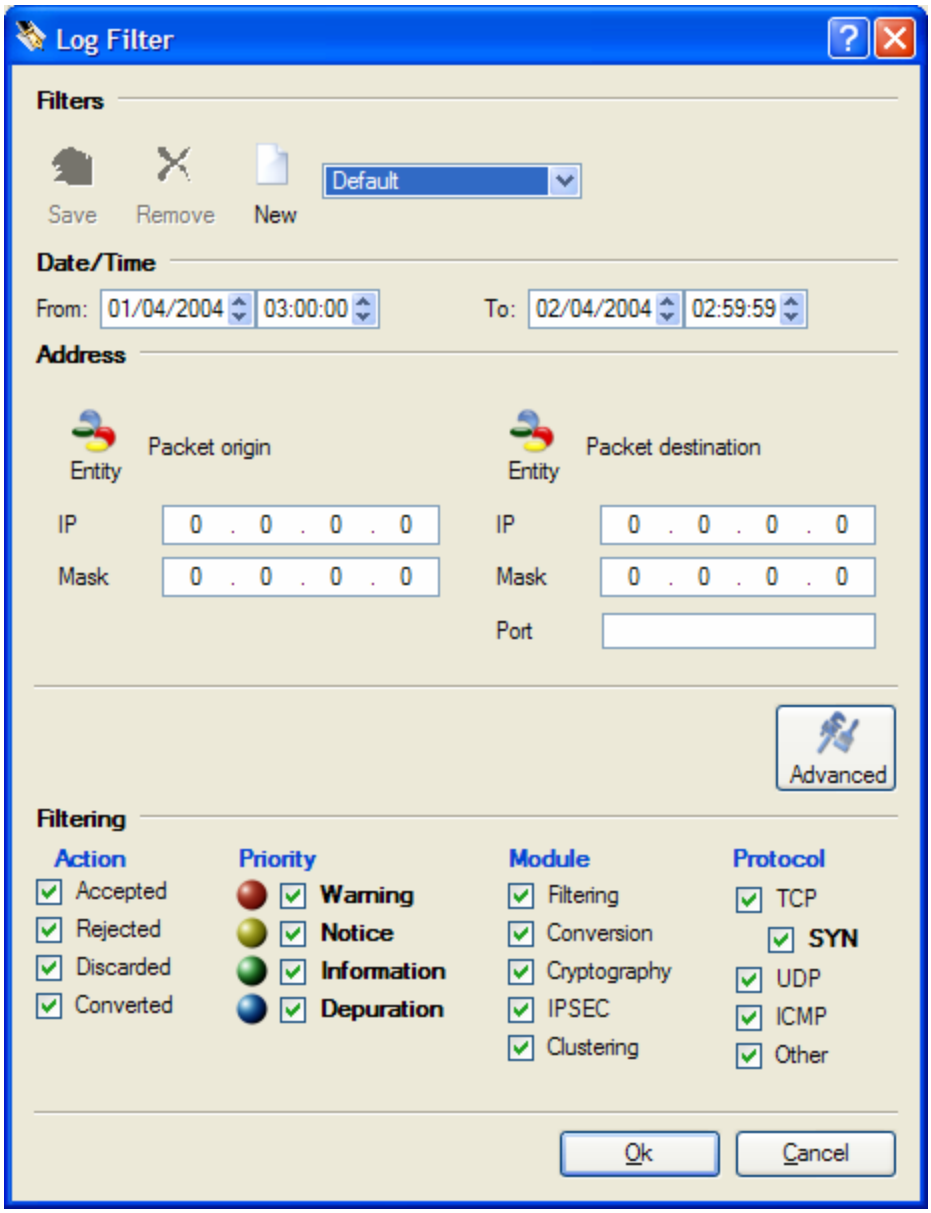
Defines how often the log information window is updated by the firewall.

 Goes forward and backward through the Log.

Expands Log messages to show all the information.

The window below shows up when the Filter icon is selected:

The Log Filtering Window



The **Save**, **Remove**, and **New** buttons are located in the top part of the window. It allows saving a research profile to be used later by the administrator.

To save a log filter, do the following:

1. Fill up all the fields in the desired way.
2. Give it a name in the field **Filters**
3. Click on the Save button.

To apply a saved filter, select its name in the **Filters** field. All fields will be automatically filled with the saved data.

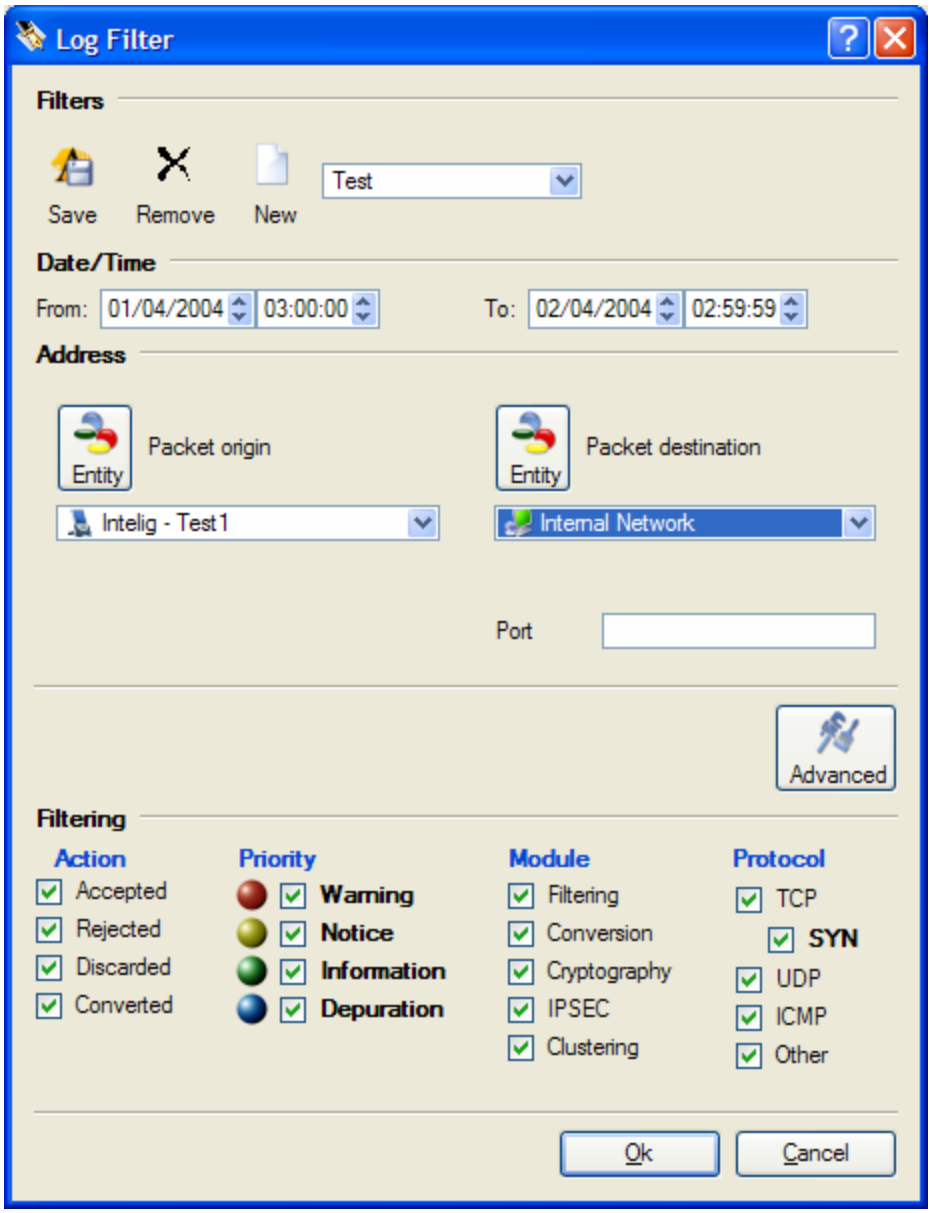
To remove a filter, do the following:

1. Select the filter to be removed in the **Filters** field.
2. Click on Remove.

The defaul filter is configured to show all records of the current day. To view information of other time periods, configure the **From** and **To** fields, in the Date/Time area, to the desired dates (the initial and the final dates will be included in the view).

If you want to target source and/or destination addresses belonging to a specific set of hosts, you can use the IP / Mask fields, or the Entity button to specify it

To choose the type of filtering that will be performed, press the **Entity** button. The following fields will be displayed on the window: packet origin IP and Mask, and packet destination IP and Mask. These fields may be used to specify the source set and/or the destination set. In this case, it is possible to select an entity, in each one of these fields, that will be used to specify origin and destination sets. Buttons can be selected independently. This way, the filtering criteria can be based on one or both, an entity in the origin set or on the IP and Mask of the destination set.



To monitor a specific service, just write its number in the **Port** field. From then on, only entries with the specified service will be displayed. It is also important to select the protocol associated with the service, in the protocol field. To access it, press the Advanced button.

To specify a service in the TCP and UDP protocols, it is necessary to put the destination port number, associated to the service, in this field. In ICMP, it is necessary to put the type of the service. For other protocols, the number of the desired protocol is needed..

In addition to these fields, there are other options that may be combined to further restrict the type of information shown:

Action:

Represents the action taken by the system to deal with a specific packet. The following options can be independently selected:

- Accepted

Shows packets accepted by the firewall.

- Rejected

Shows the packets rejected by the firewall.

- Discarded

Shows packets discarded by the firewall.

- Converted

Shows the messages related to network address translation.

Priority:

Different types of messages have different priorities. The higher the priority, the more important the record. A list of all possible priorities is shown below, ordered from the most to the least important (if the firewall is configured to send a copy of the log to the Syslogd (logging subsystem), the Syslog message generation will also follow this priority scheme):

- Warning

Records with this priority level usually indicate an attack or a very serious situation (such as encryption channel configuration error). This type of record is always preceded by a message with more information about it.

- Notice

Packets that were rejected or discarded by the system are usually classified with this priority level. They either matched a rule configured to reject or discard them, or they did not fit any rule. In some situations, they may be preceded by explanatory messages.

- Information

These records add useful, non-critical information to the Firewall administration. No explanatory message precedes them. This priority level is usually associated to packets accepted by the firewall..

- Debug

Records with this priority level are usually useful only when the system is being configured. Messages of network address translation are examples with this priority level.

Module:

This option is for independently viewing the records generated by each of the three main system modules: (1) Packet Filter, (2) Network Address Translator and (3) Encryption, IPsec, and Clustering module.

Protocol:

This field specifies the protocol of the records that will be displayed. The options are:

- TCP

Records generated by TCP packets will be shown. When this option is checked, the TCP/SYN option is automatically unchecked.

- TCP/SYN

Records generated by TCP connection initiation packets – those with the SYN flag on - will be displayed. With this option checked, the TCP option will automatically be unchecked.

- UDP

Records generated by UDP packets will be shown..

- ICMP

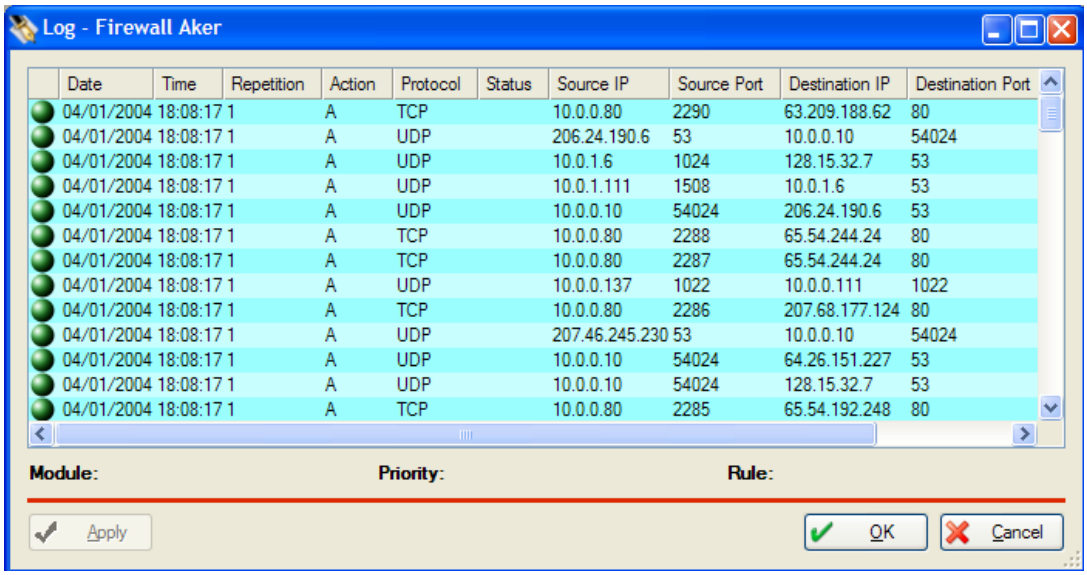
Records generated by ICMP packets will be displayed.

- Other

Packets generated by protocols other than TCP, UDP, and ICMP will be displayed. It is possible to further restrict the protocol to be displayed, by specifying its number, through the **Destination Port** or **Type of Service** fields

- The **OK** button will apply the chosen filter, and show the filtered information on the Log window.
- The **Cancel** button will cancel the filtering operation, and the Log window will display the same information it showed before.

The Log Window



The Log Window will be displayed after a new filter is applied. It has a list of several entries. All entries have the same format, however, depending on the generating packet protocol, some fields may be missing. Also, some entries will be preceded by a special text message, with additional information about the record (the meaning of each type of record will be shown in the next section)..

Important notes:

- Records will be shown 100 at a time.
- Only the first 10,000 records matching the chosen filter will be shown. The remainder can be accessed by exporting the log to a file, or by using a filter that generates less records.
- To the left of each message, a colored icon will be displayed, representing its priority. A legend is presented below:

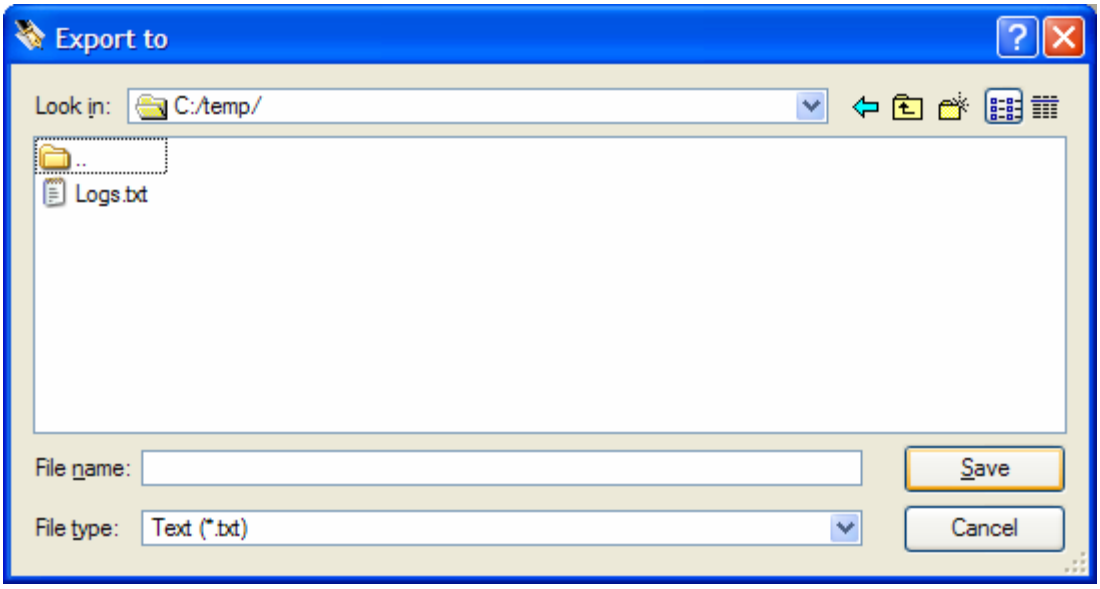
Blue	Debug
Green	Information
Yellow	Notice
Red	Warning

- Additional information about a record can be obtained by clicking over a message.

If a log file is deleted, the only way to recover the information is restoring a backup copy.

Logs will be exported together with their additional messages if the Expand option is checked, and the option to export text file type is chosen. Otherwise, the log will be exported without messages..

This option is very useful when you want to send a copy of the log to someone else, to keep a text copy of important information, or to import a log by one of the log analyzers cited above. The following window will show up when the Export button is pressed.



To export the log content, name the file to be created, choose its type, and click on **Save**. To cancel the operation, click on **Cancel**.

If a file with the same name already exists, it will be erased.

- The **Next** button, represented by a right pointing arrow in the toolbar, shows the next 100 records selected by the filter. If there are no more records, this option is disabled..
- The **Previous** button, represented by a left pointing arrow in the toolbar, shows the previous 100 records. If there are no previous records, this option is disabled.
- The **Help** button shows specific help for the Log Window.

13-2 Format and Meaning of the Fields of Log Registers

Below, there is a description of each record format, followed by a description of each field. Record format is the same for both GUI and command line interface.

Records generated by the Packet Filter or by the Encryption Module

These record types may be preceded by a special message. A complete list of all possible special messages and their meanings can be found in Appendix A.

- **TCP protocol**

Record format:

```
<Date> <Time> - <Repetition> <Action> TCP <Status> <Source IP> <Source
Port> <Destination IP> <Destination Port> <Flags> <Interface>
```

Fields description:

Date: Record generation date.
Time: Record generation time.
Repetition: Number of times the record was consecutively repeated. This field is shown between parentheses in the command line interface.
Status: This field, seen between parentheses in the command line interface, uses up to three independent letters. They are:

A: Authenticated packet
E: Encrypted packet
S: Packet using SKIP or AKER-CDP key exchange

Action: This field indicates the action executed by the firewall with each packet. It may have the following values:

A: Packet accepted by the firewall
D: Packet discarded by the firewall
R: Packet rejected by the firewall

Source IP: Source IP address of the packet that generated the record..
Source Port: Source Port of the packet that generated the record.
Destination IP: Destination IP address of the packet that generated the record.
Destination Port: Destination Port of the packet that generated the record.
Flags: TCP protocol flags present in the packet that generated the record. This field may have up to six independent letters. Each letter indicates that its corresponding flag was turned “on” in the packet. Their meanings are as follows:

S: SYN
F: FIN
A: ACK
P: PUSH

R: RST (Reset)
U: URG (Urgent Pointer)

Interface: Firewall network interface through which the packet was received.

- **UDP protocol**

Record format:

```
<Date> <Time> - <Repetition> <Action> UDP <Status> <Source IP> <Source
Port> <Destination IP> <Destination Port> <Interface>
```

Fields description:

Date: Record generation date.
Time: Record generation time.
Repetition: Number of times the record was consecutively repeated. This field is shown between parentheses in the command line interface.
Status: This field, seen between parentheses in the command line interface, uses up to three independent letters. They are:

A: Authenticated packet
E: Encrypted packet
S: Packet using SKIP or AKER-CDP key exchange

Action: This field indicates the action executed by the firewall with each packet. It may have the following values:

A: Packet accepted by the firewall
D: Packet discarded by the firewall
R: Packet rejected by the firewall

Source IP: Source IP address of the packet that generated the record.
Source Port: Source Port of the packet that generated the record.
Destination IP: Destination IP address of the packet that generated the record.
Destination Port: Destination Port of the packet that generated the record.
Interface: Firewall network interface through which the packet was received.

- **ICMP protocol**

Record format:

```
<Date> <Time> - <Repetition> <Action> ICMP <Status> <Source IP>
<Destination IP> <Type of Service> <Interface>
```

Fields description:

Date: Record generation date.
Time: Record generation time.
Repetition: Number of times the record was consecutively repeated. This field is shown between parentheses in the command line interface.

Status: This field, seen between parentheses in the command line interface, uses up to three independent letters. They are:

A: Authenticated packet
E: Encrypted packet
S: Packet using SKIP or AKER-CDP key exchange

Action: This field indicates the action executed by the firewall with each packet. It may have the following values:

A: Packet accepted by the firewall
D: Packet discarded by the firewall
R: Packet rejected by the firewall

Source IP: Source IP address of the packet that generated the record.
Destination IP: Destination IP address of the packet that generated the record.
Type of service: Type of ICMP service used by of the packet that generated the record.
Interface: Firewall network interface through which the packet was received.

- **Other protocols**

Record format:

```
<Date> <Time> - <Repetition> <Action> <Protocol> <Status> <Source IP>
<Destination IP> <Interface>
```

Fields description:

Date: Record generation date.
Time: Record generation time.
Repetition: Number of times the record was consecutively repeated. This field is shown between parentheses in the command line interface.
Status: This field, seen between parentheses in the command line interface, uses up to three independent letters. They are:

A: Authenticated packet
E: Encrypted packet
S: Packet using SKIP or AKER-CDP key exchange

Action: This field indicates the action executed by the firewall with each packet. It may have the following values:

A: Packet accepted by the firewall
D: Packet discarded by the firewall
R: Packet rejected by the firewall

Protocol: Protocol name of the packet that generated the record (if the firewall cannot recognize the protocol name, its number will be shown instead).
Source IP: Source IP address of the packet that generated the record.

Destination IP: Destination IP address of the packet that generated the record.
Interface: Firewall network interface through which the packet was received.

Records generated by the Network Address Translator

Record format:

```
<Date> <Time> - <Repetition> C <Protocol> <Source IP> <Source Port>
<Translated IP> <Translated Port>
```

Record fields description

Date: Record generation date.
Time: Record generation time.
Repetition: Number of times the record was consecutively repeated. This field is shown between parentheses in the command line interface.
Protocol: Protocol name of the packet that generated the record. It may be TCP or UDP.
Source IP: Source IP address of the packet that generated the record.
Source Port: Source Port of the packet that generated the record.
Translated IP: IP address to which the packet source address was translated.
Translated Port: Port to which the packet source port was translated.

13-3 Using the Command Line Interface

The command line interface for log access has similar capabilities to the GUI; however, it has more limited filtering options. Another limitation is that it is not possible, through the command line interface, to access the additional information obtained when we select a log record in the GUI, or when we activate the *Expand* option.

Program location: `/etc/firewall/fwlog`

Syntax:

```
Aker Firewall - Version 5.0
fwlog clear [log | events] [<begin_date> <end_date>]
fwlog show [log | events] [local | cluster] [<begin_date> < end_date>]
[priority]
```

Program Help:

```
Usage: fwlog help
     fwlog clear [log | events] [<begin_date> <end_date>]
     fwlog show [log | events] [local | cluster] [<begin_date> <
end_date>] [priority]


fwlog – command line interface to view log and events
     show     = displays log or events content. It may show only local
log, or whole cluster log.
     clear    = erases all log or events records.
     help     = displays this content.
For the show command, we have:
     begin_date  = first date from which records will be shown
     end_date    = last date until which records will be shown
                   (Dates must be follow the mm/dd/yyyy format.
                   If dates are not entered, current date will be
used, i.e.,
                    today's records will be shown.)
     priority    = Optional field. When informed, it must have one of
the following values:
                   ERROR, WARNING, NOTICE, INFORMATION, or DEBUG
                   (Only records with the specified priority level
will be listed.)
```

Example 1: (showing log of day 07/07/2003)

```
#fwlog show log 07/07/2003 07/07/2003

07/07/2003 19:06:54 (01) D UDP 10.4.1.126 137 10.4.1.255 137 de0
07/07/2003 19:06:47 (01) D UDP 10.4.1.120 138 10.4.1.255 138 de0
07/07/2003 19:06:35 (01) D UDP 10.4.1.210 138 10.4.1.255 138 de0
07/07/2003 19:06:22 (01) A TCP 10.4.1.24 1027 10.5.1.1 23 de0
07/07/2003 19:06:21 (02) R TCP 10.4.1.2 1028 10.7.1.14 79 de0
07/07/2003 19:06:21 (01) A ICMP 10.5.1.134 10.4.1.12 8 de1
07/07/2003 19:06:20 (01) A ICMP 10.4.1.12 137 10.5.1.134 0 de0
07/07/2003 19:06:02 (01) A UDP 10.4.1.59 1050 10.7.1.25 53 de0
```

Example 2: (showing log of day 07/07/2003, only the "notice" priority level)

```
#fwlog show log 07/07/2003 07/07/2003 notice

07/07/2003 19:06:54 (01) D UDP 10.4.1.126 137 10.4.1.255 137 de0
07/07/2003 19:06:47 (01) D UDP 10.4.1.120 138 10.4.1.255 138 de0
07/07/2003 19:06:35 (01) D UDP 10.4.1.210 138 10.4.1.255 138 de0
07/07/2003 19:06:21 (02) R TCP 10.4.1.2 1028 10.7.1.14 79 de0
```

Example 3: (erasing the log file)

```
#fwlog clear log 10/21/2003 10/23/2003
Records removal was requested to the log server
```

14-0 Viewing System Events

We will show in this chapter, how to view system events. A very useful resource to track firewall operation, and to detect possible attacks and configuration errors.

What are system events?

Events are high level firewall messagesl, i.e., those not directly related to packets (as logs are). In events, there may be messages generated by one of the three large modules (Packet Filter, Network Address Translator, and Authentication/Encryption), and also by any other firewall component, such as proxies and server processes in charge of specific tasks.

Basically, the type of information available varies from useful system tracking messages (generated, for example, every time the machine is restarted, or every time a session is established with the firewall, etc.) to more critical configuration and execution error messages.

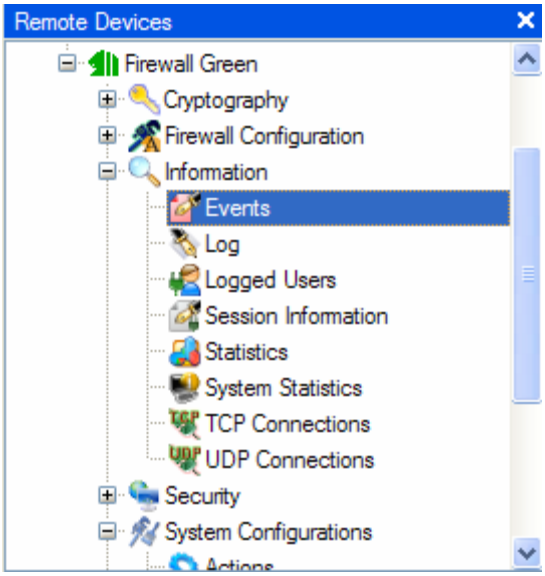
What is an event filter?

Despite being configured to record every possible event, the security system usually must provide, specific information, comparatively minute in volume (for example, all messages issued yesterday). The event filter is a mechanism offered by Aker Firewall to create logical views of the total set of event messages, facilitating access to the desired information.

Only information previously recorded in the events will be viewed through the filter. To obtain a certain type of information, it is necessary first to configure the system to record it, and then, use a filter to view it.

14-1 Using the Graphic User Interface

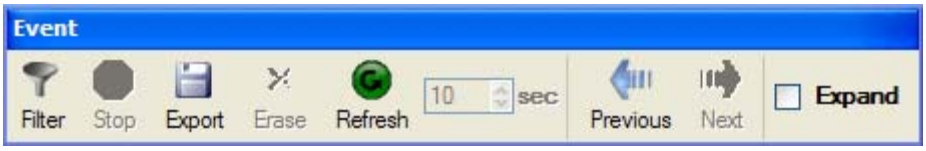
To access the Events Window, do the following:



- Click on the *Information* menu of the firewall you want to view the events
- Select *Events* option

The Events toolbar

When the *Events* option is selected, its toolbar shows up. Located next to the other bars, it can be dragged and left floating on top of Events information. It looks like this:



Legend:

 Opens the Firewall Event Filter Window

 This icon is only enabled when the firewall is performing an event search. It is used to stop the search.

 Exports events into several file types

 Deletes firewall events


Refreshes the filtered log screen within the specified time period (see next icon).

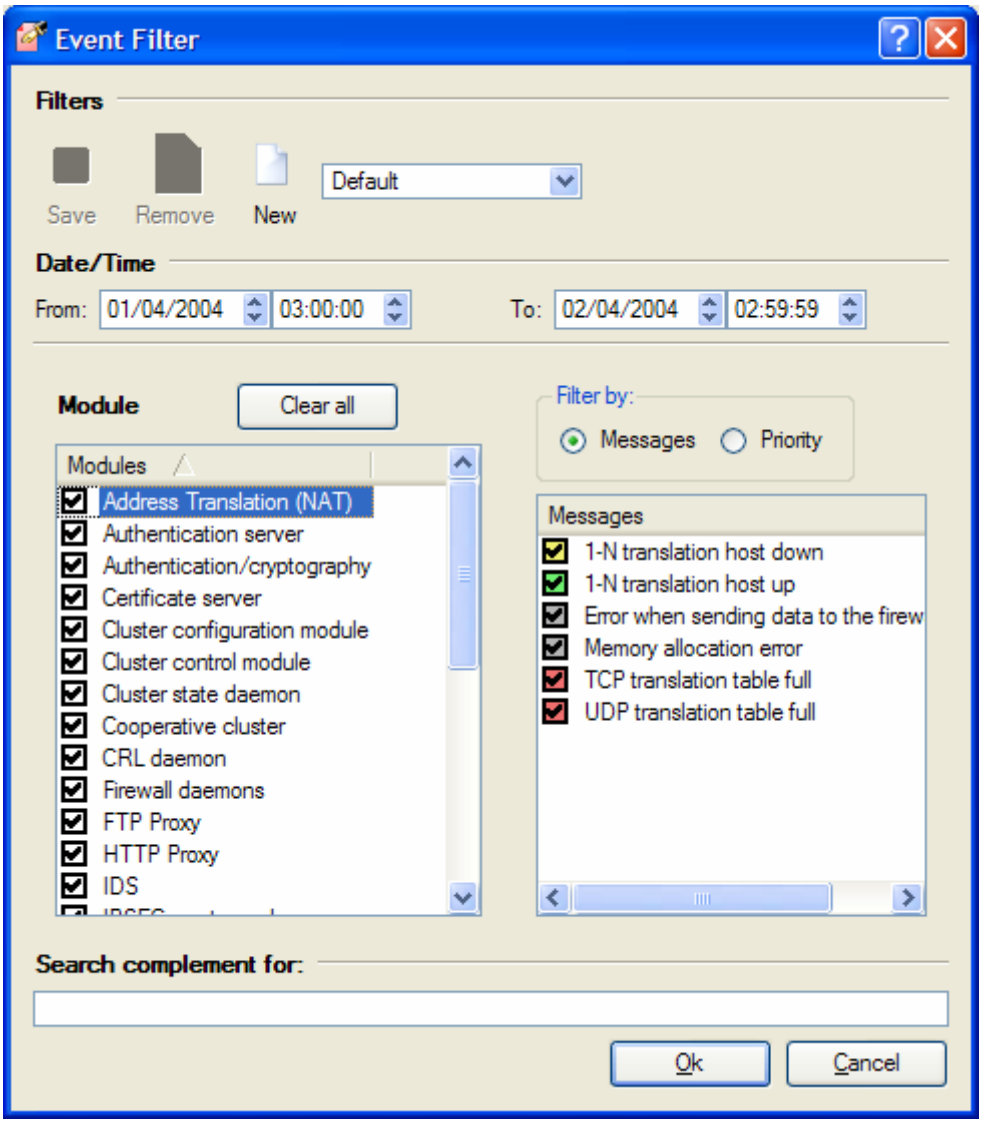
Sets log screen refresh time interval.


Goes backward and forward in the events list.

Expands events messages, displaying maximum available information

The window below shows up when the Filter icon is selected:

The Events Filtering Window



The **Save**, **Remove**, and **New** buttons are located on the top part of the window. A new search filter may be saved, used at a later time by the administrator, and removed when no longer needed

To save an events filter, do the following:

1. Modify fields as needed.
2. Type in the name of the new filter in the **Filters** area.
3. Click on Save.

To apply a saved filter, select its name in the **Filters** area. All fields will be automatically filled with the saved data.

To delete a filter, do the following:

1. Select the filter to be removed in the **Filters** field.
2. Click on Remove.

The default filter is configured to show all messages of the current day. To view other days' messages, set the From/To fields, in the Date/Time area accordingly..

In addition to the date criterion, it is also possible to filter messages to be shown according to their generating module or by their Priority. In the **Filter** by option, you can choose between the Messages or the Priority lists.

- **Message filtering**

When the option Filter by Messages is selected, a list of all firewall modules is displayed on the left side of the window. When a module is selected, a list of all the different messages that module can generate is displayed on the right.

Hint: To select all messages of a module, click on the box next to it.

- **Priority filtering**

Different types of messages have different priorities. The higher the priority of a record, the more important it is.

When the option Filter by Priority is selected, a list of all firewall modules is displayed on the left side of the window. When a module is selected, a list of all the different message priorities it may generate is displayed on the right.

All possible priorities, ordered by importance level, are explained below. (If the firewall is configured to send a copy of the events to the syslogd, the priorities with which the messages are generated in the syslog will be the same as below.)

- Error

Records matching this priority level indicate some type of configuration or system operation error (insufficient memory, for example). Messages with this priority level are unusual and must be handled immediately.

- Warning

Indicates some type of serious, atypical situation (remote user validation failure, for example).

- Notice

Records with this priority level have information considered important to the system administrator, but are associated to routine situations (for example, an administrator initiated a remote session).

- Information

These records add useful, although not vital, information to the Firewall administration (for example, the end of a remote administration session).

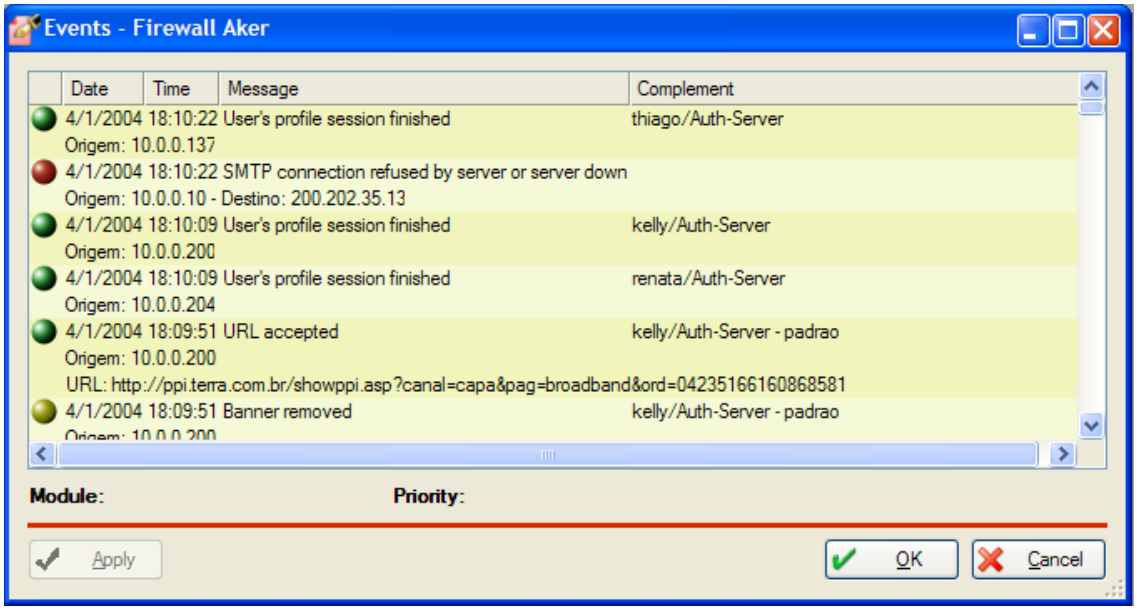
- Debug

Records with this priority level have the least important information, except for audits. Examples of these types of messages are those generated by the remote administration module, every time the firewall configuration is modified, or when the firewall is reinitialized.

As a final filtering resource, there is the **field Search complement for**. It is used to specify a text that must be present in messages complements. Only messages complements containing this text will be shown. This feature enables viewing all WWW pages accessed by a certain user, just by inputting the user's name in this field.

- The **OK** button applies the chosen filter, and displays the Events Window with the selected information.
- The **Cancel** button cancels the filtering operation, and the Events Window is shown with previous unmodified information.

The Events Window



The Events Window is displayed after a new filter is applied. It has a list with several messages. Usually, each line corresponds to a different message, however, there may be messages with 2 or 3 lines. Message format will be explained in the next session.

Important observations:

- Messages will be shown 100 at a time.
- Only the first 10,000 messages matching the chosen filter will be shown. The remainder can be seen by exporting events to a file, or by using a filter that generates less events.
- To the left of each message, a colored icon will be displayed, representing its priority. Icon color legend is shown below:

Blue	Debug
Green	Information
Yellow	Notice
Red	Warning
Black	Error

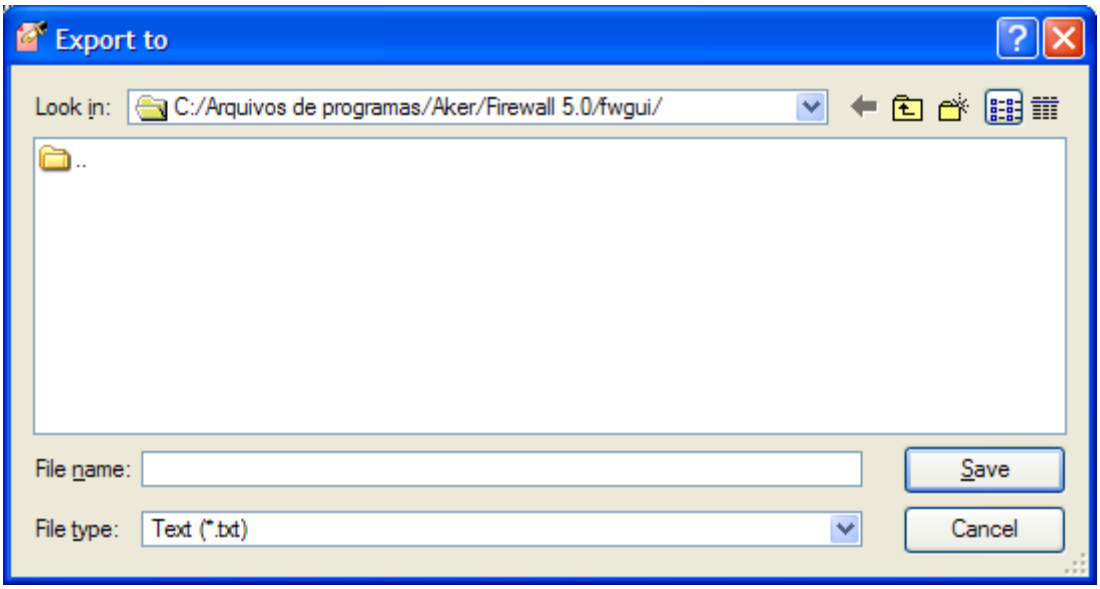
- Additional information about a message can be obtained by clicking on it.

 If all events are deleted, the only way to recover the information is restoring a backup copy.

- The **Save** button, located in the toolbar, saves all information selected by the current filter either in a text file format, or in formats that allow them to be imported by Aker and WebTrends(R) log analyzers. These files will have several lines of the same content displayed in the window.

 Events will be exported together with their additional messages if the *Expand* option is checked, and the option to export file of text type is chosen. Otherwise, the events will be exported without the messages..

This option is very useful when you want to send a copy of the log to someone else, to keep a text copy of important information, or to import a log by one of the log analyzers cited above. The following window will show up when the Export button is pressed.



To export the log content, name the file to be created, choose its type, and click on **Save**. To cancel the operation, click on **Cancel**.

If a file with the same name already exists, it will be erased..

- The **Next 100** button, represented by a right pointing arrow in the toolbar, shows the next 100 records selected by the filter. If there are no more records, this option is disabled..
- The **Previous 100** button, represented by a left pointing arrow in the toolbar, shows the previous 100 records. If there are no previous records, this option is disabled.
- The **Help** button shows specific help for the Log Window.

14-2 Format and Meaning of the Fields of Event Messages

Below, there is a description of each message format, followed by a description of each of its fields. A complete list of all possible messages and their meanings can be found in Appendix A.

Record format

<Date> <Time> <Message> [Complement]
[Complementary message 1]
[Complementary message 2]

Fields description:

Date: Record generation date.
Time: Record generation time.
Message: Text message describing what happened.
Complement: This field contains additional information. It may or may not show up, depending on the message. In the command line interface, if it shows up, it will be between parentheses.
Complementary message 1 and 2: These complements only exist in case of messages related to connections handled by transparent and non-transparent proxies. They are always displayed in the line below the main message. Complementary messages contain connection source address, and, in case of transparent proxies, the destination address

14-3 Using the Command Line Interface

The command line interface for events access has similar capabilities to the graphical user interface. All GUI functions are available, except for the message filtering option. Another limitation is that it is not possible, through the command line interface, to access the additional information obtained when we select events message in the GUI, or when we activate the *Expand* option.

The software program that supports the events' command line interface is the same one used with the log interface, and was also explained in the previous chapter.

Localização do programa: `/etc/firewall/fwlog`

Syntax:

```
Aker Firewall - Version 5.0
fwlog clear [log | events] [<begin_date> <end_date>]
fwlog show [log | events] [local | cluster] [<begin_date> < end_date>]
[priority]
```

Program Help:

```
Usage: fwlog help
     fwlog clear [log | events] [<begin_date> <end_date>]
     fwlog show [log | events] [local | cluster] [<begin_date> <
end_date>] [priority]

fwlog – command line interface to view log and events
     show     = displays log or events content.  It may show only
local log, or all
                cluster log.
     clear    = erases all log or events records
     help     = displays this message
For the "show" command, the following parameters are available:
     begin_date  = first generation date of records that will be shown
     end_date    = last generation date of records that will be shown
                   (Dates must follow the mm/dd/yyyy format.
                  If dates are not informed, current date will be
used, i.e.,
                   today's records will be shown.
     priority    = optional field. When provided, it must have one of
the following
                   values:  ERROR, WARNING, NOTICE, INFORMATION, or
DEBUG
                   Only records with the specified priority level will
be listed.)
```

Example 1: (showing events from date 10/07/2003 to date 10/08/2003)

```
#fwlog show events 10/07/2003 10/08/2003

10/08/2003 11:39:35 Administrative session closed
10/08/2003 09:13:09 Administrative session established (administrator,
CF CL GU)
10/08/2003 09:13:09 Administrative session request (10.4.1.14)
10/08/2003 09:09:49 Operation on log file (Compact)
```

```
10/07/2003 10:27:11 Aker Firewall v5.0 - Initialization complete
10/07/2003 08:57:11 UDP translation table full
```

Example 2: (showing events from date 10/07/2003 to date 10/08/2003, only with debug priority level)

```
#fwlog show events 10/07/2003 10/08/2003 debug

10/08/2003 09:09:49 Operation on log file (Compact)
10/07/2003 10:27:11 Aker Firewall v5.0 – Initialization complete
```

Example 3: (erasing events file content)

```
#fwlog clear events 21/10/2003 23/10/2003

Records removal requested to log server.
```

15-0 Viewing Statistics

In this chapter, we will explain the statistics of Aker Firewall and its characteristics.

What is the Aker Firewall Statistics Window?

In the Firewall, statistics are means of measuring data traffic through its interfaces. This traffic is translated into numbers that represent the total amount of packets sent or received, and the total number of bytes transported.

With this information, the administrator is able to relate data flow to each service, and will know whether the network physical environment needs to be improved or expanded.

Network billing is another use for this type of information. Each network host is charged according to the amount of bytes they transfer.

To perform network billing, a filtering rule with a different counter for each host must be configured. Counters must have statistical rules associated to them. These rules are configured in the Statistics Window.

How Aker Firewall Statistics work ?

The functioning of Aker Firewall statistics are based on three distinct steps:

- Creation of counters

In this step, it is necessary to create the counters that will be associated with filtering rules. They serve only as totalizers for one or more filtering rules. For more information about the creation of counters and their association with filtering rules, refer to chapters Registering entities and The stateful filter.

- Creation of statistical rules

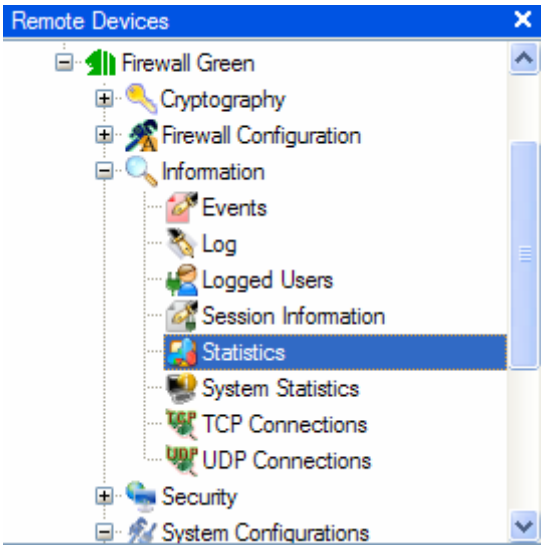
After the creation of counters and their association with the desired filtering rules, it is necessary to create statistical rules that define the poll interval and which counters will be summed up to generate the value of the statistic on a given time. This step will be explained later on this chapter.

- Visualization of statistics

After the creation of statistical rules, it is possible to view the values associated with any of the rules, export them or plot graphics. This step will also be explained on this chapter.

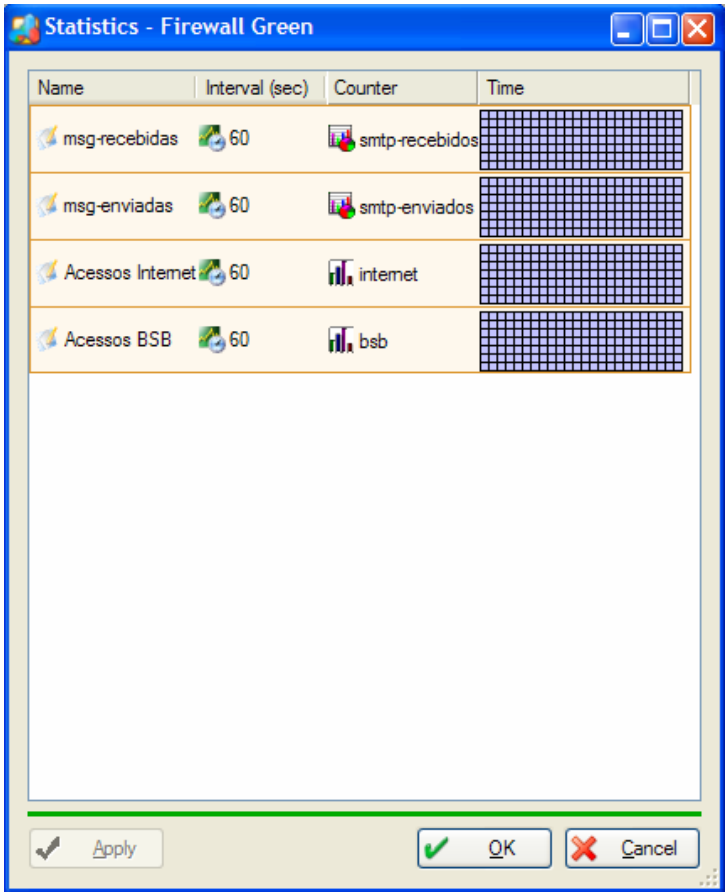
15-1 Using the Graphic User Interface

To access the Statistics Configuration Window, do the following:



- Click on the *Information* menu in the firewall window you want to manage
- Select *Statistics*

The Statistics Window



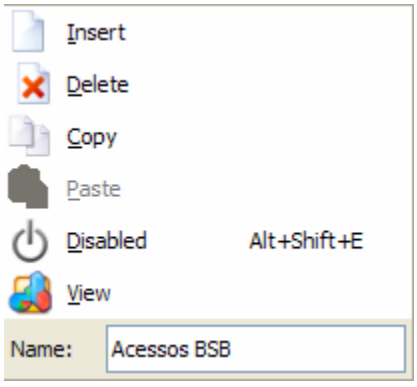
The statistics window has all the statistical rules defined in Aker Firewall. Each rule is displayed in a separate row, made up of several cells. Selected rules are displayed on a different color.

- The **OK** button updates the set of statistics and immediately enables them.
- The **Cancel** button discards all modifications and closes the window.
- The **Apply** button sends all modifications to the firewall and keeps the window open
- The scrollbar to the right is used to view the rules that do not fit the window.

Each statistic rule is composed of the following fields:

- **Name:** Statistical rule name; to facilitate referencing. Each statistic rule must have a unique name within the rules set.
- **Interval:** Corresponds to the time interval when the totalling of the rule will be made, that is, the sum of the values of all counters present in the rule.
- **Counter:** This field establishes which counters will be summed up in this rule to generate the values of the rule.
- **Time:** This table defines date and time when the rule will be applicable. Rows represent weekdays, and columns, hours. To apply the rule at a specific time, check the box corresponding to it. Otherwise, leave it blank.

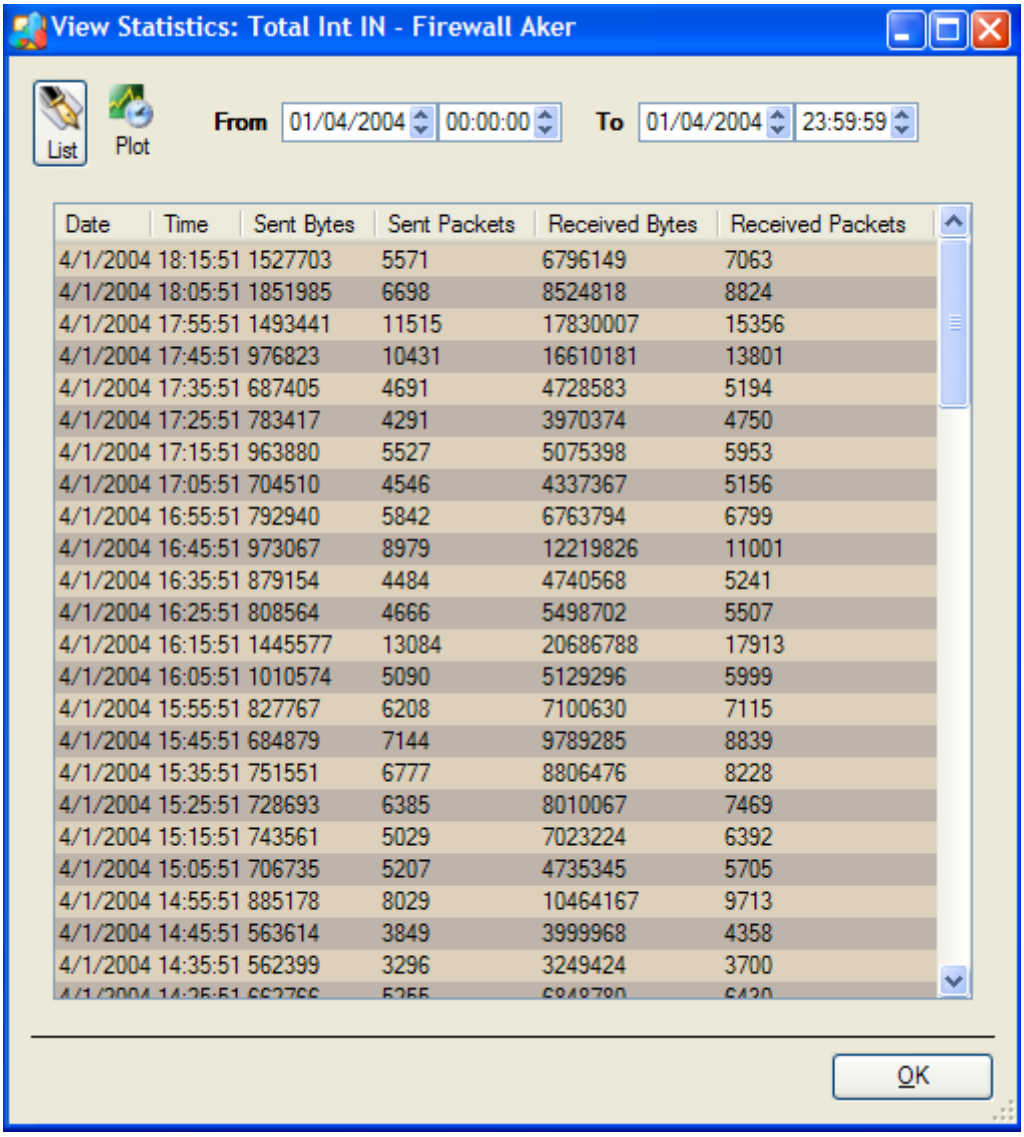
To interact with each rule, use the toolbar located on the top part of the window or right-click on it.



- **Insert:** This option allows the addition of a new rule into the list.
- **Delete:** Removes the selected rule from the list.
- **Copy:** Copies the selected rule into a temporary area.
- **Paste:** Copies the rule from the temporary area into the list. If any rule is already selected, the new one will be copied onto its position. Otherwise, it will be copied at the end of the list.
- **Enable/Disable:** This option activates or deactivates the selected rule.
- **View:** Displays the View Statistics Window corresponding to the selected rule.
- **Name:** Renames the rules.

The Visualization Statistics Window

When the **View** button is clicked or when a rule is double-clicked, the following window will be displayed:

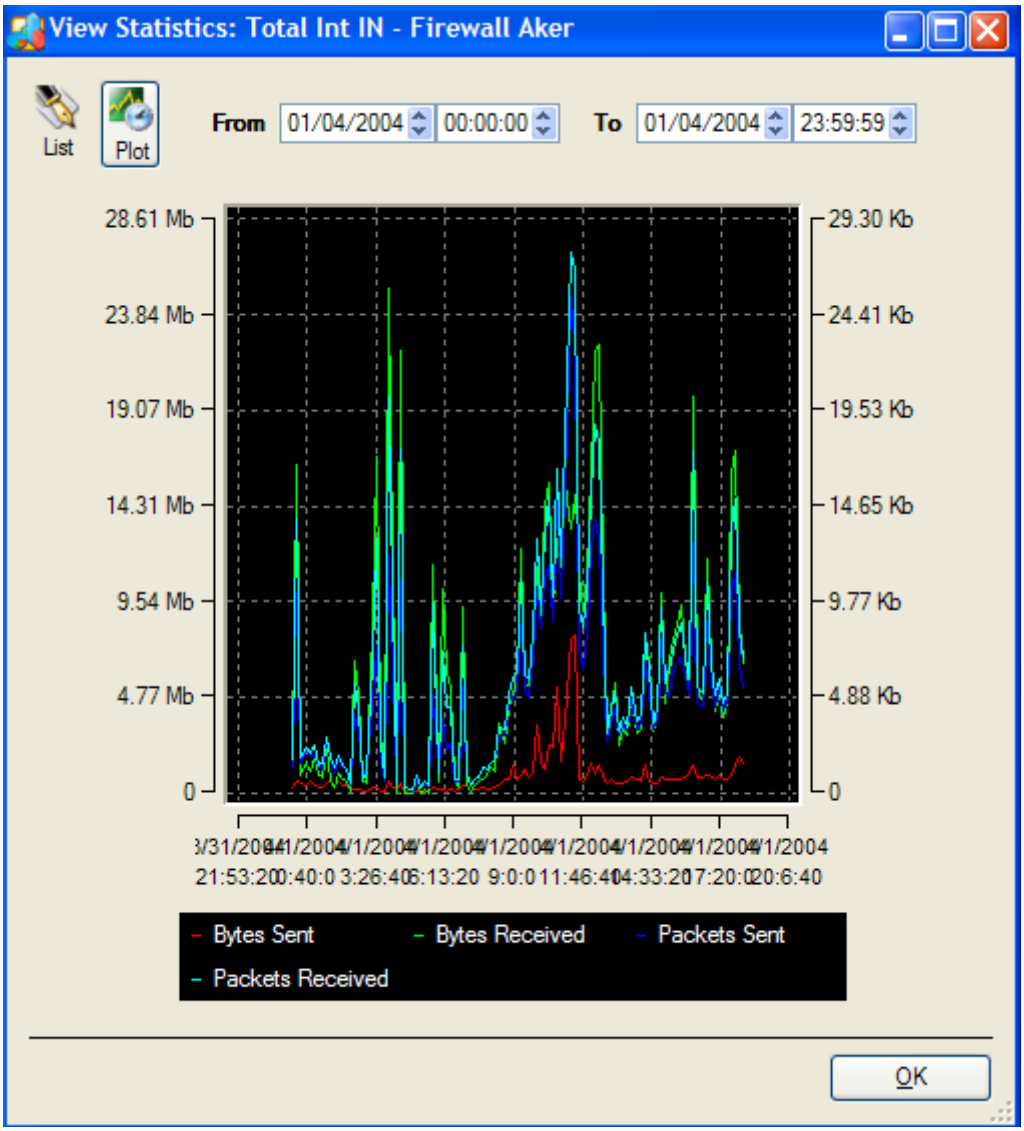


In this window, selected statistics data can be viewed graphically  or in text format  . The stats presented will correspond to a time period specified at the top. To alter it, select the **Date** field and input start/ending dates.

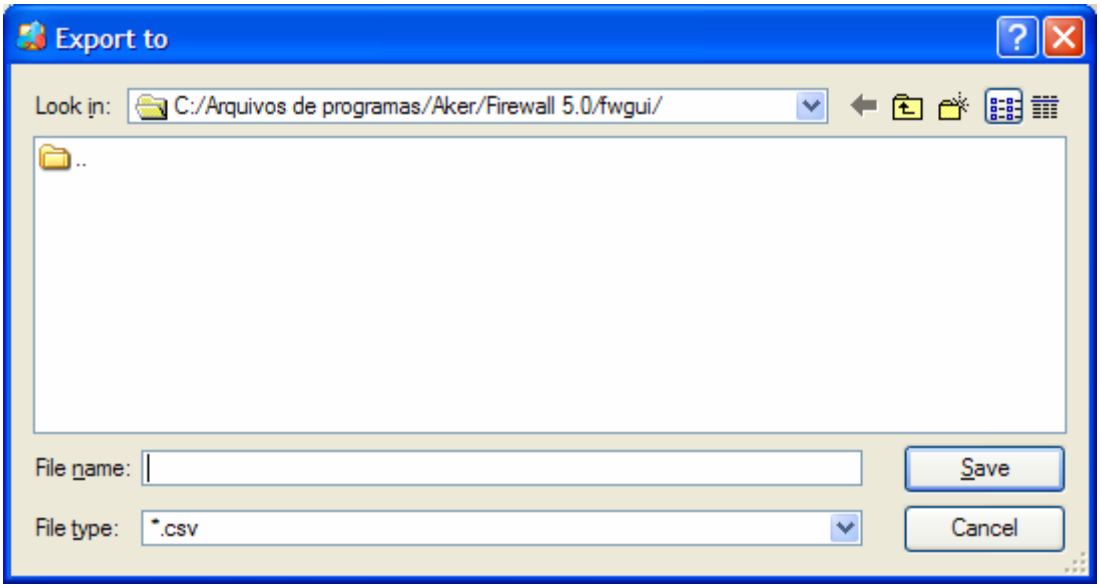
- **Reading:** Displays a set of 100 records at a time. Each record refers to the reconciling of counter stats during a specific time period.

  The **Remove** button  deletes the set of records within the specified time period.

- **Plot:** Represents the **Reading** folder data in graphical format. Graphics are generated when this button  is pressed. It allows the user to select which lines will be displayed, by pressing legend buttons.

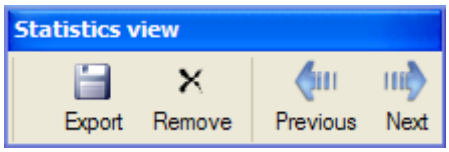


When the Save Statistics button is pressed  the following window is displayed. This file is recorded in CSV format, enabling manipulation through spreadsheet programs.



The Statistics Visualization Toolbar

The Statistics toolbar provides the following functions:



 - The Save Records button saves and exports counter generated data.

 - This button deletes selected records generated by the counters.

 - This is the navigation button of the data generated by the counters displayed by the statistics.

15-2 Using the Command Line Interface

The command line interface to handle statistics has similar capabilities to the graphical user interface. All functions are available, except for graphical data verification, as well as, which and where are the rules included in a counter.

To view the timetable do the following:

The : (colon) indicates that the rule is valid for both weekdays that appear separated by a slash (/). For example: Sun/Mon.
The . (period) indicates that rule is only valid for the weekday written after the slash (/). In the above example, Sun/Mon, it would be valid for Monday only.
The ' (apostrophe), or single quotes, indicates that the rule is only valid for the weekday written before the slash (/). This way, in Sun/Mon, it would be valid for Sunday only.

Program location: `/etc/firewall/fwstat`

Syntax:

```
fwstat help
       show [[-c] <statistic> [<initial date> <final date>]]
       include <statistic> <period> [<counter1> [counter2] ...]
       remove <statistic>
       disable <statistic> [<day> <hour>]
       enable <statistic> [<day> <hour>]
```

Program Help:

```
Aker Firewall - Version 5.0
Usage: fwstat help
              show [[-c] <statistic> [<initial date> <final date>]]
              include <statistic> <period> [<counter1> [counter2] ...]
              remove <statistic>
              disable <statistic> [<day> <hour>]
              enable <statistic> [<day> <hour>]

       help      = shows this message
       show      = with no parameters, lists all firewall statistics
                   with the following parameters, shows the collected
       statistic = statistic name
       -c        = outputs in CSV (comma separated value) format
                   (usefull to import data in spreadsheets)
       dates     = boundary dates for statistic output
       include   = adds a new statistic named "statistic"
       remove    = removes a statistic named "statistic"
       period    = data collection period (seconds)
       counter_n = name of the counter entities to collect
       disable   = disables a statistic
       enable    = enables a statistic
       day, hour = if specified (alway both) enables or disables
                   only for the specified time. 'day' is one of:
                   {sun, mon, tue, ...} and 'hour' is one of {0..23}
```

Example 1: (showing statistics)

```
#fwstat show
Name  : statistics1                                        (enabled)
----
Period : 17400 seconds (s)
Counters: a1
Time:
Day\Time|0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20
21 22 23
-------------------------------------------------------------------------
---------
Sun/Mon |:  :                          :  :  :  :  :  :  :  :  :  :
:  :  :  :
Tue/Wed |:  :                          :  :  :  :  :  :  :  :  :  :
:  :  :  :
Thu/Fri |:  :                          :  :  :  :  :  :  :  :  :  :
:  :  :  :
Sat     |'  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '
'  '  '  '

Name  : statistics2                                        (enabled)
----
Period  : 100  seconds(s)
Counters: a1  a11
Time:
Day\Time|0  1  2  3  4  5  6  7  8  9 10 11 12 13 14 15 16 17 18 19 20
21 22 23
-------------------------------------------------------------------------
---------
Sun/Mon |:  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :
:  :  :  :
Tue/Wed |:  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :
:  :  :  :
Thu/Fri |:  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :  :
:  :  :  :
Sat     |'  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '  '
'  '  '  '
```

Example 2: (showing statistics from date 10/28/2001 to date 10/29/2001)

```
#fwstat show statistics 10/28/2001 10/29/2001
Day          Time       Sent (bytes/packets)      Received
(bytes/packets)
-------------------------------------------------------------------------
-
10/29/2001 17:24:54          320/1                     321/1
10/29/2001 17:23:14          652/6                     654/6
10/29/2001 17:21:34          234/2                     980/9
10/29/2001 17:19:54          324/3                     650/6
10/29/2001 17:18:14          325/3                     150/1
10/29/2001 17:16:34          985/9                     240/2
10/29/2001 17:14:54          842/8                     840/8
10/29/2001 17:13:14          357/3                     289/2
10/29/2001 16:58:14          786/7                     261/2
```

16-0 Viewing and Removing Connections

This chapter shows how to view and remove TCP connections and UDP sessions in real- time.

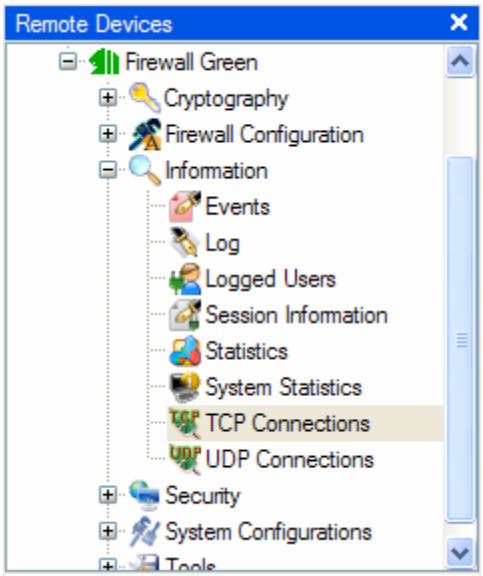
What are active connections?

Active connections are TCP connections or UDP sessions which are active through the Firewall. Each one of these connections has been validated through a stateful filter rule, which has been added by the system administrator, or through an entry in the state table, automatically added by Aker Firewall.

For each of these connections, the firewall keeps a lot of information in its state tables. Some of these piece of information are especially useful to the administrator and they can be viewed at any moment through the active connections window. This information contains the exact hour of establishment of the connections and their idle time, that is, the amount of time that no packets passed through them.

16-1 Using the graphic user interface

In order to access the active connection window, the following steps must be taken:



- Click on *Information* menu on the firewall you want to view the connections
- Select *TCP Connections* or *UDP connections*

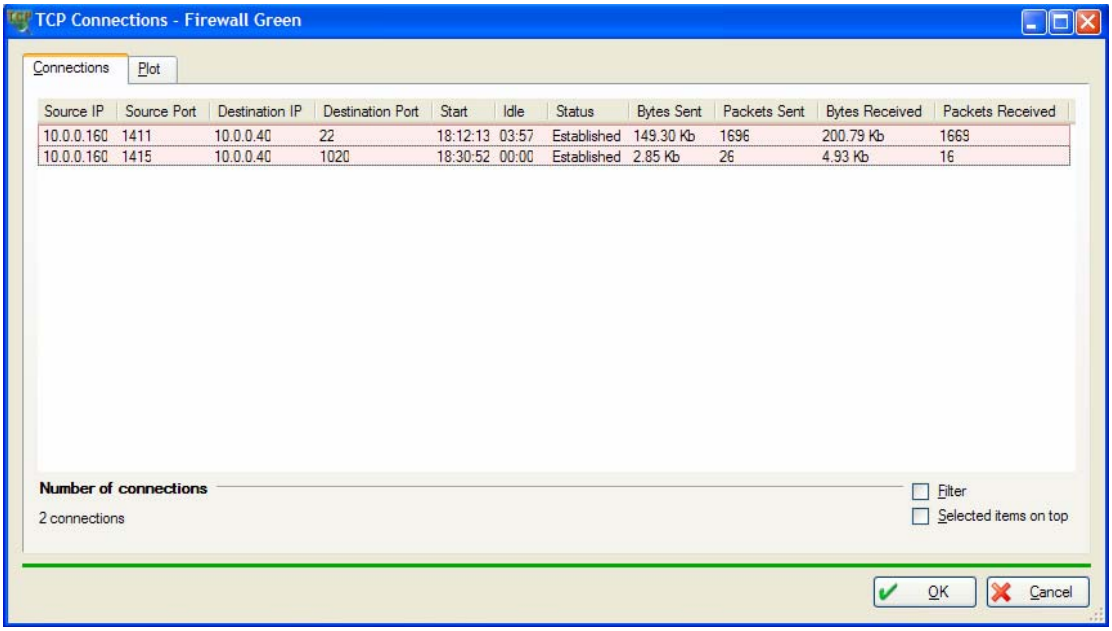
The active connections window

The active connections window is where all the connections that are running through the firewall, during a specific moment, can be viewed. The windows for the TCP and UDP protocols are identical, except for the field called **Current State,** which only exists in the TCP connections window.

In order to simplify the understanding, TCP and UDP connections are often mentioned; however, this feature is not real due to the fact that the UDP protocol is not connection oriented. In fact, the meaning of the UDP connection term is an UDP session where a two-way traffic takes place. Each session can be seen as a set of request and response packets which go through the firewall to a specific service, provided by one host and accessed by another.

This window consists of two tabs: the first tab shows a list with the active connections and the second tab displays a real-time graphic with the most used hosts and services.

- **The connections tab**

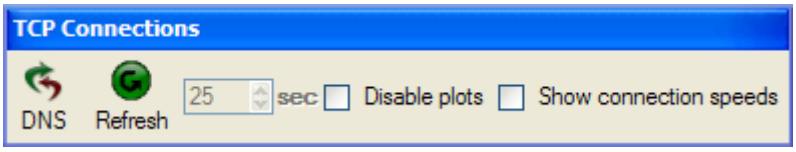


This tab consists of a list with an entry for each active connection. A message with the total number of active connections at a specific moment is shown at the bottom of the window.

- The **OK** button will close the active connections window.
- The **Filter** option shows the filtering options, enabling the selection of source or destination addresses and/or ports to be displayed in the window.
- The **Selected itens on top** option displays the selected connections on the top of the window, for better visualization
- The **Delete** option, displayed when the right mouse button is clicked on a connection, will remove the selected connection.

When a TCP connection is removed, the firewall sends reset packets to the hosts which are taking part in the connection, effectively dropping it, and removes the entry from its state table. In case of UDP connections, the firewall

simply removes the entries from its state table, prohibiting then, the acceptance of packets to the removed connections.



- The **Refresh** button, located on the toolbar, will activate (or deactivate) the automatic refresh of the displayed information, which is enabled by default. The first time this button is clicked, the automatic refresh will be deactivated. To reactivate it, just click on it again. The refresh interval can be configured by changing the value on the right of this button.

- The **DNS** button, located on the toolbar, will trigger the domain name system (DNS) to resolve the names of the hosts whose IP addresses are listed. The following should be mentioned:

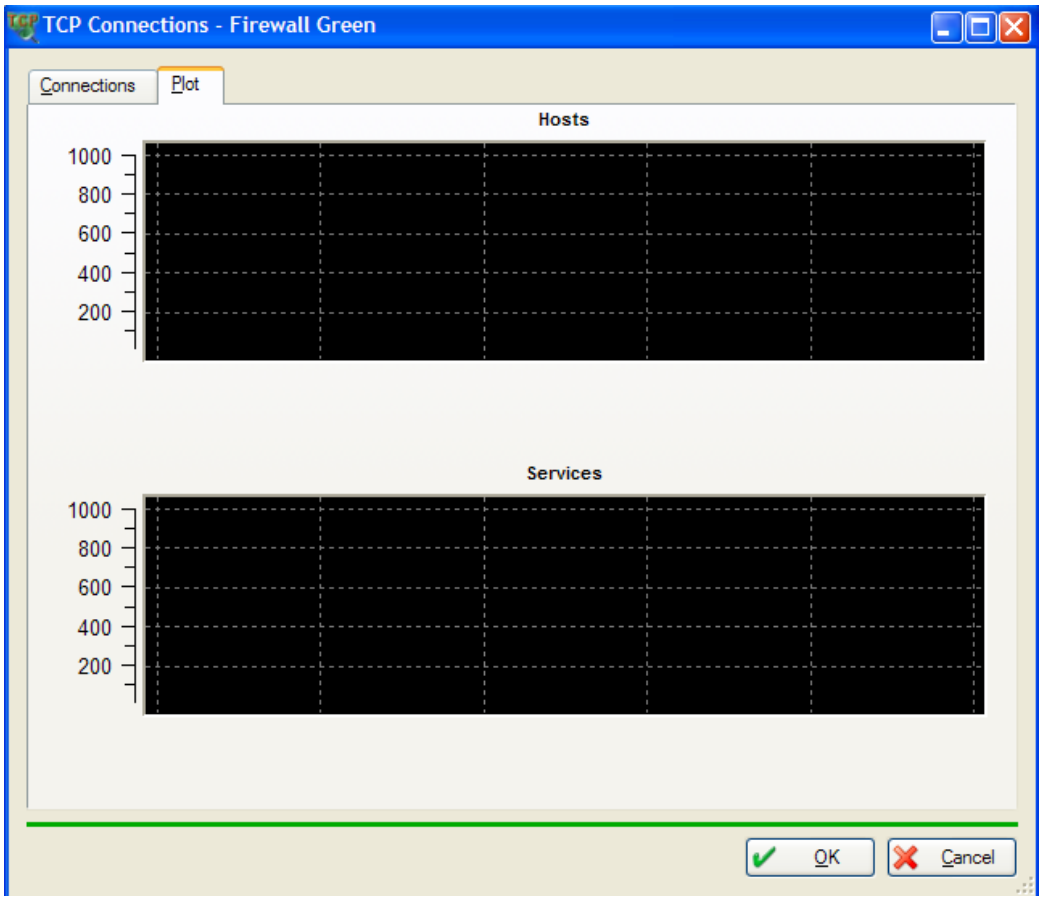
1. The name resolution is very often a slow service, and because of this trait, the resolution is performed in the background.
2. Many times, due to reverse DNS configuration problems (which is used to resolve names from IP addresses), the resolution of certain addresses won't be possible. In such case, the addresses which have not been resolved will be kept in their original form and it will be indicated, besides them, that they don't have a reverse DNS configured.

- The **Disable plots** option disables the plotting of the connections graphic and it is useful for slow speed computers

- The **Show connection speeds** option, if enabled, causes the interface to calculate and show each connection speed in bits/s.

- It is possible to sort the connection list by any of its fields, being just necessary to click on the field title. The first click will generate an ascending sort and the second will reverse the list.

- **The plot tab**



This tab consists of two graphics: the upper one shows the most used services and the lower one shows the most accessed hosts. In the right side there is a caption showing which host or service correspond to which graphic color.

The time interval of the graphic is the same as the one configured for the connections tab

The meaning of the fields of an active connection

Each line of the active connections list represents one connection. The meaning of its fields is the following:

Source IP: IP address of the host which initiated the connection.

Source port: Port used by the source host to establish the connection.

Destination: IP address of the host which the connection was established to.

Destination port: Port which the connection has been established to. This port is usually associated with a specific service.

Start: Connection establishment time.

Idle: Number of minutes and seconds the connection is idle.

Status: This field is displayed only in case of TCP connections. It represents the connection state at the moment it is displayed. It can have the following values:

SYN Sent: It indicates that the connection request packet (packet with the SYN flag) has been sent, however, the server has not responded yet.

SYN Exchanged: It indicates that the connection request packet has been sent and the server has responded with a confirmation that the connection has been accepted.

Established: It indicates that the connection is established.

Listening at port: It indicates that the server is listening at the indicated port, waiting for a connection from the client. This state only occurs for FTP data connections.

Bytes sent/received: These fields appear only in case of TCP connections and indicate the amount of bytes that passed through a connection in both directions.

Packets sent/received: These fields appear only in case of TCP connections and indicate the number of packets that passed through a connection in both directions.

16-2 Using the command line interface

The command line interface allowing access the active connection list holds the same capacities of the graphic user interface. The same program deals with both TCP and UDP connections.

Program: `/etc/firewall/fwlist`

Syntax:

```
fwlist help
fwlist show [[-w] [TCP]] | [UDP] | [sessions]
fwlist remove [TCP | UDP] Source_IP Source_Port Dest_IP Dest_Port
fwlist remove session Source_IP
```

Program help:

```
fwlist - Lists and removes active TCP/UDP connections or sessions
Usage: fwlist help
       fwlist show [[-w] [TCP]] | [UDP] | [sessions]
       fwlist remove [TCP | UDP] Source_IP Source_Port Dest_IP
Dest_port
       fwlist remove session source_IP

       help   = shows this message
       show   = lists the active connections or sessions
       remove = removes an active connection or session
```

Example 1: (listing the TCP active connections)

```
#fwlist show TCP

Source(IP:port)      Destination(IP:port)  Start    Idle    State
-------------------------------------------------------------------------
10.4.1.196:1067      10.4.1.11:23          15:35:19 00:00
Established
10.4.1.212:1078      10.5.2.1:25           15:36:20 00:10
Established
```

Example 2: (listing the UDP active connections)

```
#fwlist show UDP

Source(IP:port)      Destination(IP:port)  Start    Idle
-----------------------------------------------------------
10.4.1.1:1099        10.4.1.11:53          15:35:19 00:00
10.4.1.18:1182       10.5.2.1:111          15:36:20 00:10
```

Example 3: (removing a TCP connection and listing the connections)

```
#fwlist remove tcp 10.4.1.196 1067 10.4.1.11 23

#fwlist show TCP

Source(IP:port)      Destination(IP:port)  Start    Idle    State
-------------------------------------------------------------------------
```

```
10.4.1.212:1078      10.5.2.1:25           15:36:20 00:10
Established
```

17-0 Working with Proxies

This chapter contains all the necessary knowledge to understand the Aker Firewall proxies operation. Specific details of each proxy will be discussed in the next chapters.

17-1 Planning the installation

What are proxies ?

Proxies are specialized programs that usually run in firewalls and are used as a bridge between the internal network of an organization and the external servers. Its operation is simple: they wait for a request of internal network, pass this request to the remote server in the external network and send the answer back to the internal client.

Most of the time the proxies are used by all the clients of one subnet and, due to its strategic point, they normally implement a cache system for some services. Moreover, as the proxies work with application data, a different proxy for each service is necessary.

Traditional Proxies

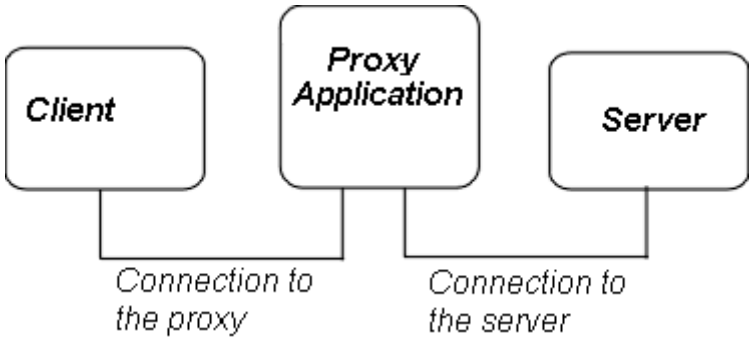
In order for a host to use the services of a proxy, the host must know that the proxy exists, that is, the host has to know that, instead of connecting to the remote server, it should connect to the proxy and pass its requests to it.

There are some clients that already have their own proxy support (most of the existent browsers can be mentioned as examples of this type of client). To use the proxy functions, in this case, it is only necessary to configure them to do it. Most of the clients, however, are not ready to work this way. If this is the case, the only possible solution is to change the TCP/IP stack in all the client hosts, in order to make that all connections be transparently passed to the proxies.

This approach brings several difficulties, apart from being extremely hard to modify all the client hosts, most of the time there is no way to modify the TCP/IP implementation of some platforms, making the clients of these platforms unable to use the proxy.

Another problem of the traditional proxies is that they can only be used for access from internal to external hosts (it is not possible to require external clients to pass their requests to your proxy in order to the proxy pass them to the internal server).

The picture bellow illustrates the basic operation of a traditional proxy:

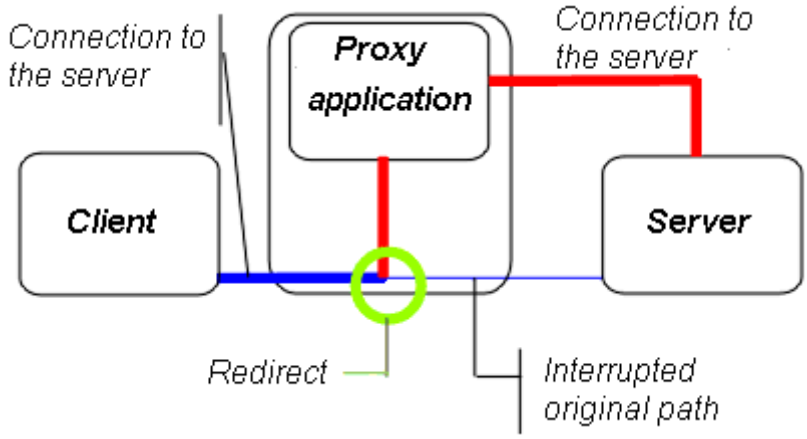


Transparent Proxies

Aker Firewall introduces a new concept of firewall, with the use of transparent proxies. These transparent proxies are capable of being used without any modification on the clients and servers, because none of them will know about their existence.

Its operation is very simple: whenever the firewall decides that an specific connection must be treated by a transparent proxy, this connection is redirected to the appropriate proxy. When the connection is received, the proxy opens a new connection to the remote server and passes the requests of the client to this server.

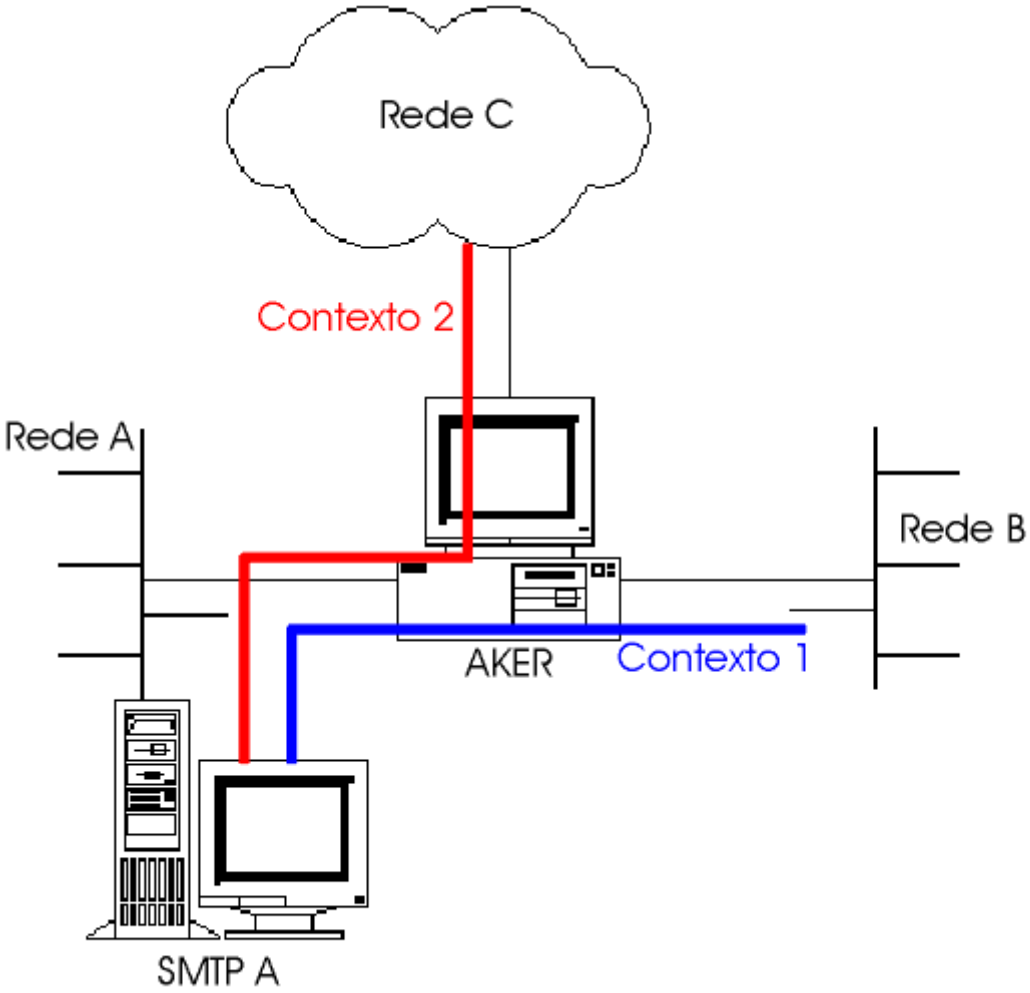
The great advantage of working like this is the possibility to offer an additional security for specific services without losing the flexibility and without modifying any of the clients or servers. Besides, it is possible to use transparent proxies in internal or external requests, indifferently.



Transparent proxies and contexts

Aker Firewall introduces a new development related to the transparent proxies: the contexts. To understand them, let's first analyze a network topology, where its existence is necessary:

Suppose there is an Aker Firewall connected to three distinct networks, called ***A***, ***B*** and ***C,*** and that the networks *A* and *B* are networks from two departments of the same company and network *C* is the Internet. Suppose there is a SMTP server shared by networks *A* and *B* to send and receive e-mails. All this is showed in the drawing bellow:



Now, suppose it is desired to configure the firewall to redirect all the SMTP connections to the SMTP proxy, in order to provide better protection and more control over this traffic.

It is important to have a way to treat distinctly the connections for **A** with *B* and *C* as sources: The network *B* will use the SMTP server of A as a relay when sending its e-mails, however the same will not be allowed from the *C* network. It can be also desired to limit the maximum size of the messages originated in the *C* network, to avoid attacks of denial of service based on lack of disc space, without, at the same time, limiting the size of the messages originated in the *B* network.

To allow this different treatment, the *contexts* concept was created. Contexts are nothing more than different configurations for the transparent proxies in order to enable different operation modes for different connections.

In the last example, two contexts could be created: one to be used in the connection from *B* to *A* and another from *C* to *A* .

Aker Firewall proxies

Aker Firewall implements transparent proxies for FTP, Telnet, SMTP, POP3 and HTTP protocols and non-transparent proxies for the services accessed through a WWW browser (FTP, Gopher, HTTP and HTTPS) and for clients that support the SOCKS protocol. To use the non-transparent proxies, a client that can be configured to do it is necessary. Among the clients that support this type of configuration are the Netscape Navigator(TM) and the Internet Explorer(TM).

The transparent proxies can be used to control external access to the internal networks as well as access from the internal network to external services. Non-transparent proxies can only be used by a host in the internal network.

Aker Firewall also allows the implementation of user defined proxies, which are proxies created by third-parties using the proxy development API that Aker Security Solutions provides. The objective is to permit that institutions that have proprietary protocols develop support in the firewall for these protocols.

Aker Firewall authenticators

Aker Firewall SOCKS, Telnet and WWW proxies support user authentication, that is, they can be configured to allow a specific session to be established only if the user identifies himself, through a name and a password, to the firewall and he is allowed to start the desired session.

The great problem with this kind of authentication is how the firewall will validate the received names and passwords. Some products require all users to be registered in a firewall database or to be valid users for the host the firewall runs on. Both methods have a great limitation because they don't use the users database usually present in a local network.

In Aker Firewall, a more versatile and simple solution has been chosen: instead of demanding the users to be registered in the firewall, they are validated in their own local network servers, either Unix or Windows NT.

For the firewall to know in which servers it must authenticate the users, and also to allow secure communication with these hosts, the concept of *authenticators* was created. Authenticators are Unix or Windows NT hosts that run a program called *Authentication Agent.* This program is distributed as part of Aker Firewall and its basic function is to serve as interface between the firewall and the remote databases.

For Aker Firewall to use a database in a remote server, you need to:

1. Install and configure the authentication agent in the host where the users database resides (this procedure will be described in the sections Installing the authentication agent in Unix and Installing authentication agent in Windows NT).
2. Register an entity of the authenticator type with the address of the host where the agent was installed and with the correct access password (for further

information on how to register an entity, refer to the chapter Registering Entities).

3. Indicate to the firewall that it must use the authenticator registered in the step 2, to perform the users authentication (this procedure will be described in the chapter Configuring the authentication parameters).

Aker Firewall 5.0 is incompatible with authenticators of versions older than 4.0. If you are upgrading from a old version and the firewall is performing user authentication, it is necessary to reinstall the authenticators.

It is also possible to perform authentication through LDAP and RADIUS protocols. In this case, there is no need to install the authenticators on the server hosts, being it enough to create the authenticators of the corresponding types and indicate to the firewall they are to be used, according to steps 2 and 3 listed above.

17-2 Installing the authentication agent on Unix platforms

To install the authentication agent, it is necessary to mount the Aker Security Suite CD-ROM in the host where it will be installed or copy the contents of the agent installation directory from the CD-ROM to some temporary directory in this host (this copy can be done by FTP or NFS, if there is no CD-ROM drive in the host where the agent will be installed).

After performing the CD-ROM mount, or the files copying to any directory, run the following command:

`#/installation_directory/en/agent/`*`plataform`*`/aginst`

Where *installation directory* is the directory where the installation files are located, *platform* is the desired platform and *directory*, the destination directory. To install, for example, the agent on the directory `/usr/local/bin`, in the FreeBSD platform and with the CD-ROM mounted in the directory `/cdrom`, the command would be:
`#/cdrom/en/agent/freebsd/aginst`

 The symbol # stands for the shell prompt while you are logged as root. Do not type it as part of the command.

The installation program will copy the agent executable file (*`fwagaut`*) to the `/usr/local/bin` directory and a configuration file model (*`fwagaut.cfg`*) to the `/etc` directory. After the installation is complete, it is necessary to customize this file, as described on the next section.

 If you answered *"Yes"* when the installation program asked if you wanted to start the agent automatically on each boot, an entry will be created on an initialization file in order to start the agent automatically. The name of this initialization file depends on the Unix flavor used.

Syntax of the configuration file of the authentication agent

After installing the authentication agent, it is necessary to create a configuration file with the addresses of the firewalls that can use it and the access passwords of each one. This file is in text format and can be created by any editor.

 The configuration file of the authentication agent must have its access rights configured in a way that only the root user can read or change its contents. To do it, the command *chmod* can be used, with the following syntax: `#chmod 600 file_name`.

Its syntax is:

- Each line must have the IP address of a Aker Firewall that will use the agent, one or more blank spaces or *tab* characters and the access password the firewall will use in the communication.
- Lines beginning with the character `#`, as well as blank lines, are ignored

An example of a possible configuration file is shown below:

```
# Configuration file for the Aker Firewall 4.00 authentication agent
#
# Syntax: Firewall IP address and access password (in each line)
#
# The password must not have spaces and must have up to 31 characters
#
# Lines beginning with the '#' character are considered comments
# Blank lines are allowed

10.0.0.1 password_test
10.2.2.2 123password321
```

 The default place for the agent configuration file is **`/etc/fwagaut.cfg`**, however it is possible to create it with any other name or in another directory, provided it is informed to the agent at startup. This will be shown in the next section.

Syntax of the execution of the authentication agent

The authentication agent for Unix has the following execution syntax:

```
fwagaut [-?] [-c FILE_NAME] [-s <0-7>] [-q]
Where:
      -? shows this message and returns to the shell prompt
      -c Specifies the name of an alternate configuration file
      -s Specifies the syslog facility where the authenticator
         messages will be sent to. 0 = local0, 1 = local1, ...
      -r Allows root user validation
      -e Accepts users with empty passwords
      -q Quiet mode. Don't show any messages upon startup
```

Suppose that the agent is located in the `/usr/local/bin` directory and the configuration file has been created with the name `/usr/local/etc/fwagaut.cfg`. In this case, to start the agent, the command line would be:

```
/usr/local/bin/fwagaut -c /usr/local/etc/fwagaut.cfg
```

If it is desired to start the agent with the configuration file on the default location, it is not necessary to use option **`-c`**, just run it with the command:

```
/usr/local/bin/fwagaut
```

 The authentication agent must be started by the root user

When any modification is made on the configuration file, it is necessary to inform this to the agent, if it is running. To do it, the following command must be run:

```
#kill -1 pid
```

Where *pid* is the process number of the authentication agent. To get this number, the command **`#ps -ax | grep fwagaut`** can be used in Unices based on BSD, or **`#ps -ef | grep fwagaut`**, in Unices based on System V.

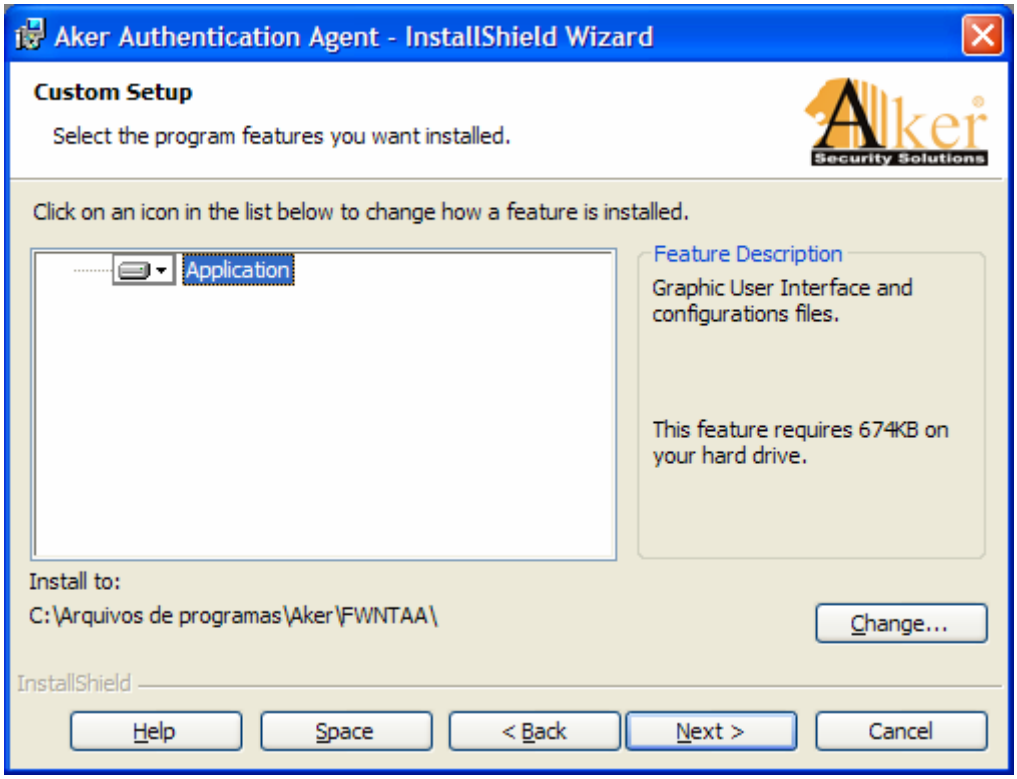
 The authentication agent listens to requests on port 1021/TCP. There can be no other application using this port while the agent is active.

17-3 Installing the authentication agent in Windows NT

The installation of the authentication agent for NT is very simple. To install it, it is necessary to insert the Aker Firewall 4.0 CD-ROM in the destination host or copy the contents of the agent installation directory of the CD-ROM to some temporary directory on this host.

Then, it is necessary to click on the *Start* menu, select the option *Run* and type the following command in the *Open* field: **`D:\en\agent\NT\setup`** (if the CD-ROM drive letter is different from **D**, replace the letter D by the equivalent letter).

The program will first display a window asking for confirmation to proceed with the installation. To continue the installation, is necessary to answer **Yes** to the question. After that a window with the license will be displayed and then the window where the installation directory can be specified. This window has the following format:



After selecting the installation directory, it is necessary to click on the **Copy files** button, which will perform the agent installation. This installation consists in the creation of a directory with the agent files, called **fwntaa**, in the **Program Files** directory, in the creation of a group called *Aker Firewall* with the configuration and agent removal options, and the creation of a service called **Aker Firewall Authentication Agent**. This service is a normal Window NT service and can be stopped or started through the *Control Panel*, in the *services* icon.

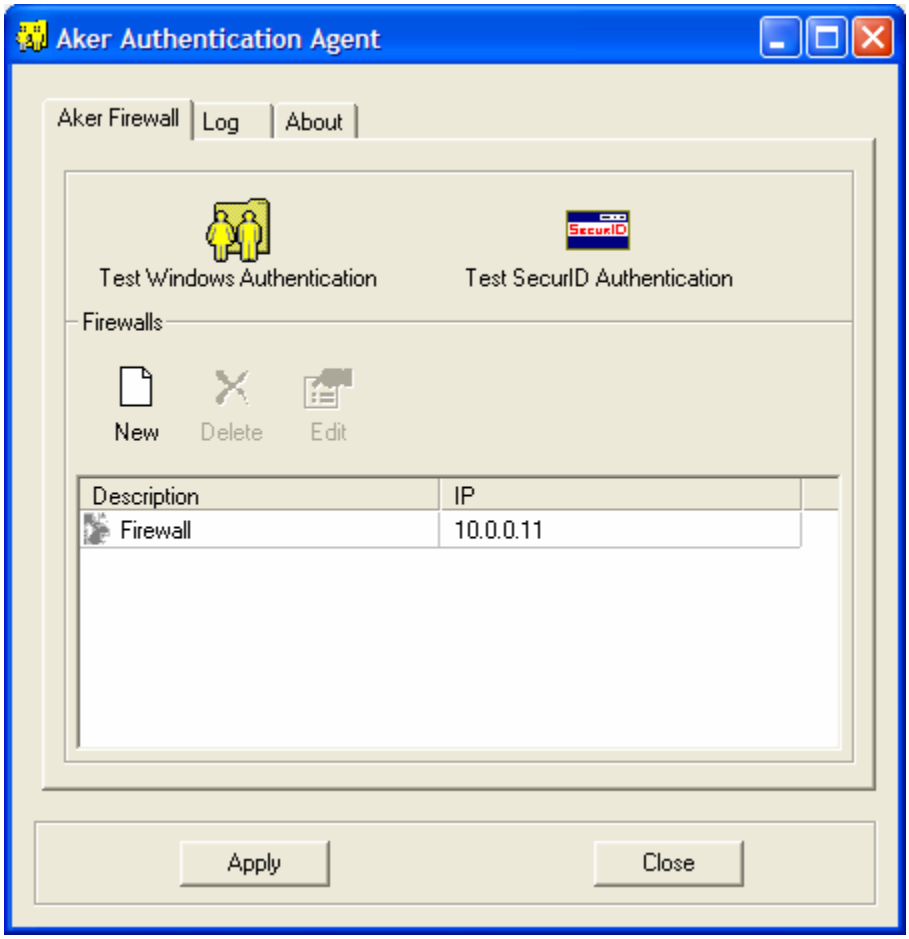
The authentication agent listens to requests on ports 1016/tcp and 1021/TCP. There can be no other application using these ports while the agent is active.

Configuration of the authentication agent for NT

After the installation of the agent, it is necessary to proceed with its configuration. This configuration allows the registration of all the firewalls that will use the agent, as well as the definition of the messages that will be produced by the agent while it is running. Differently from the authentication agent for Unix, this configuration is done through a separate program.

To access the configuration program, it is necessary to click on the *Start* menu, select the group *Aker Firewall* and inside this group, the option *Configure authentication agent*. After this is performed, the agent configuration window, which consists of 3 tabs, will be displayed:

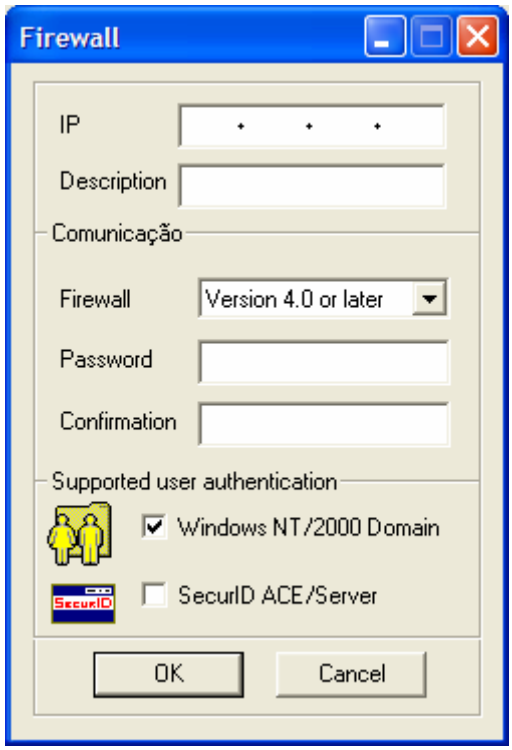
- **Firewalls configuration tab**



This tab contains all the configuration options of the agent. In the upper part of the window there are two buttons that allow the adminstrator to test the authentication of an user, in order to check if the agent is working fine. In the lower part of the tab there is a list of all firewalls authorized to connect to the authentication agent.

In order to add a new firewall to the list, just click on the **Add** button, located in the toolbar. To remove or edit a firewall, just select the firewall to be removed or edited and click on the corresponding option in the toolbar.

In case of the *Add* or *Edit* options, the following window will be displayed:



IP: It is the IP address of the firewall that will connect to the agent.

Description: It is a free text field, used only for documentation purposes.

Password: It is the password used to generate the authentication and encryption keys, used on the communication with the firewall. This password must be the same as the one configured in the entity. For further information, refer to the chapter Registering Entities.

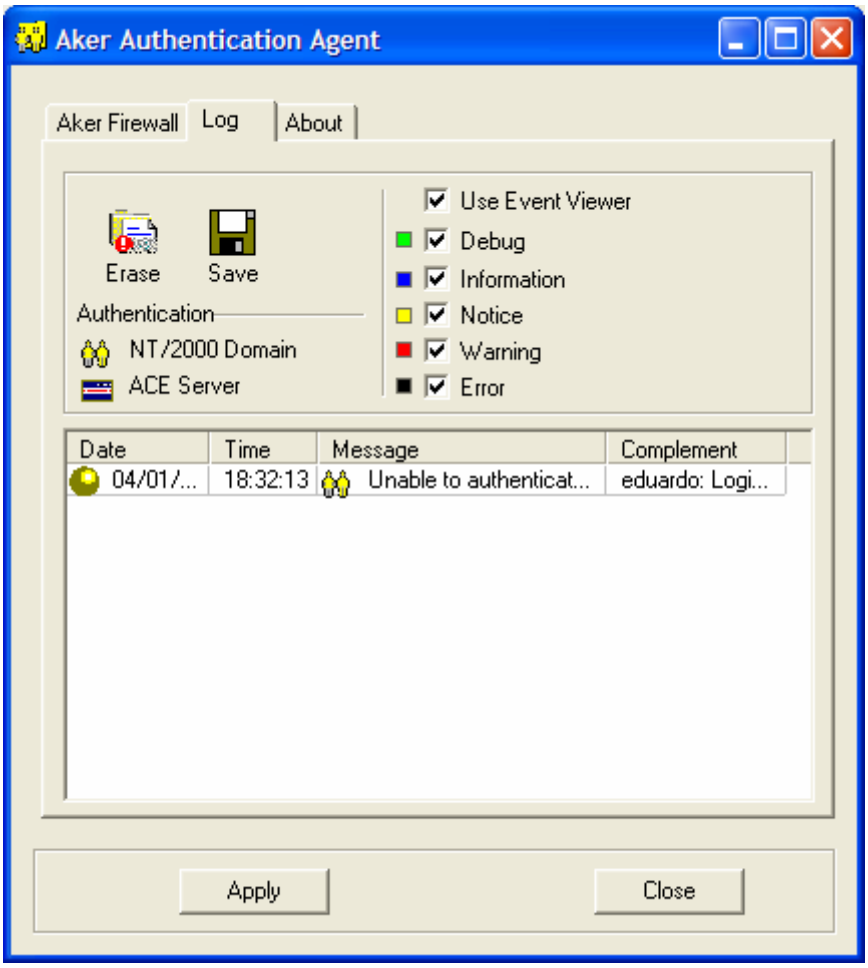
Confirmation: This field is used only to check if the password was typed correctly. It must be typed exactly as the *Password* field.

User authentication methods: This field indicates which user authentication methods will be accepted. It consists of two options which can be selected independently:

Windows NT/2000 domain: If this option is checked the agent will perform user authentication using the user database from Windows NT/2000.

SecurID ACE/Server: If this option is checked the agent will perform user authentication consulting the SecurID ACE/Server.

- **Log tab**



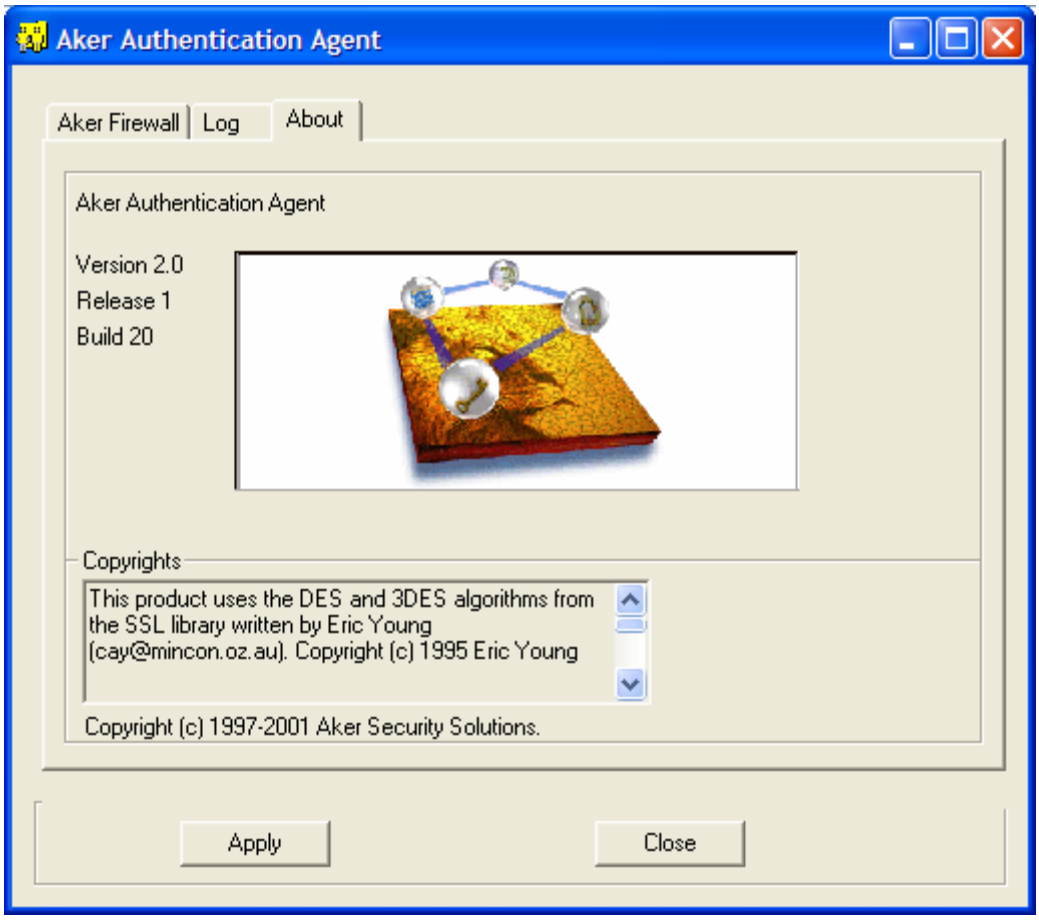
This tab is really useful to monitor the authentication agent operation. It consists of a list with several messages, sort by time. Besides each message there is a colored icon representing its priority. The colors have the following meaning:

Green	Debug
Blue	Information
Yellow	Notice
Red	Warning
Black	Error

If it is not desired that messages of a specific priority be generated, it is enough to uncheck the check-box at its left.

The option **Use event viewer**, if is checked, sends all messages to Windows event viewer.

- **About tab**



This is a purely informative tab and is useful to get some pieces of information about the client, such as its version and release.

Removal of the authentication agent for NT

To make the removal of an authentication agent for NT easier, there is an utility that does it automatically. To start it click on the *Start* menu, select the *Aker Firewall* group and in this group, the option, *Remove authentication agent*. After this, a window asking for confirmation will be displayed.

To uninstall the agent, click on the **Yes** button. To cancel the removal, click on the **No button.**

18-0 Configuring Authentication Parameters

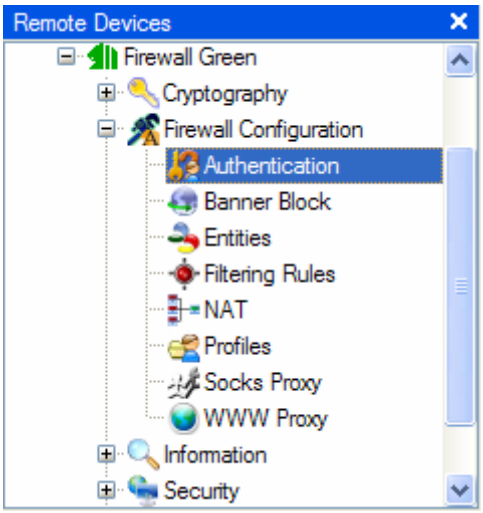
In this chapter, we will explain the Authentication Parameters and their configuration, which are essential to enable user authentication by the firewall.

What are Authentication Parameters?

Authentication parameters are used to inform the firewall which authentication methods are allowed, which authenticators must be searched to authenticate a specific user, and in which order. In addition, they control the way the search is performed, allowing for authentication flexibility.

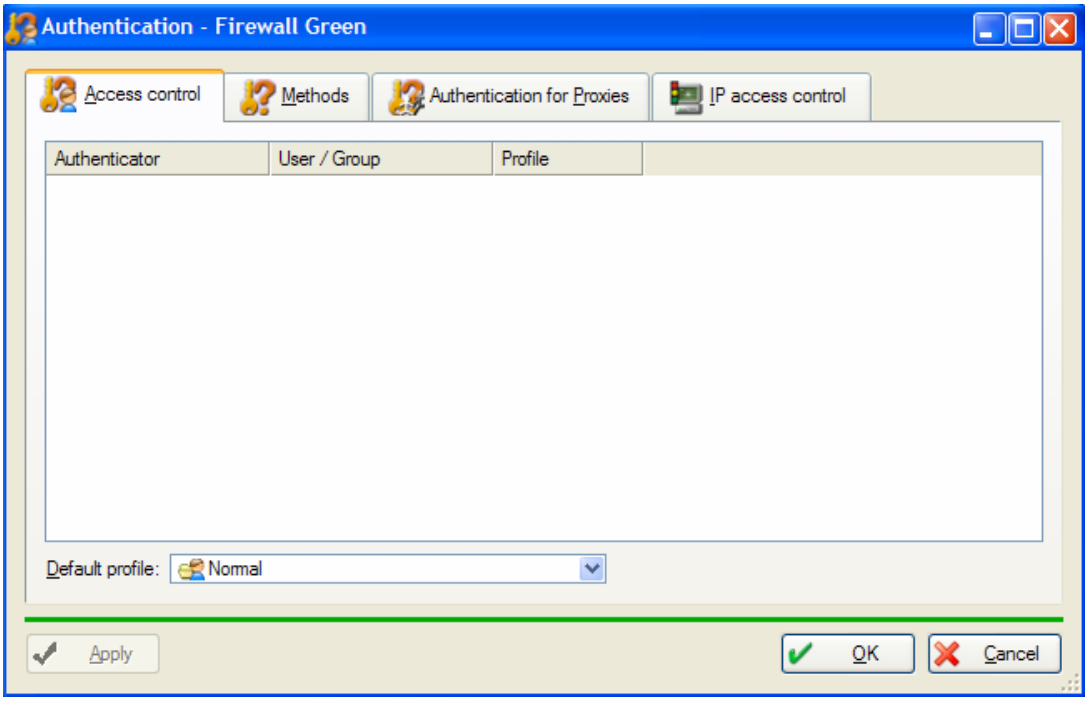
18-1 Using the Graphic User Interface

To access the Authentication Parameters Window, do the following:



- Click on the *Firewall Configuration* menu on the firewall you want to manage
- Select *Authentication*

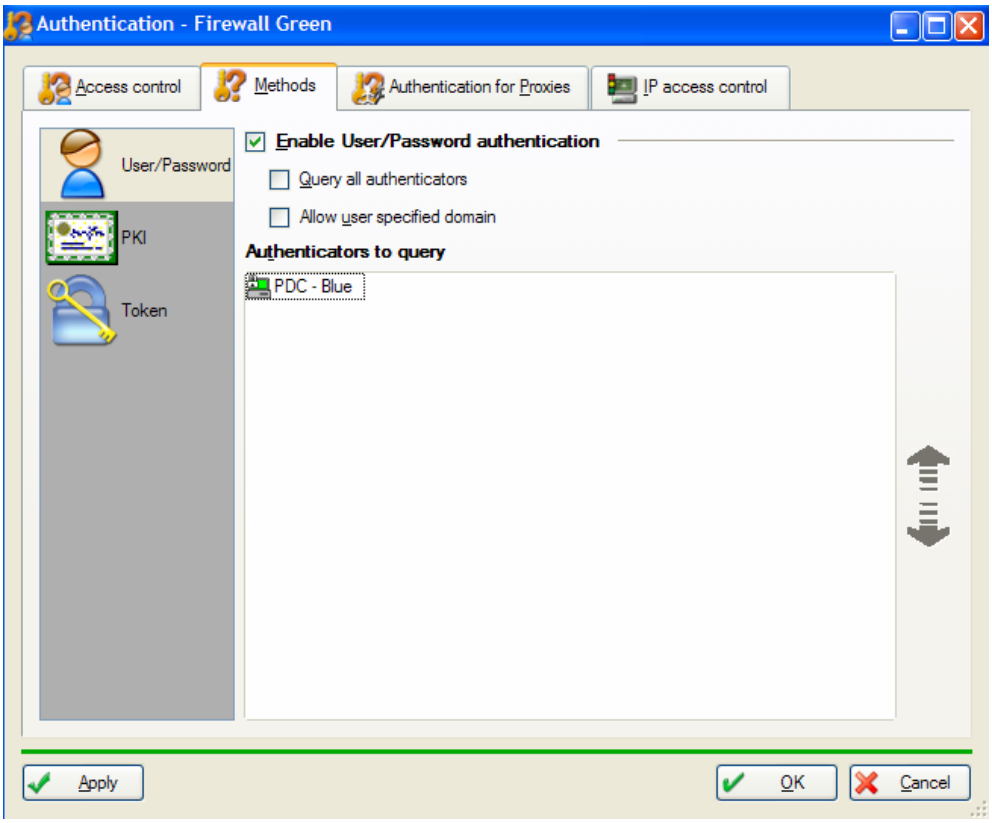
The Authentication Window



This window has four tabs: the first one is the **Access Control tab**, where users and groups from the authenticators are associated to profiles. The configuration procedure is explained in more details in the User Access Profiles chapter. In the second tab, Authentication Methods are chosen. User/Password, Certification Authorities (PKI), and Token (SecurID) authentication parameters are defined here. The third tab configures the Authentication for Proxies. In the fourth and last tab, the IP Access Control is configured. This item is also explained in more details in the User Access Profiles chapter.

- The **OK** button closes the Parameters Configuration window and applies all modifications.
- **Apply** sends all alterations to the firewall and keeps the window open.
- The **Cancel** button closes the window and discards any modification.

Methods



Enable User/Password authentication: This option indicates whether the firewall will accept username/password user authentication. If active, all other corresponding parameters must be configured.

Query all authenticators: This parameter establishes if the firewall should try to validate the same user with other authenticators on the list, whenever an authenticator returns an invalid password message.

If this option is checked, the firewall goes through all authenticators on the list, until it either receives a correct authentication response, or it reaches the end of the list. If this option is not checked, the search will terminate with the first authenticator response, be it a message of correct authentication, or of invalid password.

This option is only used for invalid password responses. If an authenticator responds that the user is not registered in its database, the firewall continues searching with the next authenticator on the list, regardless this option's value.

Allow user-specified domain: This parameter indicates if users being authenticated can tell the firewall in which authenticator they want to be validated.

If this option is checked, users can add to their name a slash / and an authenticator name. This will make the authentication request go straight to that authenticator. If this option is not checked, the request will go through authenticators in the order configured by the administrator.

This option does not require that the user supplies an authenticator name. It is optional. If the user decides not to specify an authenticator, the authentication will happen in the usual sequence.

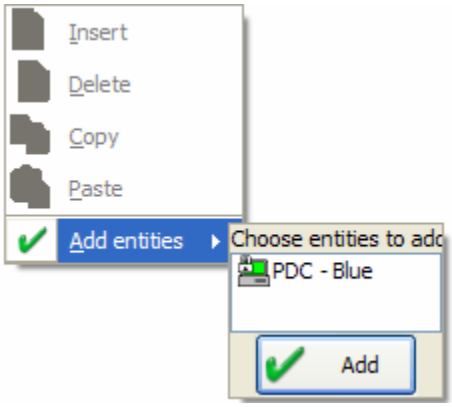
To illustrate domain specification, let's use a system with two configured authenticators (called *Unix* and *Windows_NT*). In this system, if a user called *administrator* wants to be authenticated in the *Windows_NT* host, the login or username should be: *administrator/Windows_NT*. If the suffix is not specified, the firewall will try to authenticate the user, initially through the *Unix* authenticator. If there is no user registered with this name in the *Unix* database or the *Allow user-specified domain* option is set, the firewall will then try to authenticate the user through the *Windows_NT* authenticator.

The authenticator specified by the user must be in firewall Authenticators to query list.

Authenticators to query

To add an authenticator in the Authenticators to query list, do the following:

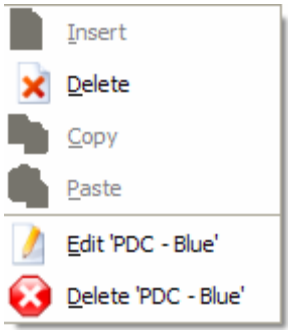
1. Right click anywhere in the Authenticators to query panel. The menu below will show up. Or, if you prefer, drag an Authenticator entity, from the Entities list, to this same place.



2. Choose **Add entities** option and select the authenticator to be added on the list on the right.

To delete an authenticator from the Authenticators to query list, do the following:

1. Select the authenticator to be deleted, and press delete in the keyboard, or
2. Right click over it, and select Delete in the opened menu.



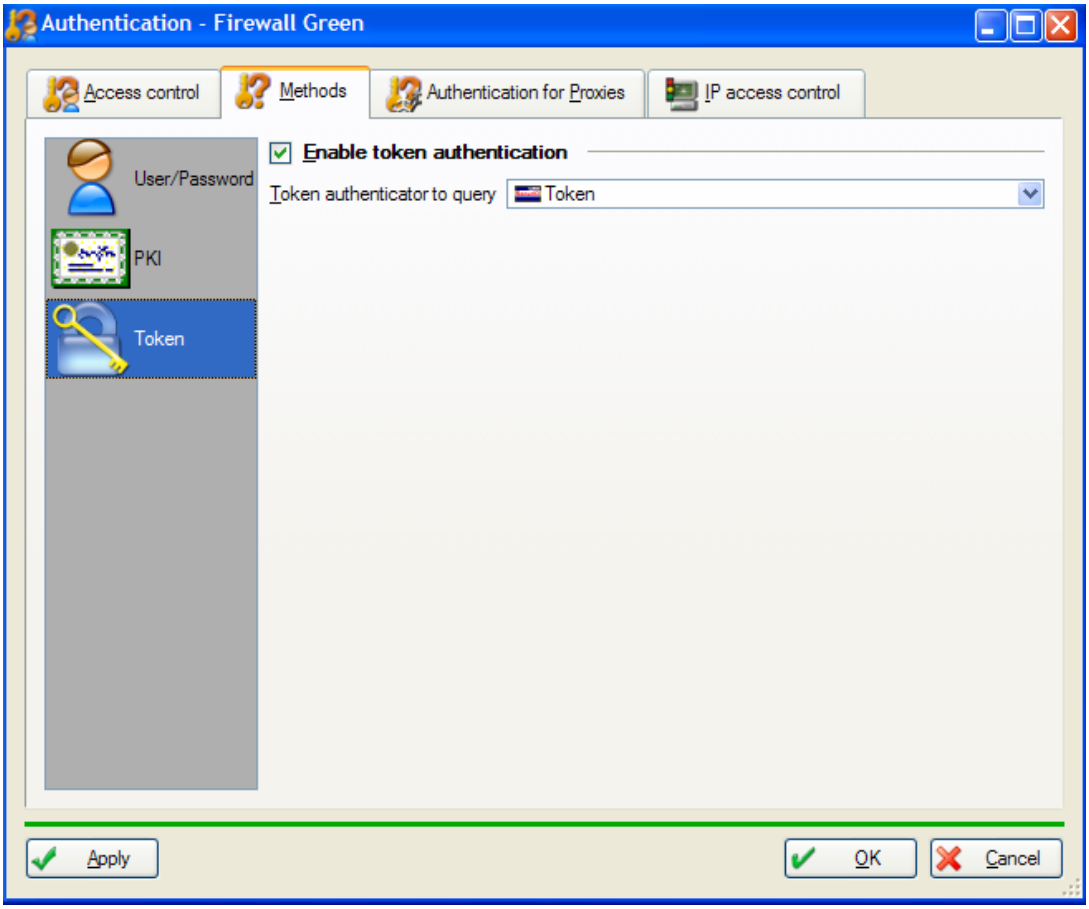
To change the query order of the authenticators, do as follows:

1. Select the authenticator that will have its query order position changed.
2. Click on one of the arrows on the right side of the list. The up arrow will move the authenticator up one position on the list. The down arrow will move it down one position.

Hint: It is possible to directly add and delete authenticators by drag and dropping them on the corresponding window.

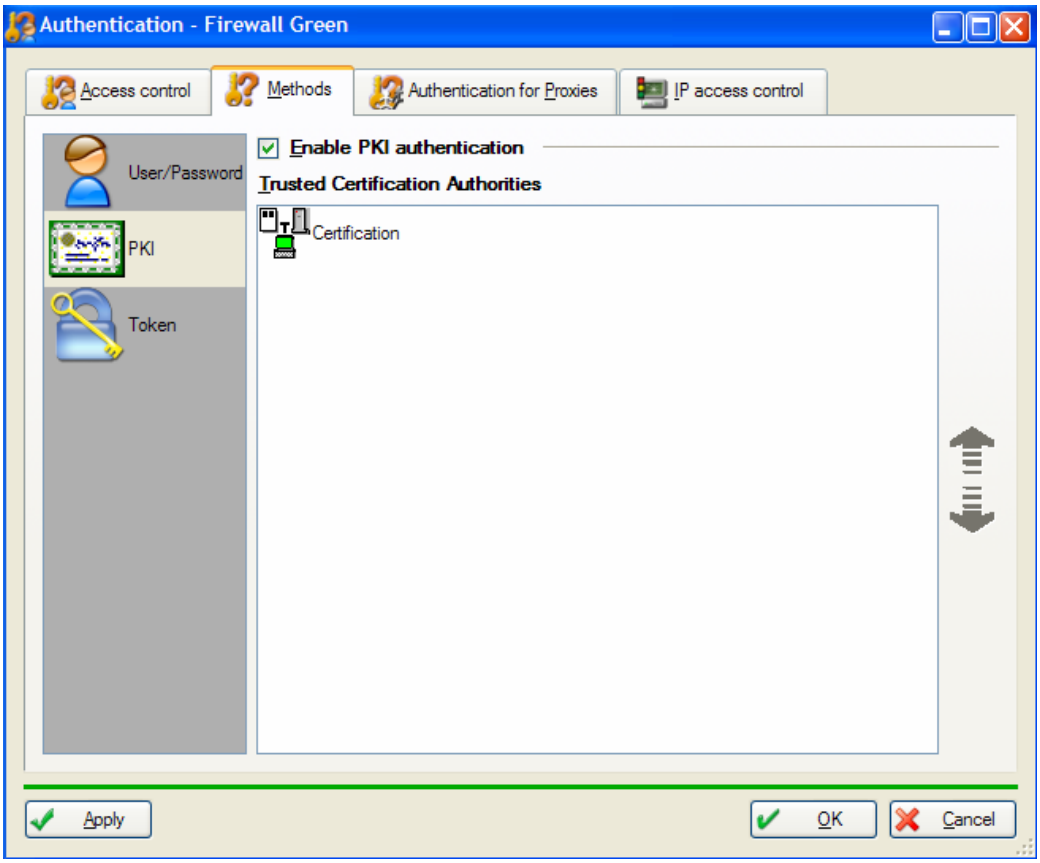
The authenticators will be searched in the listed order, from top to bottom.

Enable token authentication: This option determines if token authentication will be accepted by the firewall. If active, the name of the token authenticator must be defined.



Token authenticator to query: Indicates the token authenticator to which the data to be validated will be redirected.

Enable PKI authentication: This option indicates if smart card authentication will be accepted by the firewall. If active, the Trusted Certification Authorities must be configured.



Trusted Certification Authorities

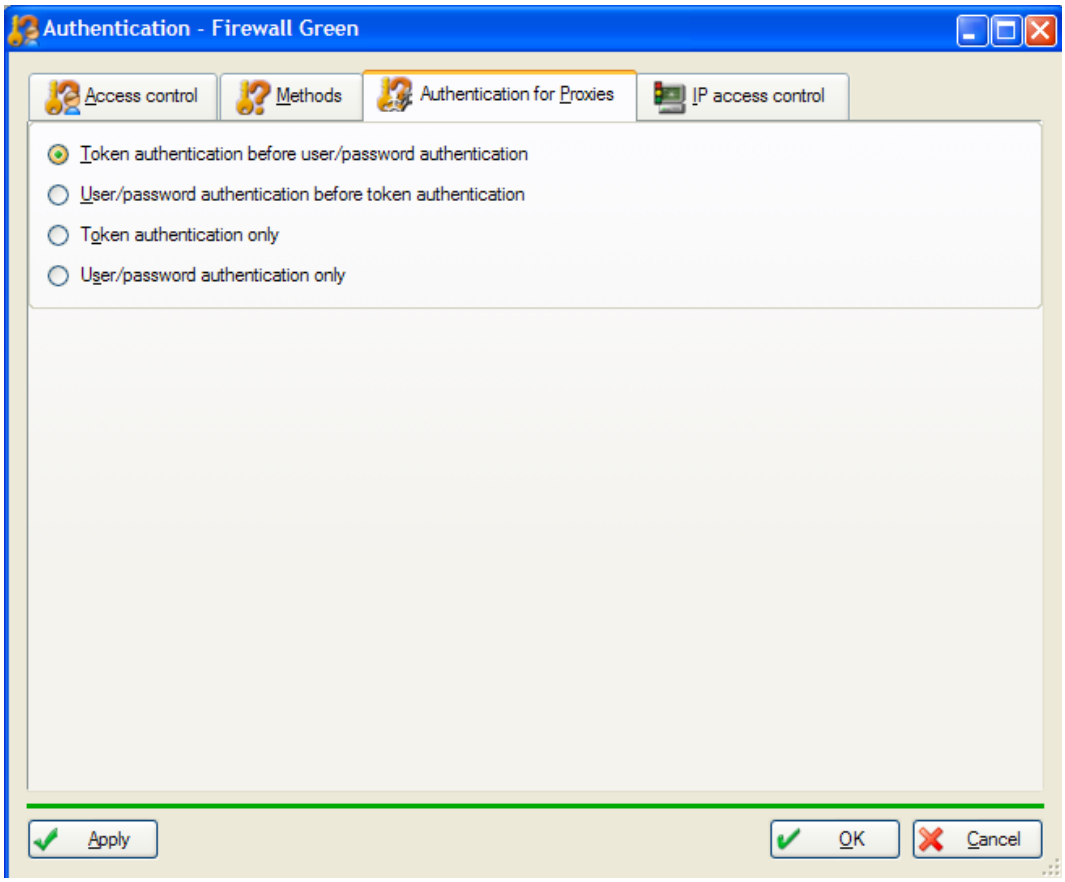
To add a Certification Authority in the Trusted Certification Authorities list, take these steps:

1. Right click anywhere in the Trusted Certification Authorities panel. A menu will show up.
2. Choose **Add entities**.
3. On the list to the left, select the Certification Authority to be added.
4. Click **Add**.

To delete a Certification Authority from the list, do the following:

1. Select the authority to be removed and press delete in the keyboard, or
2. Right click over the entity to be removed and choose the **Delete** option.

Authentication for proxies



These parameters indicate the authentication methods accepted by the proxies and the validation order. This is important, because when users are authenticated through a browser, for example, it is not possible for them to specify if they are using token or user/password authentication. Possible configuration options are:

- Token authentication before user/password authentication
- User/password authentication before token authentication
- Token authentication only
- User/password authentication only

18-2 Using the Command Line Interface

The command line interface allows the configuration of the authentication methods to be used and the authenticator's query list.

Program location: `/etc/firewall/fwauth`

Syntax:

```
Usage: fwauth [show | help]
       fwauth [add | remove] [ca | token | authenticator] <entity>
       fwauth [domain | query_all] [yes | no]
       fwauth proxy [token | password] [yes | no]
       fwauth proxy first [token | password]
```

Program help:

```
Aker Firewall - Version 5.0
fwauth – Configures authentication parameters.
Usage: fwauth [show | help]
       fwauth [add | remove] [ca | token | authenticator] <entity>
       fwauth [domain | query_all] [yes | no]
       fwauth proxy [token | password] [yes | no]
       fwauth proxy first [token | password]

       show           = displays current configuration
       help           = displays this message
       add            = adds an entity to the active authenticators
list
       remove         = removes an entity from the active
authenticators list
       domain         = enables user specified domains
       query_all      = queries all registered authenticators
       proxy password = enables user/password authentication for
proxies
       proxy token    = enables token authentication for proxies
       proxy first    = especifies the first authentication method to
be used
```

Example 1: (showing authentication parameters)

```
#fwauth show
AUTHENTICATION USER/PASSWORD
-----------------------------
Query all authenticators: yes
User can specify domain: no
Registered authenticators:
aut_local


PKI AUTHENTICATION
-------------------
There are no registered authenticators

TOKEN AUTHENTICATION
-----------------------
There are no registered authenticators
```

Example 2: (adding an authenticator to the active authenticators list)

```
#fwauth add authenticator "agent 10.0.0.12"
Authenticator added
```

19-0 User Access Profiles

In this chapter, we will explain what access profiles are used for in the Firewall Aker and how to configure them.

19-1 Planning the Installation

What are access profiles? ?

Traditional firewalls base their protection rules and access controls in hosts, through their IP addresses. While Aker Firewall allows this kind of control, it also allows the definition of access controls based on users. This way, it is possible for certain users to have their privileges and restrictions enforced, regardless of which host they are using at a given moment. This offers the maximum in flexibility and security.

To allow this user level access control, Aker Firewall introduced the comcept of access profiles. Access profiles represent the rights to be given to a specific user at the firewall. These access rights cover all firewall supported services, WWW pages control and access control through the SOCKS proxy. This way, from a single place, it is possible to define exactly what can and cannot be accessed.

How does Access Profile Control work?

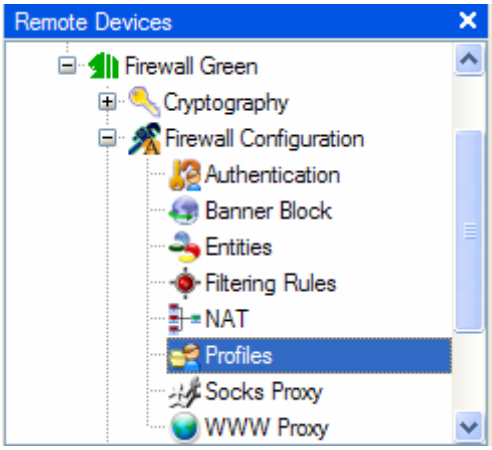
In order to use the access profiles, initially it is necessary to create the desired profiles and, after this is done, the profiles are associated with users or groups from one or more authenticators. From now on, every time an user is logged on the firewall with Aker Authentication Cliente, Aker Encryption Client or any other product that offers equal functionality, the firewall will identify the corresponding access profile and configure the access permissions according to this profile. Everything is performed transparently to the end user.

To make using access profiles possible, it is necessary to either have Aker Authentication Client, or Aker Encryption Client, installed in all client hosts, or to use check the Java Authentication client option in the WWW proxy. Otherwise, it will only be possible to use the WWW pages access control and SOCKS proxy access control. The user authentication through WWW and SOCKS proxies is possible since they will ask for an username and a password and search for the corresponding profile when they don't identify an active session for a specific host.

19-2 Registering Access Profiles

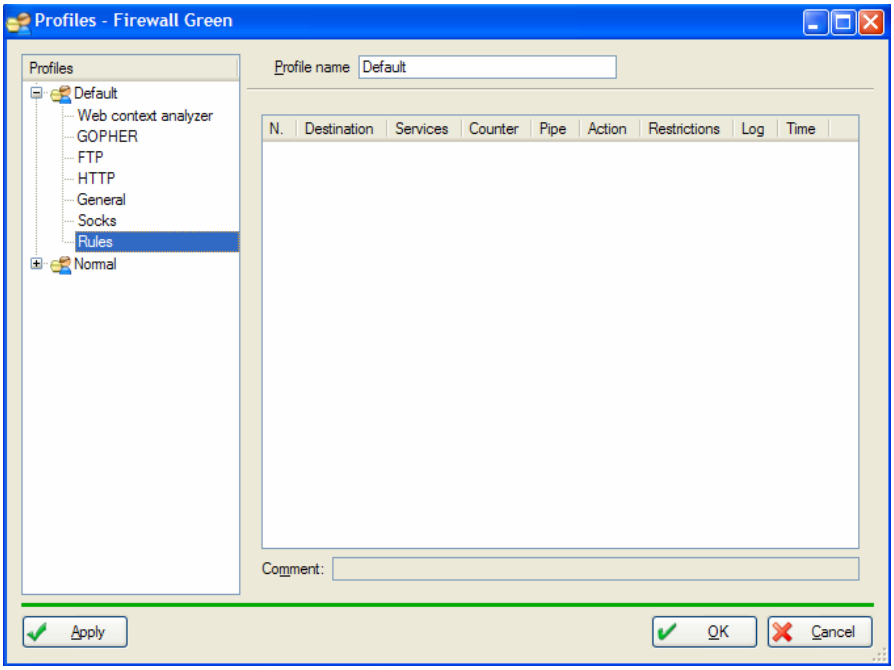
The access profiles define which WWW pages can be viewed and which type of services can be accessed. Also, for each WWW page or service, there is an associated timetable through which it is possible to define specific hours when the service or page can be accessed.

To access the access profile window, follow these steps:



- Click on the *Firewall Configuration* menu in the Firewall window you want to manage
- Select *Profiles*

The Profiles Window



The Profiles Window contains all access profiles defined in the Firewall Aker. It has a list where each profile is shown on a separate line.

- The **OK** button will close the Profiles window.
- The **Apply** button sends all alterations to the firewall and keeps the window open.

To perform any operation on a specific profile, just click on it, and then click on the corresponding option in the toolbar. The following options are available:

- **Insert:** Adds a new profile to the list.
- **Delete:** Removes the selected profile from the list.
- **Copy:** Copies the selected profile to a temporary area.
- **Paste:** Copies the profile from the temporary area to the list.
- **Insert child profile**: Adds a new profile which is a child of the current one, i.e., establish an hierarchy of profiles
- **Profile Report:** Generates a report on the profile list, in html format.

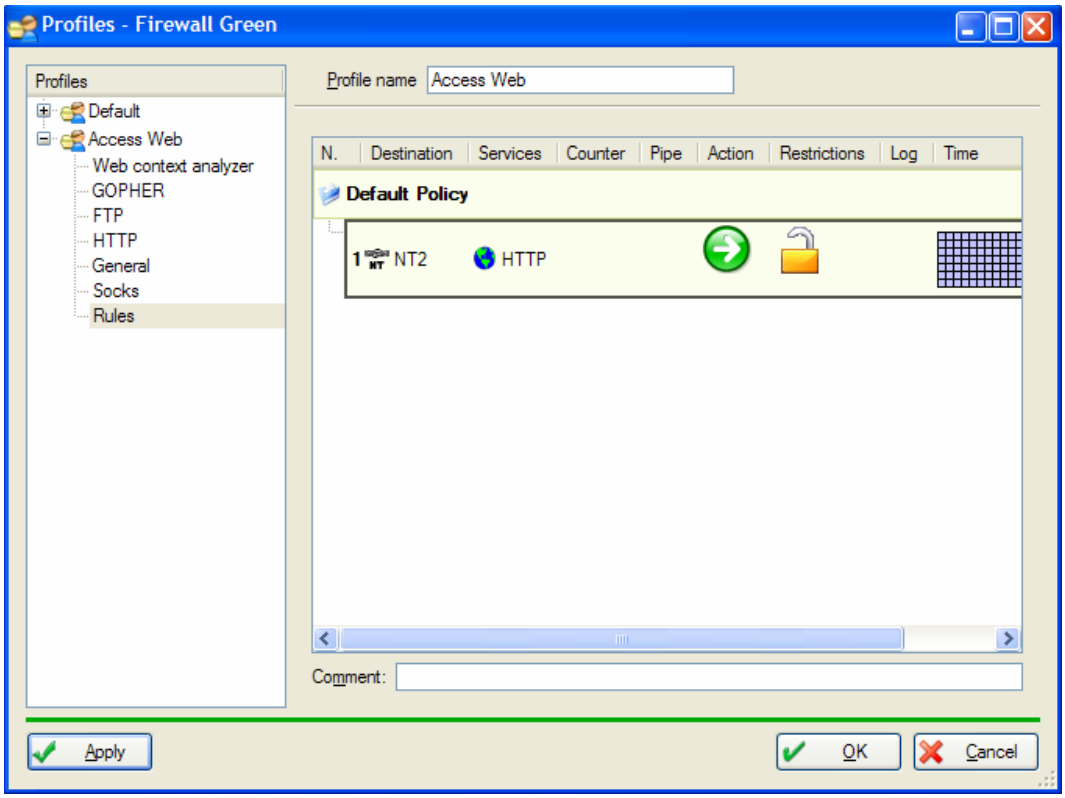
To delete an access profile, it cannot be associated to any user (for more information, see the Associating Users with Access Profiles session).

The child profile, created using the *Insert child profile* option creates a new profile that will inherit automatically the configurations of the father profile.

In the top part of the window, there is the field **Name**, used to specify the name that will uniquely identify the access profile. This name will be displayed in the profiles list and in the access control window. There may not be more than one profile with the same name.

Each access profile is composed of seven different topics. Depending on what topic is selected at a given moment, the right part of the window will change according to display different options. The configuration options are:

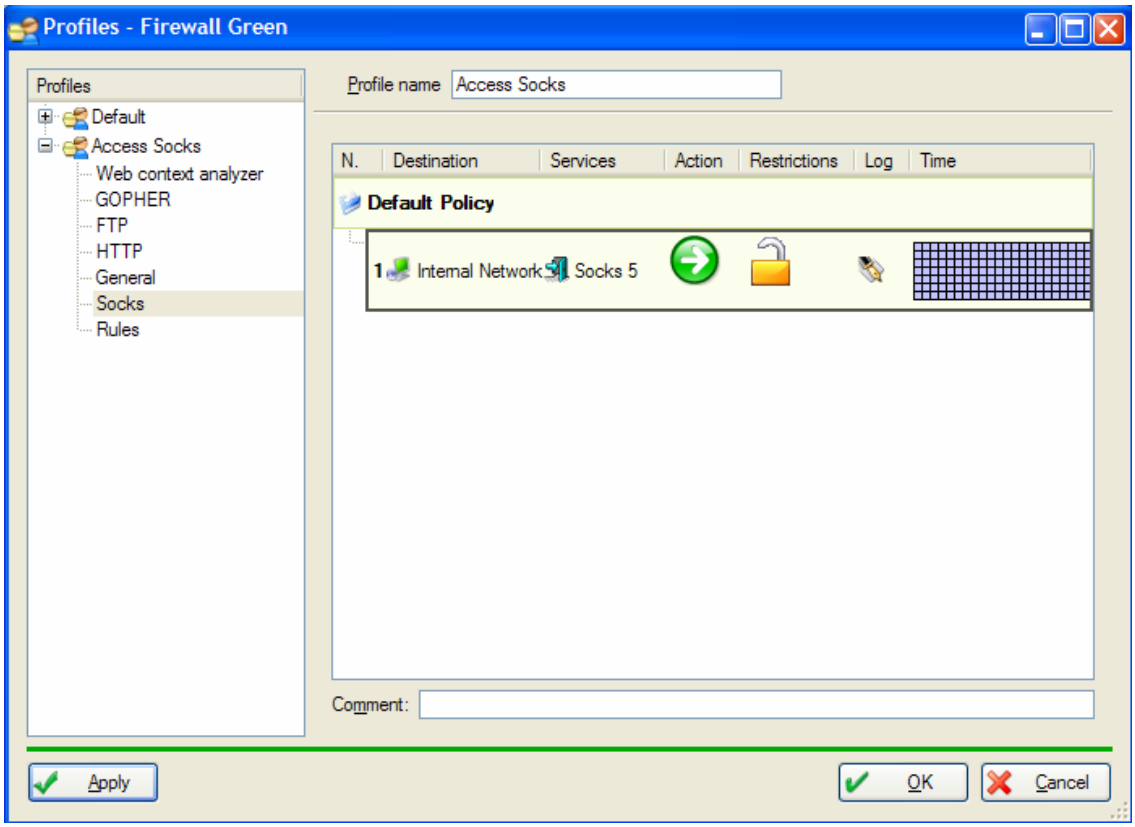
Rules



Access profile filtering rules are specified in the Rules Tab. This tab format is exactly the same as the Filtering Rules Window, except that in this case, it is not required to specify source entities (for more information, check the chapter The Stateful Filter).

Access profile filtering rules consider as the source, the host in which the session was established. Thus, it is only necessary to specify the destination entities and the services that can be accessed.

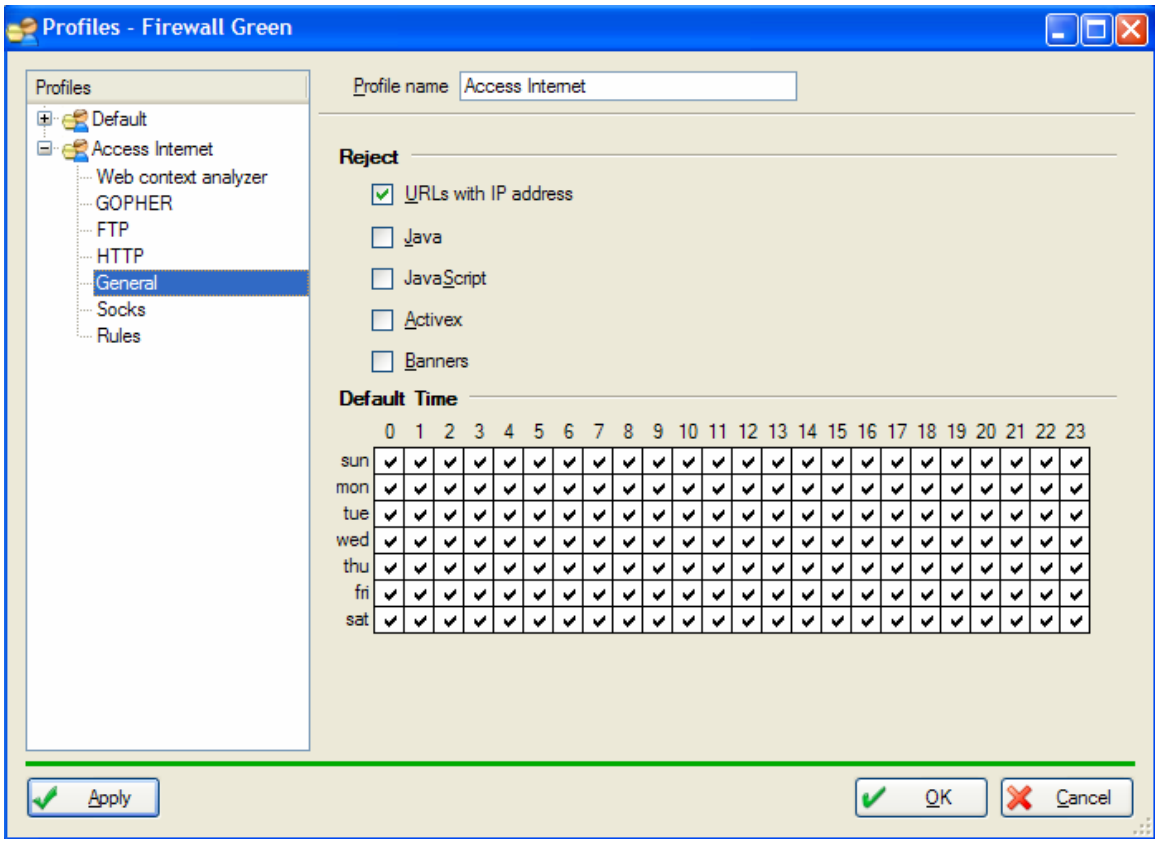
SOCKS Rules



The SOCKS Rules Tab allows the configuration of filtering rules for SOCKS proxy access. It has the same format as the Filtering Rules Window, except that it is not required to specify a source entity (for more information, see the chapter The Stateful Filter).

SOCKS proxy filtering rules consider as source the host in which the session was established. Therefore, it is only necessary to specify the destination entities and the services that may be accessed..

General



The following options are available on general section:

Block: This field defines the blocking options for WWW sites. They are:

- **URLs with IP address:** If this option is checked, access to URLs with IP addresses will be rejected, (for example, http://127.0.0.1/index.html), while access using URLs names will be accepted.

If the WWW proxy is configured to filter URLs, this option must also be configured to avoid access via IP address. Otherwise, even with the name blocked, the user will continue being able to access the URL via its IP address. It is possible to add IP addresses to the WWW filtering rules (if this filtering option is active). Since IP addresses frequently change and many servers have more than one, however, effective filtering becomes extremely difficult.

Additionally, many administrators know that poorly configured sites (specially webmail) redirect flow to servers via their IP address. So, if this option is active, these sites may become inaccessible.

- **Java, Javascript and Activex:** This field defines a special filtering for the WWW pages, blocking or not features considered dangerous in some environments. It has three options that can be checked independently: **Javascript**, **Java** and **ActiveX**. For each checked option, the corresponding applets will be filtered.

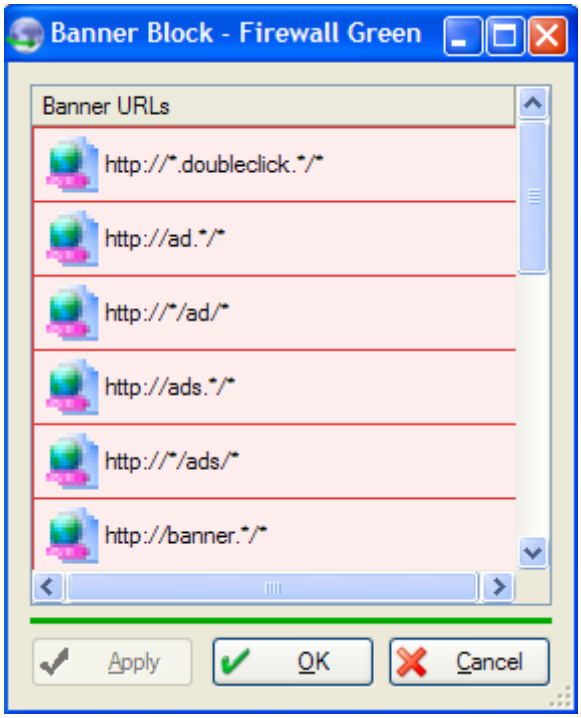
The filtering of Javascript, Java and ActiveX is made in a way that the filtered page is viewed as if the client browser did not have support for the filtered languages. In some cases, this can cause the pages to loose their functionality.

- **Banners:** This option performs the blocking of advertisement banners on web pages. If it is checked, the firewall will replace the banners for empty spaces on the pages, lowering the loading delay.

If the blocking is active, it will be performed based on global rules, equal to all profiles. In order to configure these rules, it is enough to:

- Click on the Configurations menu on the main window
- Select Banner Block

The following window will be displayed:

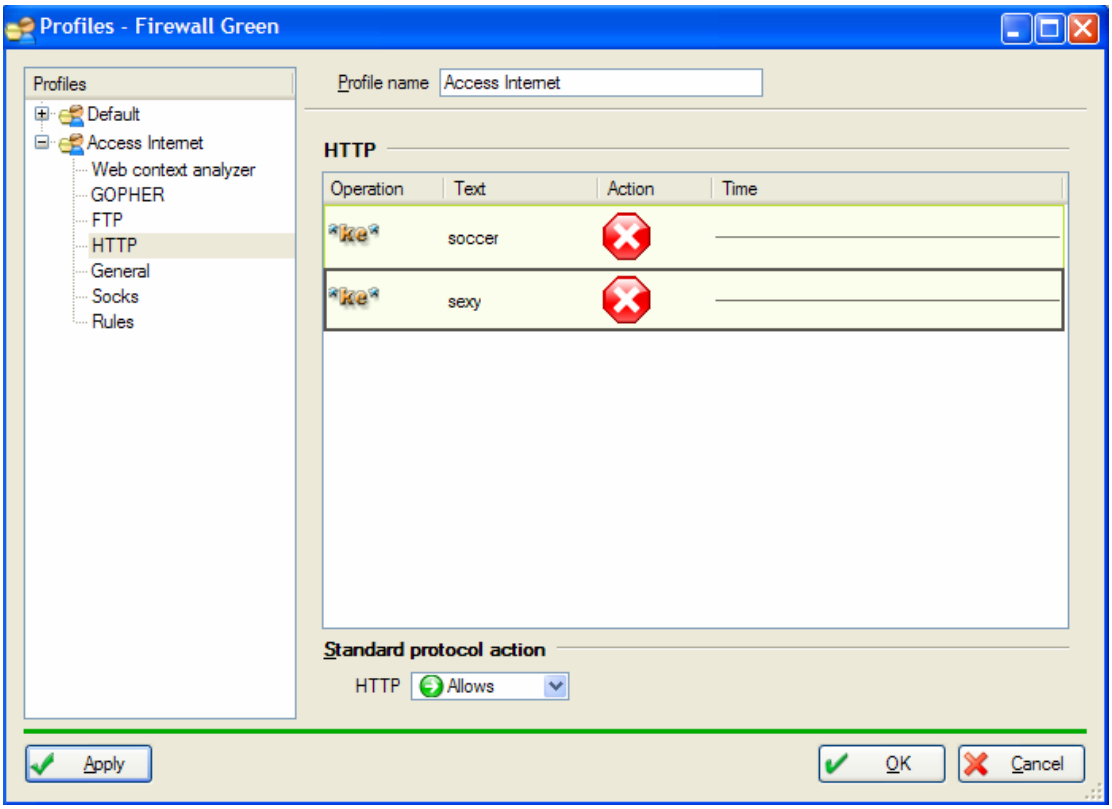


This window consists of several rules based on regular expressions. If an URL matches any of the rules, it will be considered as a banner and will be blocked.

Default timetable: This table defines WWW filtering rules default schedule. After adding WWW filtering rules, it is possible to choose between using this default timetable and specifying a different time.

Rows represent weekdays, and columns, the time of the day. To apply the rule at a specific time of the day, check the box beneath it, on the row of the desired day of the week. Otherwise, leave it blank. To make configuration easier, you may click on a square and drag the mouse over squares you want to check/uncheck, while keeping the button pressed. The table will be altered as the mouse moves over the cells.

HTTP/FTP/GOPHER



In the WWW Filtering tab URLs filtering rules for HTTP/HTTPS, FTP, and Gopher are defined. It has a list where each rule is shown on a different row.

In the WWW Filtering tab URLs filtering rules for HTTP/HTTPS, FTP, and Gopher are defined. It has a list where each rule is shown on a different row.The HTTPS protocol, for the initial URL, is filtered as if it were the HTTP protocol.

In the bottom part of the window, there is a group that defines the action to be performed in case the target address does not match any filtering rule. This group is called **Standard Protocol Action** and It has three options for each protocol:

Allows: If this option is selected, the firewall will accept URLs that don't match any rule.

Blocks: With this option selected, the firewall rejects URLs that don't match any rule.

Categorizes: If this is the chosen option, the firewall will send URLs that don't match any rule to be analyzed by the Aker Web Content Analyzer / Aker URL Analyzer.

To perform any operation on a rule, just select it and click on the corresponding option in the toolbar. The options are:

- **Insert:** This option adds a new rule to the list. If any existing rule is selected, the new one will be inserted in its position on the list, pushing it down. Otherwise, the new rule will be included at the end of the list.

- **Delete:** Removes the selected rule from the list.
- **Copy:** Copies the selected rule to a temporary area.
- **Paste:** Copies the rule from the temporary area into the list. If any existing rule is selected, the new one will be copied into its position. Otherwise, it will be copied to the end of the list.

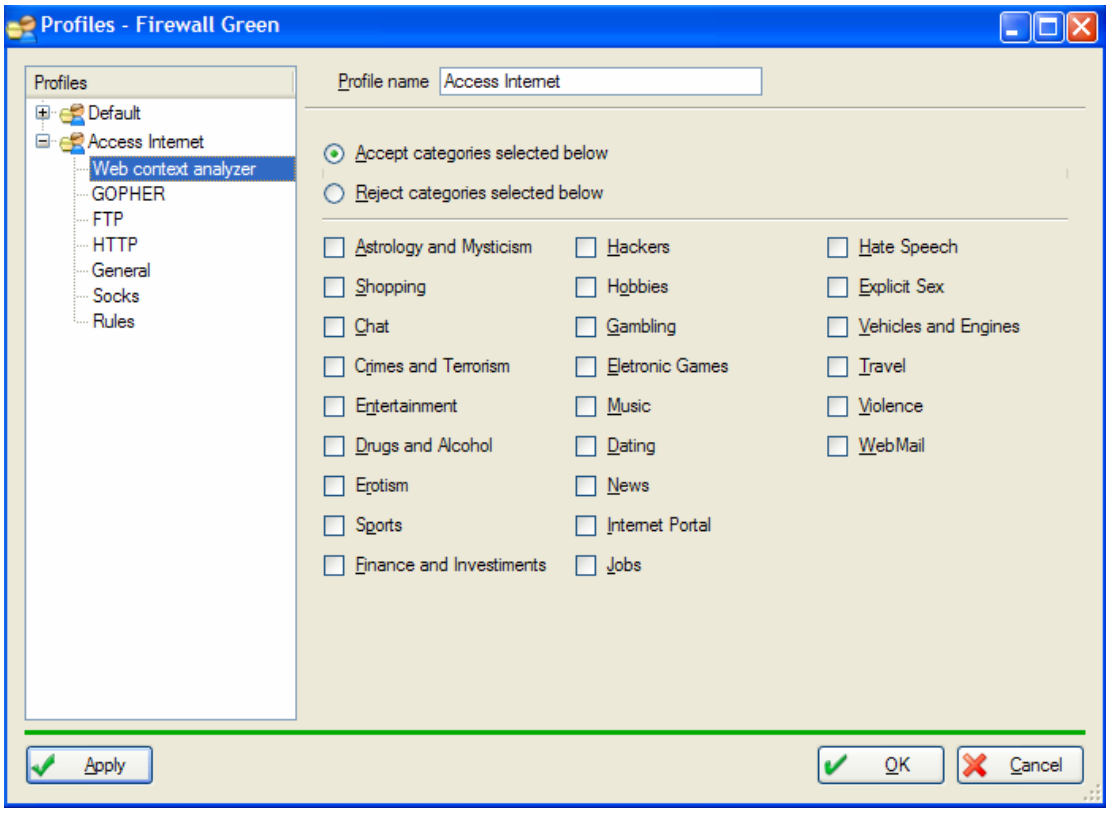
Hint: A rule position may be altered by dragging and dropping it at the desired position.
Note that the cursor will change into a hand holding a stick. "Note that the cursor will have
a dotted line square below it."

The order of the WWW filtering rules is extremely important. When the firewall receives an address connection request, it researches the list from the beginning, looking for a matching rule for that address. As soon as one is found, the action associated to it is executed.

Each filtering rule consists of an operation, which indicates the type of search that will be performed, and the text to be searched. The following operation options are available:

- **CONTAINS:** The URL must contain the specified text anywhere.
- **DOES NOT CONTAIN:** The URL cannot contain the specified text.
- **IS:** The URL content must be the same as the specified text.
- **IS NOT**: The URL content must be different from the specified text.
- **STARTS WITH:** The URL content must begin with the specified text.
- **DOES NOT START WITH:** The URL content must not start with the specified text.
- **ENDS WITH:** The URL content must end with the specified text.
- **DOES NOT END WITH:** The URL content must not end with the specified text.
- **REGULAR EXPRESSION:** In this case the URL will be matched against an regular expression

Web Content Analyzer



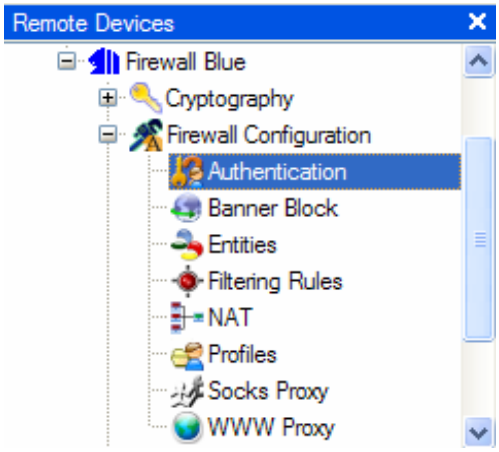
This tab is only useful if the Aker Web Content Analyzer is being used. It allows specification of the URL categories that could be viewed by the user.

If the option **Accept categories selected below** is checked, the firewall only allows user access to URLs that belong to one of the checked categories. But if the option **Reject categories selected** below is checked, the firewall only allows user access to URLs that do not belong to any of the checked categories.

19-3 Assigning Access Profiles to Users

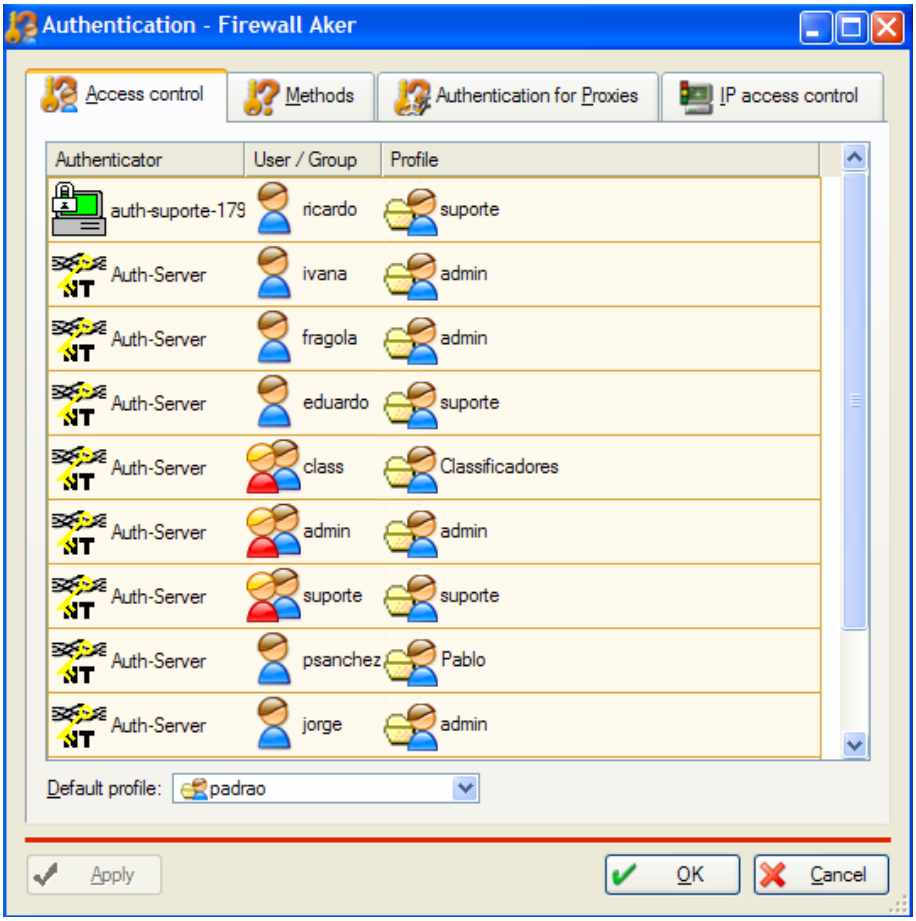
Once the access profiles are created, it is necessary to associate them with users and groups of one or more firewall authenticators or Certification Authorities. This is done through the Access Control window.

To open the Access Control window, do as follows:



- Click on the *Firewall Configurations* menu in the firewall window you want to manage
- Select *Authentication*
- Click on the *Access Control* tab

The Access Control tab

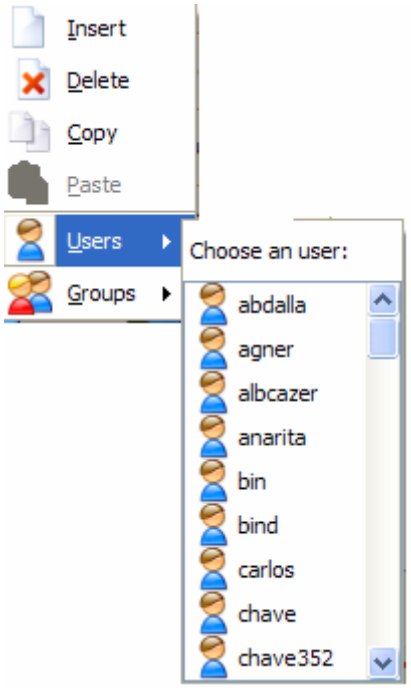


The access control window allows the association between users/groups with access profiles.

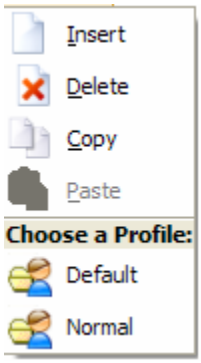
In the lower part of the window, there is a field to specify the **Default Profile**. This access profile is used every time a user is authenticated in the firewall and whose name or group is not in the access control list.

To assign a user or group to an access profile, procede as follows:

1. Right-click on the list of associations and select the **Insert** option
2. Select the authentication to obtain the list of users or groups, by right-clicking on the *Authenticatior* field. For more information about authenticators, refer to chapter Configuring the authentication parameters).
3. Right-click on the *User/Group* field and select between users or groups listing and the corresponding list will be generated automatically from the selected authenticator. Using this list, select the desired user or group.



4. Right-Click on the *Profile* field to include the desired profile, as shown below:



To delete an association of a user/group with a profile, do as follows:

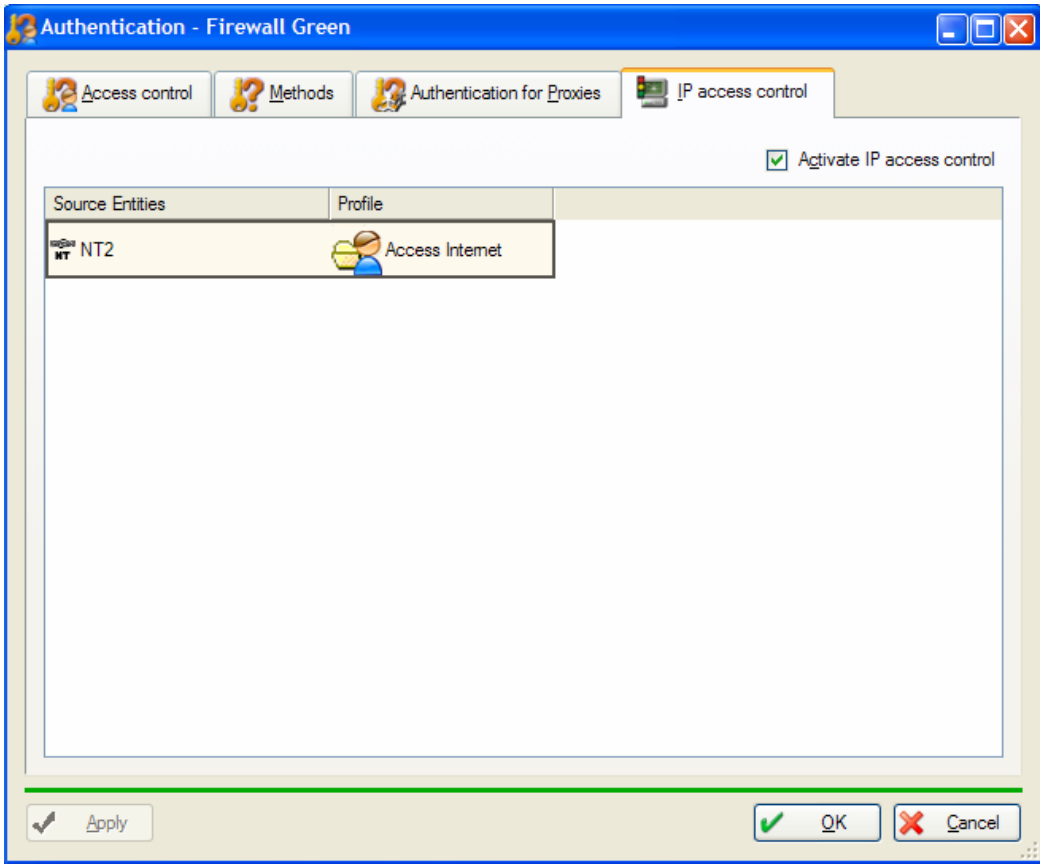
1. Click on the association to be deleted, in the lower part of the window.
2. Click on the **Delete** button.

To change the position of an association on the list, do the following:

1. Select the association that will be moved to another position
2. Click in one of the arrow buttons to the right of the list. The up arrow button will move the selected association one position up. The down arrow button will move it one position down.

The order an association occupies on the list is critical. When a user is authenticated, the firewall will start researching its name or group in the beginning of the list. As soon as a match is found, the corresponding profile will be assigned to that user.

The IP Access Control window



The firewall can control access through known IP addresses along with profiles created for this purpose. The administrator just needs to register the known networks and drag it to the Source Entities position. Then add to the Profile column, the profile or profiles needed in the rule.

Note: the Activate IP access control box must be checked.

20-0 Aker Authentication Client

We will explain here the Aker Authentication Client, what it is and its use: a tool that allows for high level of security.

20-1 Planning the Installation.

What is Aker Authentication Client?

In the previous chapter, user access profiles, their usefulness to the firewall administrator, and how to assign them to firewall authenticator users, were the themes covered. How the firewall detects what host a specific user is using in a given moment, however, was not detailed.

The Aker Authentication Client enables the firewall to determine exactly which users are accessing which hosts. This software, which must be installed in all hosts where user access control is needed, works in a totally transparent way to the end user. It intercepts user logon in the domain, or requests a new authentication if token or smart card authentication is being used, and sends these data, encrypted, to the firewall. The firewall then validates the received data using its authentication agents, token authenticators, or Certification Authorities. And, if the user has been correctly validated, it establishes a session for the validated user, from the machine where the session was established.

From this moment on, the user will have a configured access profile and access to all services it makes available. When the user logs off, the Authentication Client detects it and sends the information to the firewall. Once again, everything is done in a transparent and automatic way.

The Authentication Client will use port 1022/UDP (Aker-CL service) to communicate with other firewalls to establish user sessions. It is necessary at least one filtering rule allowing access to the firewall, from the hosts with the Authentication Client installed. Otherwise, it will not be possible to establish the sessions.

The Authentication Client does not work through Network Address Translation. So, it is not possible for a host behind a firewall that performs network address translation, to establish a session with a firewall located outside the translation domain.

20-2 Installing Aker Authentication Client

Aker Authentication Client works in Windows 9*/NT/2000/XP platforms. Its installation is very simple, however, it is necessary to reinitialize the computer after installation is finished, to start the Client.

To install the Authentication Client, insert the CD-ROM in the drive, and select **Install Authentication Client**, inside the **Firewall** menu, in the presentation window. If the Auto-run option is disabled, it will be necessary to take the following steps:

1. Click on the **Start** menu
2. Select **Run**
3. Select the path **D:\en\firewall\authc** and run the only file present in this path (If your CD-ROM drive uses a letter other than D, replace it accordingly).

The Installation window will show up. To continue, follow the instructions on the screen.

When the installation is over, a new group called **Aker Firewall** will be created in the **Start** menu. Inside it, a group called **Authentication Client** will also be created. To run the Authentication Client configuration, just select the **Configure Authentication Client**, inside this group..

Installing the Client using Scripts

To make the installation of Aker Authentication Client easier in a large number of hosts, it is possible to make it automatic, and perform it in a non-interactive way. For example, a logon script can be written to install the Client in case it's not already installed.

The automatic, non-interactive installation is activated through another program called **Setupbat**, located in the same directory as the installation program described above. It receives the installation options through the command line. The available options are:

`-a`	Executes the automatic installation
`-d` ***`diretório`***	directory Specifies the installation directory
`-f`	Installs the Client even if it detects a previous installation
`-e`	Installs the Client without the configuration interface

If the **–d directory** option is not specified, the Client will be installed in **C:\Program Files\aker\aker_authenticator**

If the **–e** option is specified, a configuration file must be created and distributed along with the Client, once it won't be possible to configure it through the GUI. Procedures to generate this file are described below.

Distributing a default configuration in the Client installation

In addition to automatically installing the Client, it is also possible to distribute a default configuration to be used in both the automatic and the interactive installation. This way, the firewall administrator can pre-configure the Aker Authentication Client, in such a way that end users don’t need to perform any type of configuration.

To install the Client with a default configuration, just configure it in a host in any way desired, and afterwards, copy a file to the directory where the default version will be installed in each machine. The installation program will detect the file exists, and automatically copy it to the directory where the program will be installed.

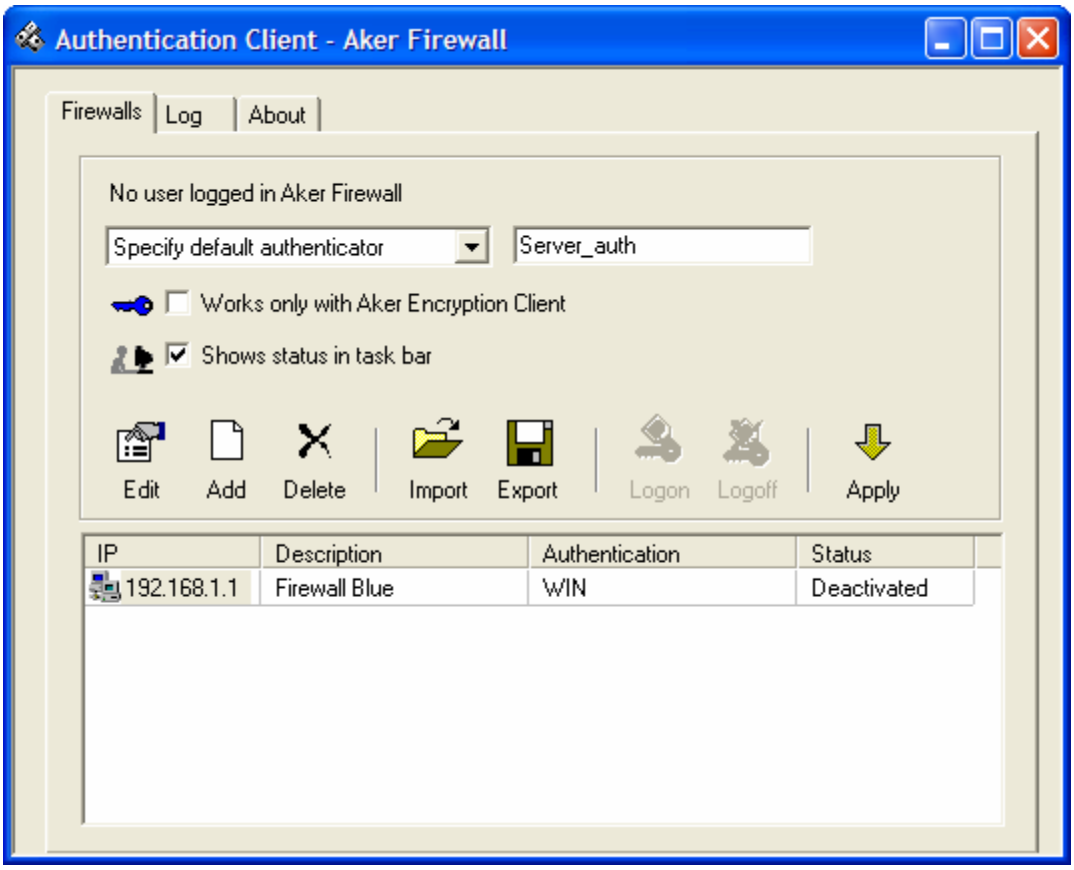
The following file can be copied:

`firewalls.clp`	List of firewalls the Client will try to logon

20-3 Configuring the Authentication Client

The Aker Authentication Client runs always in background. Its configuration requires the execution of the Configuration Program described above. The Configuration Program has three tabs, each one responsible for a specific task. They are:

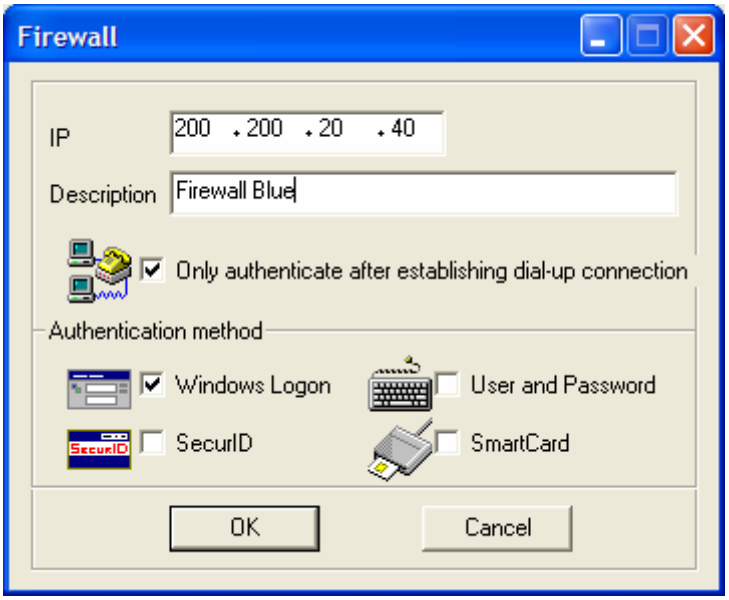
Firewalls



This is the main tab of the Client configuration. It has a list showing all the firewalls in which the Client will try to establish a session. To each firewall, there is a column indicating the authentication methods that can be used, and another indicating whether there is an active session or not.

To add a new firewall to the list, just click on the **Add** button, in the toolbar. To delete or edit a firewall, just select it, and click on the corresponding option in the toolbar.

If the **Add** or **Edit** options are chosen, the following window will be displayed:



IP: It's the IP address of the firewall to which the Client will try to establish a session.

Description: It's a text field, used solely for documentation purposes.

Authenticate only after establishing dial-up: If this option is on, the Authentication Client will try to establish a session with the firewall only after a dial-up session has been established. This option is especially useful for Clients installed in notebooks..

Supported authentication methods: This field indicates the authentication methods that will be used to validate a user to the firewall. It has the following options:

Windows logon: If this option is checked, the Authentication Client will capture the name and password of the user who logged on Windows, and will use them to establish the session with the firewall. In this case, the authentication will be totally transparent, that is, no new screen will be displayed to the user.

User and password: If this option is selected, a screen will show up prompting the user for a name and password in order to establish the session with the firewall.

SecurID: If this option is selected, a window will show up prompting the user for a name, a PIN, and a token code in order to establish the session with the firewall.

Smart Card: If this option is checked, a window will show up prompting the user for the Smart Card PIN in order to establish the session with the firewall.

If more than one option is selected (except the Windows Logon), a window will show up allowing the user to choose the authentication method at each new session.

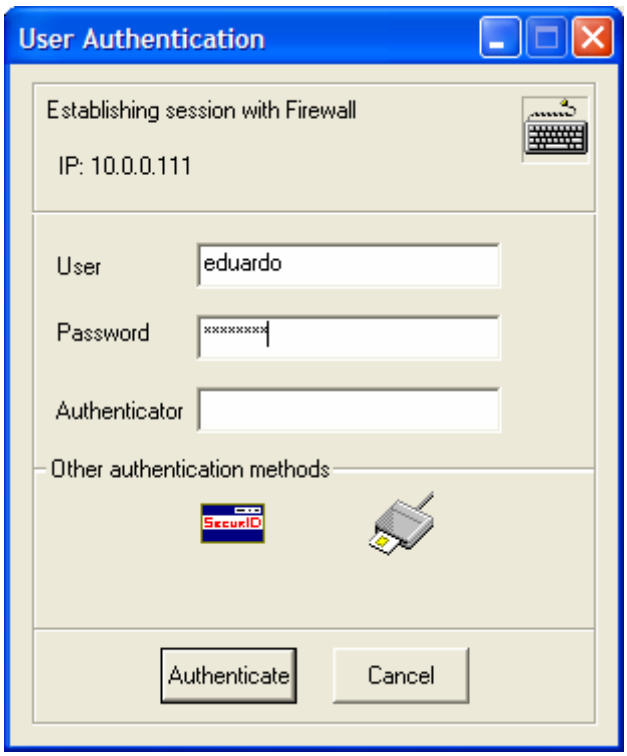
If Smart Card Authentication is chosen, and the host doesn't have a Smart Card reader, this option will be ignored..

It is possible to export the current configuration to a file, and import it later to the same or to other machine. The **Import/Export** button, in the toolbar, saves to a file the list of firewalls plus the remaining options of the window.
The **Export/Import** button loads a list of firewalls and remaining options from a file, and adds the firewalls to the current list (the new entries will be added to the end of the current list).

The **Logoff** button terminates a session with the selected firewall. It will only be enabled if the selected firewall has an active session.

The **Log** button makes the Client try to establish a session with the selected firewall. It will only be enabled if the selected firewall has no active sessions. When clicked, it will show one of the windows below, depending on the authentication method chosen:

- **User/password authentication**

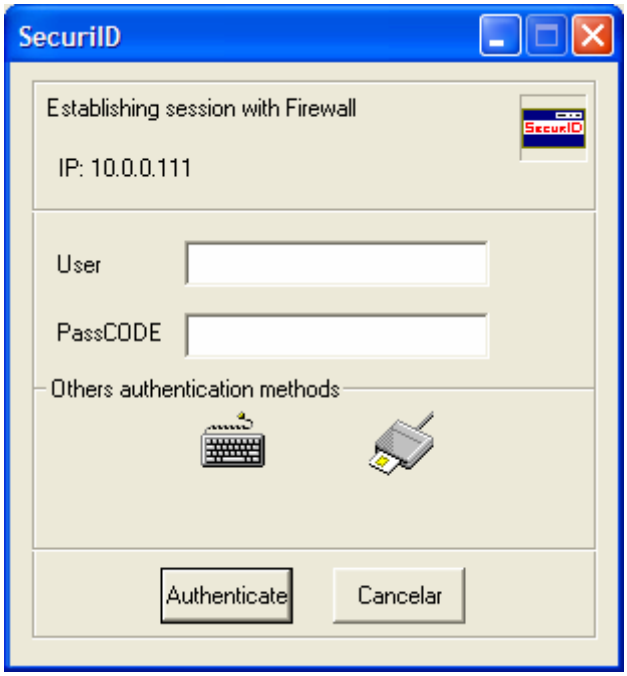


User: It's the name of the user attempting to establish the session.

Password: It's the password of the user attempting to establish the session.

Authenticator: It's the name of the authenticator through which the user wants to be authenticated. This field may be left blank. For more information on authenticators, see the chapter Configuring Authentication Parameters.

- **Token (SecurID) authentication**



User: It's the name of the user attempting to establish the session.

PassCode: It's the combination of the user PIN followed by the number of the token SecurID.

- **Smart Card authentication**

When Smart Card authentication is chosen, the screen that will be displayed will depend on the type of Smart Card being used. Above, is just one of the possibilities.

The **Apply** button is used to save recent modifications and make them permanent. When pressed, all active sessions will be terminated.

On the top part of the tab, there is a field to specify how the Authentication Client will deal with authenticators. This option is only used when the *Windows Logon* authentication is selected. It has three options:

Don't specify authenticator: This option tells the Client to send the authenticator field blank when logging in the firewall. This way, the firewall will research its authenticator list as usual.

Use NT domain as authenticator: This option tells the Client to inform the firewall the NT domain is the authenticator that should validate the user. To function properly, an active authenticator with the name of the NT domain must exist, and the firewall configured to allow user specified domain. For more information on these parameters, see the chapter Configuring Authentication Parameters.

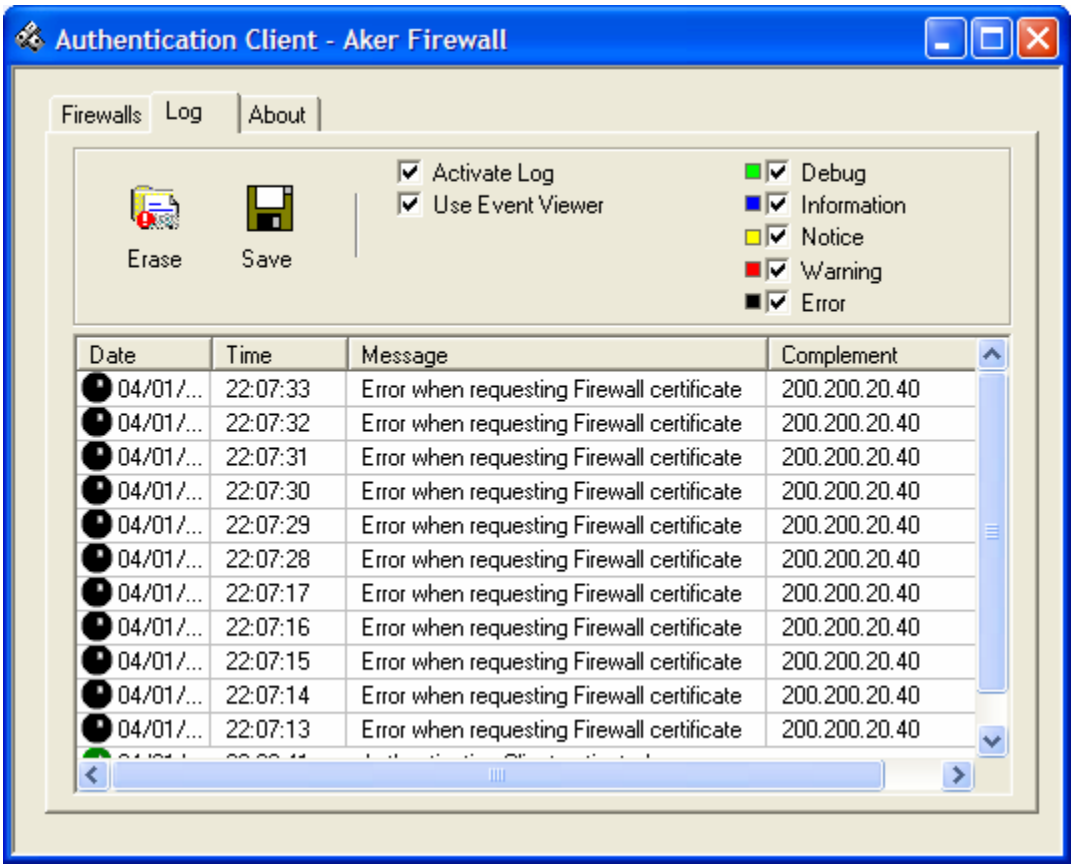
Specify Default Authenticator: This option allows users to specify the authenticator name to be used by the Client to log in the firewall. To function properly, an active authenticator with the specified name must exist, and the firewall configured to allow user specified domain. For more information on these parameters, see the chapter Configuring Authentication Parameters.

If the option **Works Only with Aker Encryption Client** is checked, it makes the Authentication Client try to establish a session with a firewall only if the Encryption Client is active. This adds a higher level of security, because the Encryption Client uses signed certificates, and, thus, is able to validate the firewall with which it is communicating.

All communication between the Aker Authentication Client and firewalls is encrypted, even if the option **Works Only with Aker Encryption Client** is unchecked. The only way the Encryption Client adds more security is because it validates, through signed digital certificates, that the other communicating firewall is really a true firewall, obstructing men-in-the-middle type of attacks.

The option **Shows Status in Taskbar**, when checked, displays an icon in the taskbar used to verify if there is any established session.

Log



This is a very useful tab to track Authentication Client operation. It has a list of several messages in chronological order. Next to each message, there is a colored icon representing its priority. Colors mean the following:

Green	Depuration
Blue	Information
Yellow	Notice
Red	Warning
Black	Error

The **Delete** button located in the toolbar erases all entries from the log.

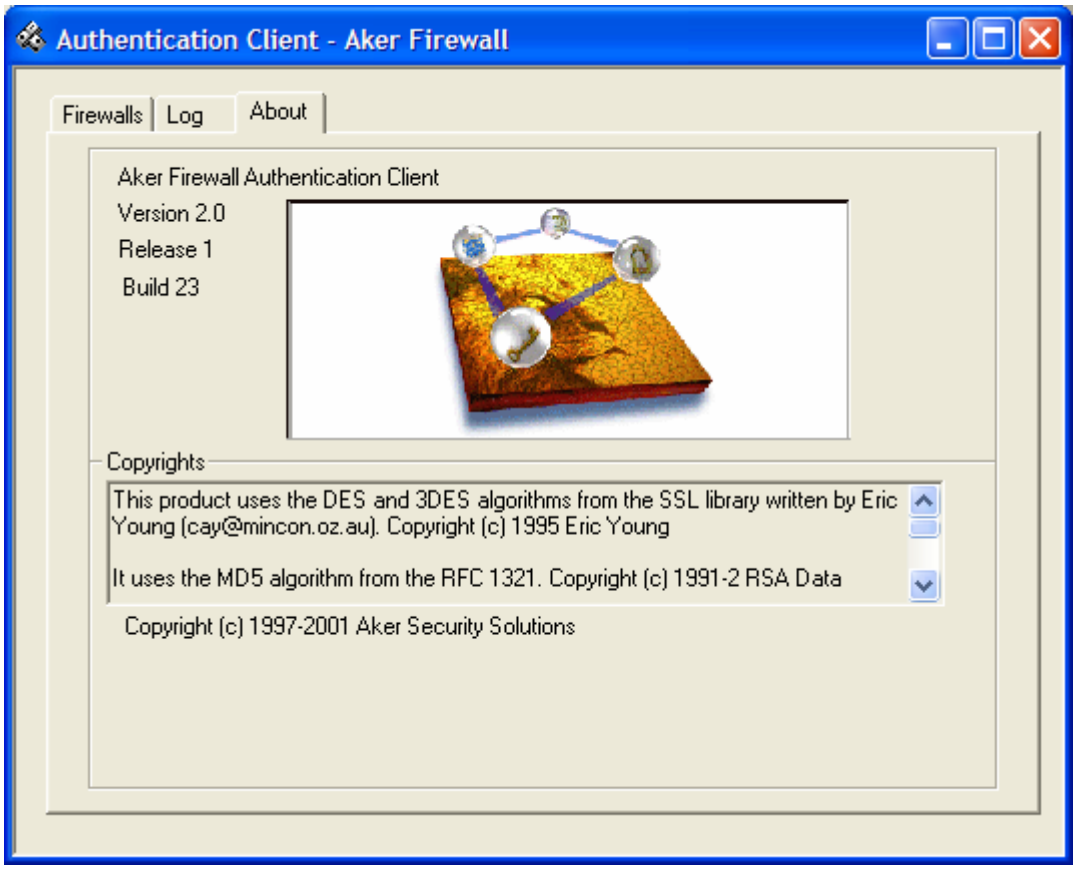
The **Save** button saves the log in a text format. When clicked, a window prompts for the name of the file being saved.

If the **Activate Log** option is not checked, the Authentication Client will stop generating new log entries.

The **Use Events Viewer**, if checked, sends all log messages to the Windows Events Viewer.

The Aker Authentication Client log is stored only while the Client is running. If the machine is reinitialized, all its information will be discarded.

About

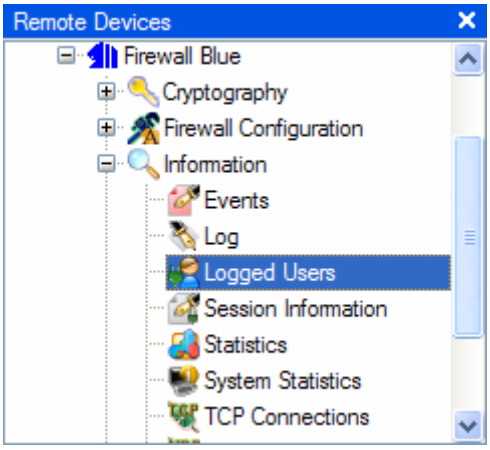


This window gives useful information about the Aker Encryption Client, such as version and release, among others.

20-4 Viewing and Deleting Users Logged on the Firewall

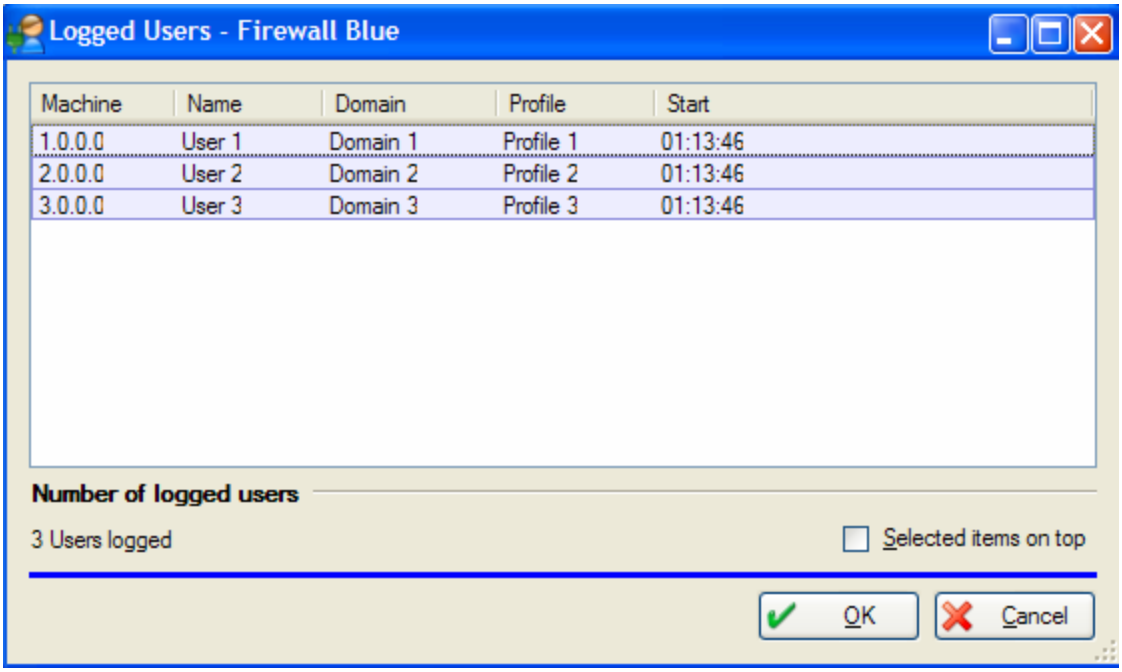
Users, who have an established session with the firewall, can be viewed at any time, through the Authentication Client. It is equally possible to delete any of these sessions. This is done in the Logged Users window.

To access the Logged Users window, do the following:



- Click on the *Information* menu in the firewall administration window
- Select *Logged Users*

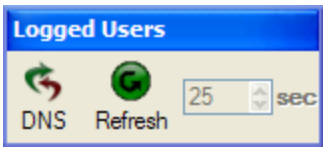
The Logged Users window



This window has a list of logged users, one entry to each user. In the bottom part of the window, there is a message informing the total number of users with established sessions at that time.

- The **OK** button closes the Logged Users window.
- The **Cancel** button closes the window.
- The **Selected items on top** box moves selected items to the top of the list of logged users.

Logged Users Toolbar



- The Refresh button updates the information displayed periodically, automatically or not. By clicking on it, you toggle between the two operation modes. Changing the value in the field just to the right configures the refresh interval.
- The **Delete** button, located in the toolbar, erases a user session. To do it, first select the session to be deleted, and then click on this button. (It will remain disabled until a session is selected.)
- The **DNS** button activates the name service to resolve the names of hosts with listed IP addresses. It is important to notice the following:

1. Name resolution is most often a slow service, and, because of that, name translation is performed in the background.
2. Many times, due to reverse DNS configuration problems (which is used to resolve IP addresses names), it is not possible to resolve certain addresses. In these cases, unresolved addresses will be kept in their original format and will be marked to show they don't have configured reverse DNS.

- It is possible to sort the session list by any one of its fields, just by clicking on the field title. The first click will sort the field in ascending order, and the second, in descending order.

Active User Session field structure

Each row on the list of user sessions represents a session. Field structure is as follows:

Icon: Is shown to the left of each user name, and may have three different formats:

Padlock: This icon indicates the user was logged only through the Encryption Client.

User: Indicates that the user was logged through the Authentication Client only.

User inside a padlock: Indicates that the user was logged through both the Authentication Client and the Encryption Client.

Host: IP address or name (if the DNS is active) of the host in which the session was established.

Name: Name of the user who established the session.

Domain: Domain name, i.e., authenticator in which the user was authenticated. If the user did not specify a domain at login time, this field will be blank.

Profile: What access profile corresponds to this session. If this field is blank, the user was authenticated before the profile table was altered. So the profile used does not exist anymore.

Start: Time of day when the session was started.

20-5 Using the Command Line Interface

The command line interface to access the list of logged users has the same capabilities as the GUI, and is simple to use. It is the same program that produces the active TCP and UDP connections list, shown before.

Program location: `/etc/firewall/fwlist`

Syntax:

```
Usage: fwlist help
     fwlist show [[-w] [TCP]] | [UDP] | [sessions]
     fwlist remove [TCP | UDP] source_IP source_Port destination_IP
destination_Port
     fwlist remove session source_IP
```

Program Help:

```
Aker Firewall - Version 5.0
fwlist - Lists and removes TCP/UDP connections and active sessions
Usage: fwlist help
     fwlist show [[-w] [TCP]] | [UDP] | [sessions]
     fwlist remove [TCP | UDP] source_IP source_Port destination_IP
destination_Port
     fwlist remove session source_IP

     help   = shows this message
     show   = lists active sessions or connections
     remove = deletes an active session or connection
```

Example 1: (listing firewall logged users sessions)

```
#fwlist show sessions
Name/Domain                          Profile          Source IP
Start
-------------------------------------------------------------------------
administrator/BSB                    Admin            10.20.1.1
08:11:27
jackw/GOA                            Default          10.45.1.1
07:39:54
wilsont/POA                          Normal           10.57.1.1
07:58:10
antonyg/GRU                          Normal           10.78.1.1
08:01:02
maryf/BSB                            Restricted       10.22.1.1
08:48:31
lucy.sky/POA                         Restricted       10.235.1.1
10:49:44
danyt/POA                            Special          10.42.2.1
06:02:19
operator/BSB                         Default          10.151.2.1
20:44:34
```

Example 2: (deleting the session of user logged from host 10.19.1.1)

```
#fwlist remove session 10.19.1.1
Session deletion was requested to the users server
```

21-0 Configuring the SMTP proxy

This chapter shows what the features of the SMTP proxy are and how to configure it.

What is the SMTP proxy ?

The SMTP proxy is a specialized program of Aker Firewall, designed to work with electronic mail (SMTP is an anagram for *Simple Mail Transfer Protocol*, the full name of electronic mail transfer service on the Internet). This proxy enables the filtering of e-mail messages based on their contents or on any field of their header. It also works as a barrier protecting the SMTP server against several types of attacks.

It is a transparent proxy (for further information refer to the chapter Working with proxies), thus, neither the server nor the client knows about its existence.

Description of a SMTP message

In order to understand the fields filtering of the SMTP proxy, some information about the e-mail messages are necessary.

An e-mail message is formed by three distinct parts: envelop, header and body. Each of these parts has a contains specific information.

- **Envelop**

The envelop is called this way because it is similar to the envelop of a standard letter. It contains basically the sender and the recipients of a message. For each recipient of a different domain, a new envelop is generated. This way, a SMTP server receives in the envelop of a message the name of all recipients of the message which are part of its domain.

The envelop is not seen by the recipients of a message. It's used only between SMTP servers.

- **Header**

The message header contains several pieces of information about the message, like the subject, date and sender's name. The header is usually shown to the message recipient.

- **Body**

The body contains the message, as it was generated by the sender.

Attacks against a SMTP server

There are several attacks which can be target against a SMTP server. They are:

- **Bugs exploits**

In this case, the attacker tries to issue a command or arguments of a command that are known to generate security breaches.

Aker Firewall SMTP proxy blocks these attacks in the way it allows only the use of commands considered secure and validating the arguments of every command.

- **Buffer overflows**

These attacks consists of generating large command strings, causing the servers that are not correctly developed to generate security failures.

Aker Firewall SMTP proxy blocks these attacks in the way it limits the maximum command strings that can be sent to the server.

- **Relay attacks**

These attacks consist of using the SMTP server of another organization to send e-mail messages. This way, the computer resources that should be available for valid requests are consumed.

Aker Firewall SMTP proxy, if correctly configured, blocks relay attacks.

Using the SMTP proxy

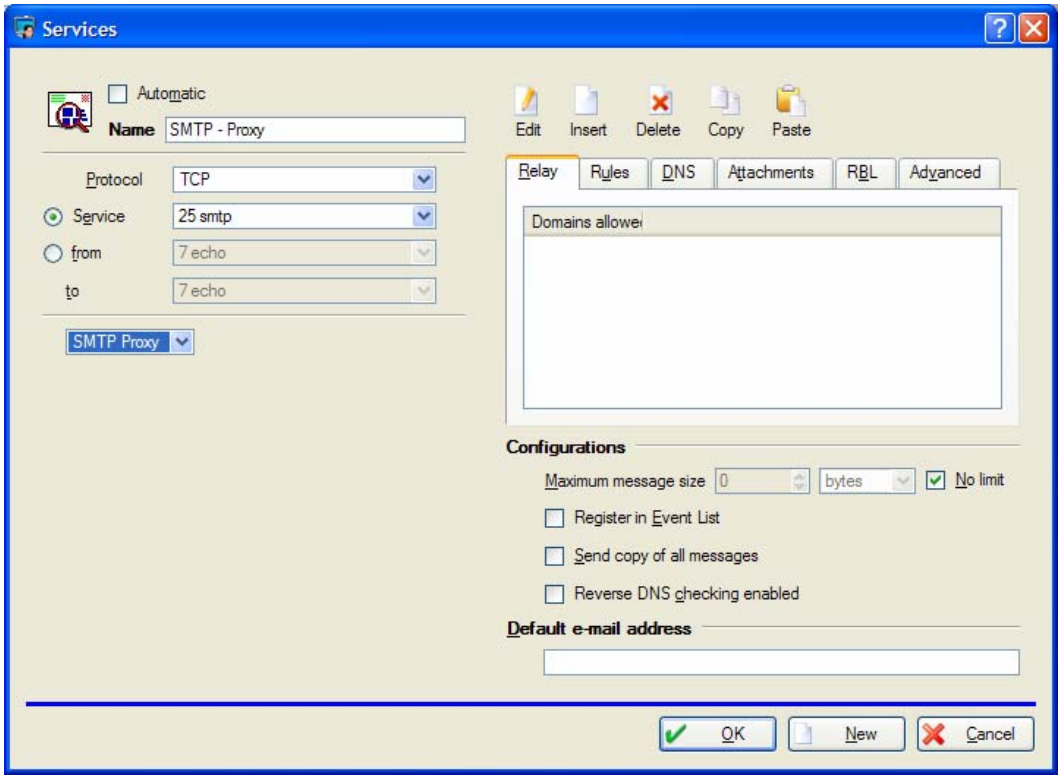
To use the SMTP proxy in a communication, it is necessary to follow two steps:

1. Create a service which will be redirected to the SMTP proxy and edit the parameters of the context to be used for this service (for further information, refer to the chapter Registering Entities)
2. Add a filtering rule allowing the use of the service created in the step 1, for the desired networks or hosts (for further information, refer to the chapter The Stateful Filter)

21-1 Configuring the parameters of a SMTP context

The properties window of a SMTP context is shown when the **SMTP proxy** option is selected, in the services edition window. Through this window it is possible to define the behavior of the SMTP proxy when dealing with a specific service.

The properties window of a SMTP context



The properties window is where all parameters of a context, associated to a specific service, are configured. It consists of some common fields followed by 6 tabs where specific parameters are configured. The common fields are:

Maximum message size: This field indicates the maximum size, in bytes, of a message in order for it to be accepted by the proxy. If it's not desired to define a maximum size, it's only necessary to check the **No limit** option, located at the right of this field.

Register in the event list: This field indicates if the messages that do not match any SMTP rule of this context will be registered in the events list.

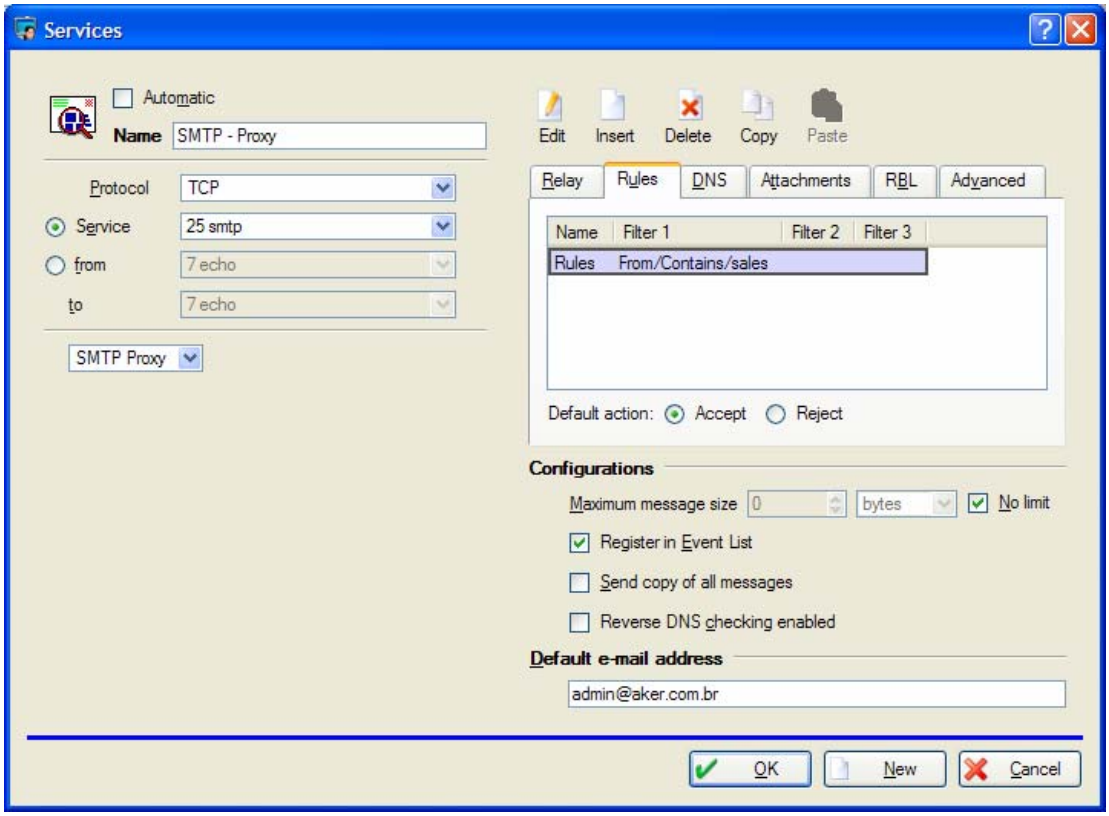
Send copy of all messages: Regardless of a message being accepted or rejected, it is possible to send a complete copy of the messages to any e-mail address. This field indicates if this copy will be sent or not.

Reverse DNS checking enabled: If this option is checked, only connections from hosts with a configured reverse DNS, pointing to a valid name, will be accepted.

Default e-mail address: It indicates the default e-mail address which copies of the messages that do not match any SMTP rule of this context will be sent to (if the option

Send copy of all messages is checked). This e-mail can also be referenced in any filtering rule of the context.

- **Relay tab**

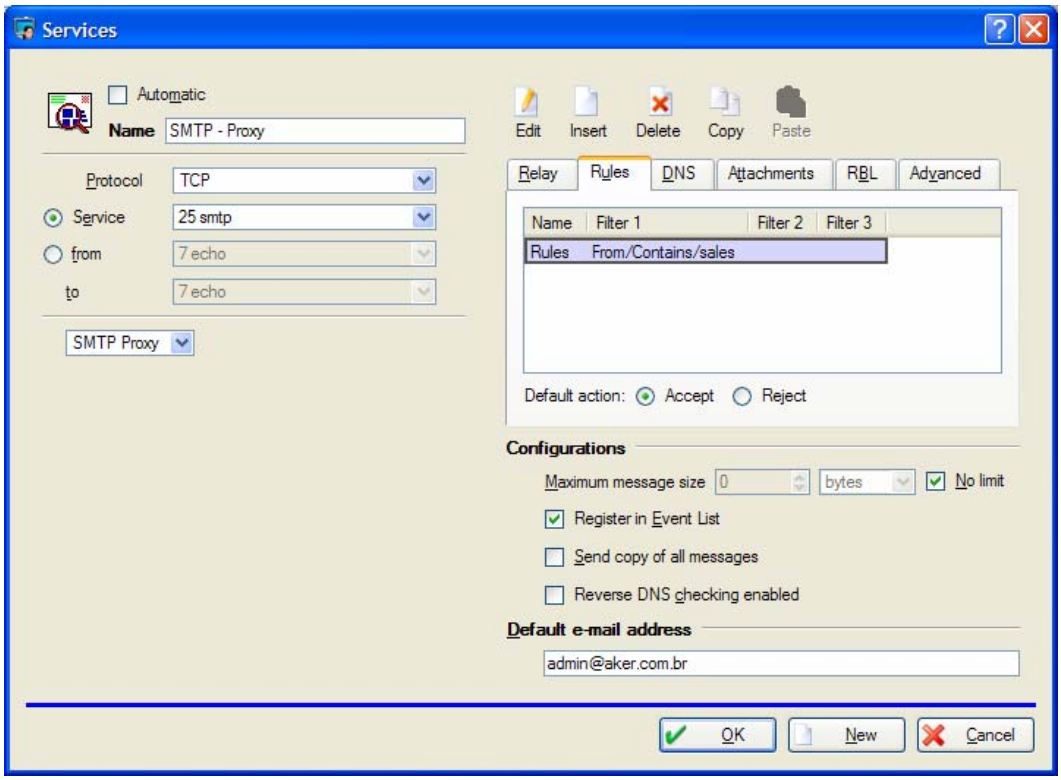


This tab allows the administrator to specify a list of valid domains to receive e-mails. E-mails sent to any domain not listed will be rejected even before their transmission begin.

If the domain list is left blank the firewall will not protect against relay, that is, it will accept e-mails to any domain.

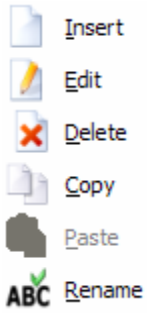
Differently from the relay control provided by SMTP servers, the firewall can only base its control on the recipients of an e-mail, and not on the sender, since it does not have the list of valid users in the protected SMTP server.

- **Rules tab**



In this tab all filtering rules for the context will be shown. These rules allow the administrator to configure filters for e-mail messages based on their contents.

In order to perform any operation on a specific rule, click the right mouse button on the rule. The following menu will appear: (this menu will be shown whenever the right button is clicked, even if there is no rule selected. In this case, only the options *Insert* and *Paste* will be enabled).



- **Insert:** This option allows the addition of a new rule in the list. If any rule is selected, the new one will be inserted in the position of the selected rule. Otherwise, the new rule will be added in the end of the list.
- **Edit:** This option opens the edition window for the selected rule.
- **Delete:** This option removes the selected rule from the list.
- **Copy:** This option copies the selected rule into a temporary area.
- **Cut:** This option removes the selected rule from the list and copies it into a temporary area.

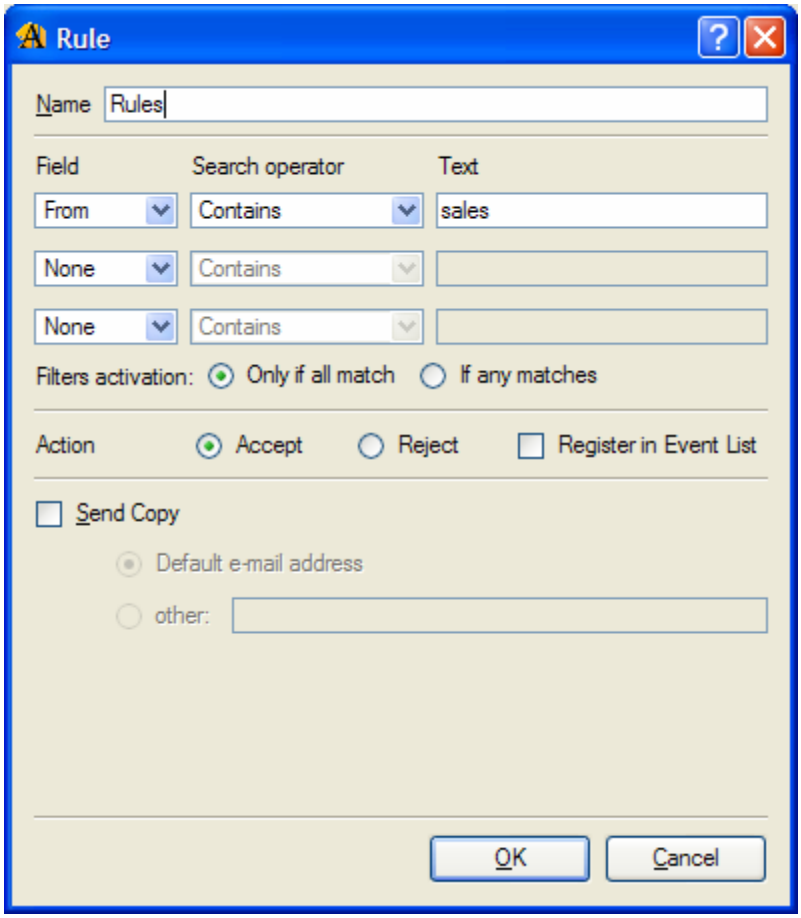
- **Paste:** This option copies the rule from the temporary area into the list. If a rule is selected, the new one will be copied in the position of the selected rule. If not, it will be copied to the end of the list.
- **Rename**: This option renames the selected rule

Hint: All these options can be accessed through the toolbar located right above the list. In this case, first select the rule, clicking on it with the left button, and then click on the desired option.

The order of rules in the list is very important. Whenever the firewall receives a message, it will search the list from the beginning looking for a rule the message matches. As soon as it is found, the action associated to it will be taken.

In the case of insertion or edition of rules, the edit window, described in the section below, will be shown:

The edit window for the SMTP rules



All the parameters related to a filtering rule for a SMTP context are configured in this window. Each rule consists basically of 3 independent conditions that may or may not be filled (in other words, it is possible to create rules with only one or two conditions).

To create a rule, it is necessary to fill in the following fields:

Name: Name that identifies the rule in the context. This name will be shown in the list of rules of the SMTP context. There cannot exist two rules with the same name.

Field: Defines the name of the field within the SMTP message where the search will take place. It can take one of the following values:

- **NONE:** The search will not be performed.
- **TO (All):** The search is performed in the destination address of the message (all of them must match the rule).
- **TO (Any)**: The search is performed in the destination address of the message (at least one has to match the rule).
- **FROM:** The search is done in the source address of the message.
- **CC:** The search is done in the list of address which will receive a copy of the message.
- **REPLY:** The search is done in the REPLY-TO field, indicating the address for which the message should be answered.
- **SUBJECT:** The search is done in the field that defines the subject of the message.
- **Header:** The search is done in all the fields that compose the header of the message.
- **Body**: The search is done in the body of the message (where the message effectively exists).

 The TO and CC fields are treated differently by the SMTP proxy: the TO field is treated as a list of all message recipients, obtained from the message envelop. The CC field is treated as a simple text, obtained from the message header, and its usefulness is very limited.

Search: Type of search to be performed in the field defined above:

- **CONTAINS**: The field to be searched must contain the supplied text in any position.
- **DOESN'T CONTAIN**: The field to be searched must not contain the supplied text.
- **IS**: The content of the field to be searched must be exactly equal to the supplied text.
- **IS NOT**: The content of the field to be searched must be different of the supplied text.
- **STARTS WITH**: The content of the field to be searched must start with the supplied text.
- **DOESN'T START WITH**: The content of the field to be searched must not start with the supplied text.
- **ENDS WITH**: The content of the field to be searched must end with the supplied text.
- **DOESN'T END WITH**: The content of the field to be searched must not end with the supplied text.
- **CONTAINS WORDS**: In this type of search, the supplied text is considered as formed by individual words (separated by spaces), instead of a continuous text. To match the search, the field must contain all the given words, regardless of their positions.

Text: Text to be searched. This field is treated as a continuous text which will be compared with the specified field, except in case of the CONTAIN WORDS search, when it is treated as several words separated by spaces. **In both cases, this field is case-insensitive.**

 The fields **Field, Search** and **Text** appear 3 times. Therefore, it is possible to define up to 3 different conditions that a message needs to fulfill in order to match the rule. If it is not desired to specify 3 conditions, just leave the value NONE on the parameter field of the conditions that will not be specified.

Filters activation: This option only makes sense when more than one condition is specified. It indicates what type of operation will be used to relate them.

- **Only if all matches**: In order for a message to match the rule, it is necessary that it satisfies all conditions.
- **If any matches**: In order for a message to match the rule, it is necessary that it satisfies one of the conditions.

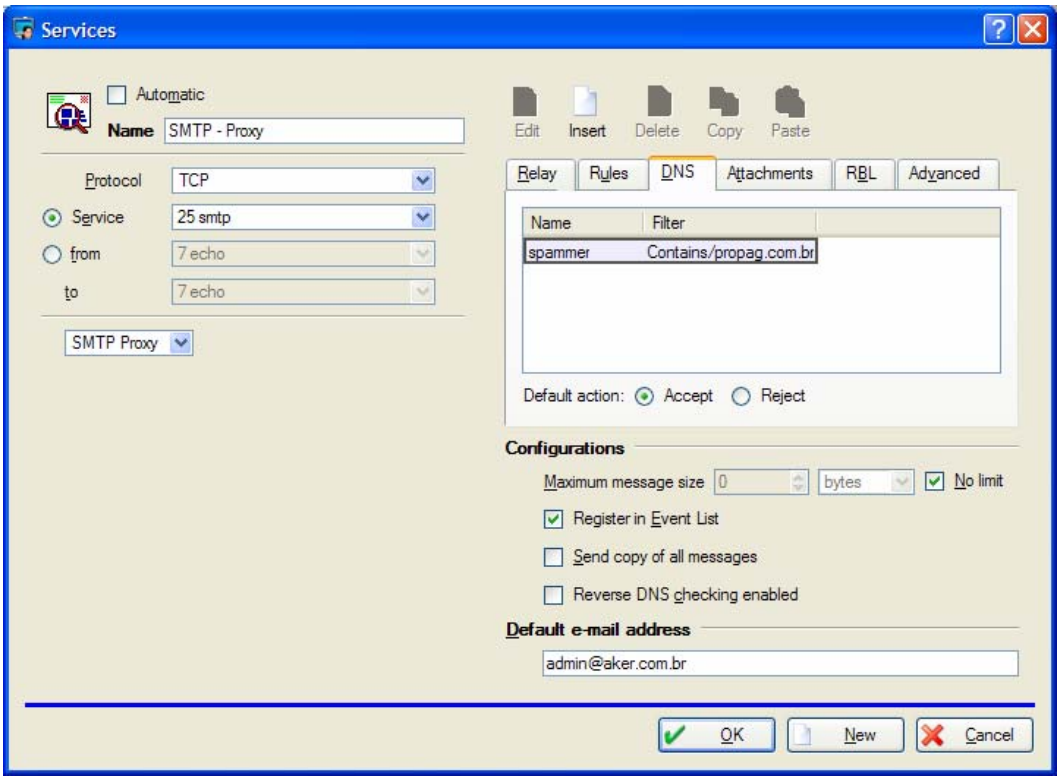
Action: The field indicates if the messages that match the rule should be accepted or rejected by the SMTP proxy.

Register in the event list: This field indicates if the messages that match the rule will be registered or not in the events list.

Send copy: For all messages that match the rule, regardless of being accepted or rejected, it is possible to send a complete copy of the message to any e-mail address. This field indicates if this copy will be sent or not. If it is checked, one of the following sending options must be chosen:

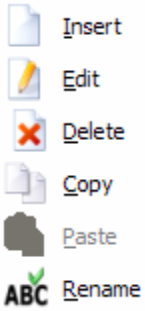
- **Default e-mail address:** The copy of the message is sent to the default e-mail address.
- **Other:** The copy of the message is sent to the address specified in the field at the right.

- **DNS tab**



In this tab all DNS filtering rules for the context will be shown. These rules allow the administrator to configure e-mail filters based on the name returned by the reverse DNS of the SMTP server that will be sending the message.

In order to perform any operation on a specific rule, click the right mouse button on the rule. The following menu will appear: (this menu will be shown whenever the right button is clicked, even if there is no rule selected. In this case, only the options *Insert* and *Paste* will be enabled).



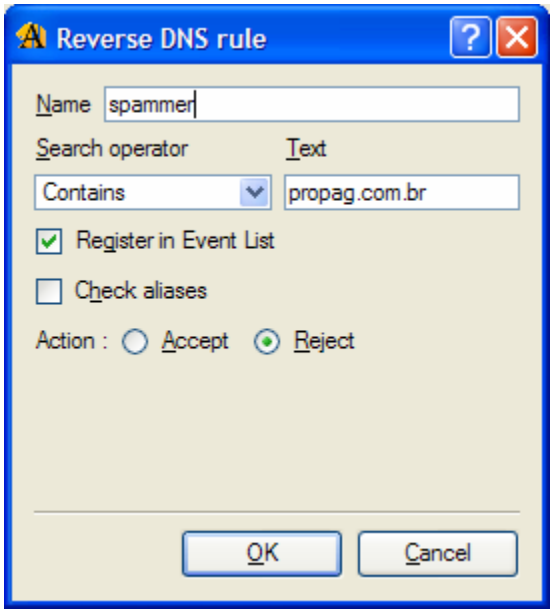
- **Insert:** This option allows the addition of a new rule in the list. If any rule is selected, the new one will be inserted in the position of the selected rule. Otherwise, the new rule will be added in the end of the list.
- **Edit:** This option opens the edition window for the selected rule.
- **Delete:** This option removes the selected rule from the list.
- **Copy:** This option copies the selected rule into a temporary area.
- **Cut:** This option removes the selected rule from the list and copies it into a temporary area.

- **Paste:** This option copies the rule from the temporary area into the list. If a rule is selected, the new one will be copied in the position of the selected rule. If not, it will be copied to the end of the list.
- **Rename**: This option renames the selected rule

Hint: All these options can be accessed through the toolbar located right above the list. In this case, first select the rule, clicking on it with the left button, and then click on the desired option.

In the case of insertion or edition of rules, the edit window, described in the section below, will be shown:

The edit window for the reverse DNS rules



To create a rule, it is necessary to fill in the following fields:

Name: Name that identifies the rule in the context. This name will be shown in the list of DNS rules of the SMTP context. There cannot exist two rules with the same name.

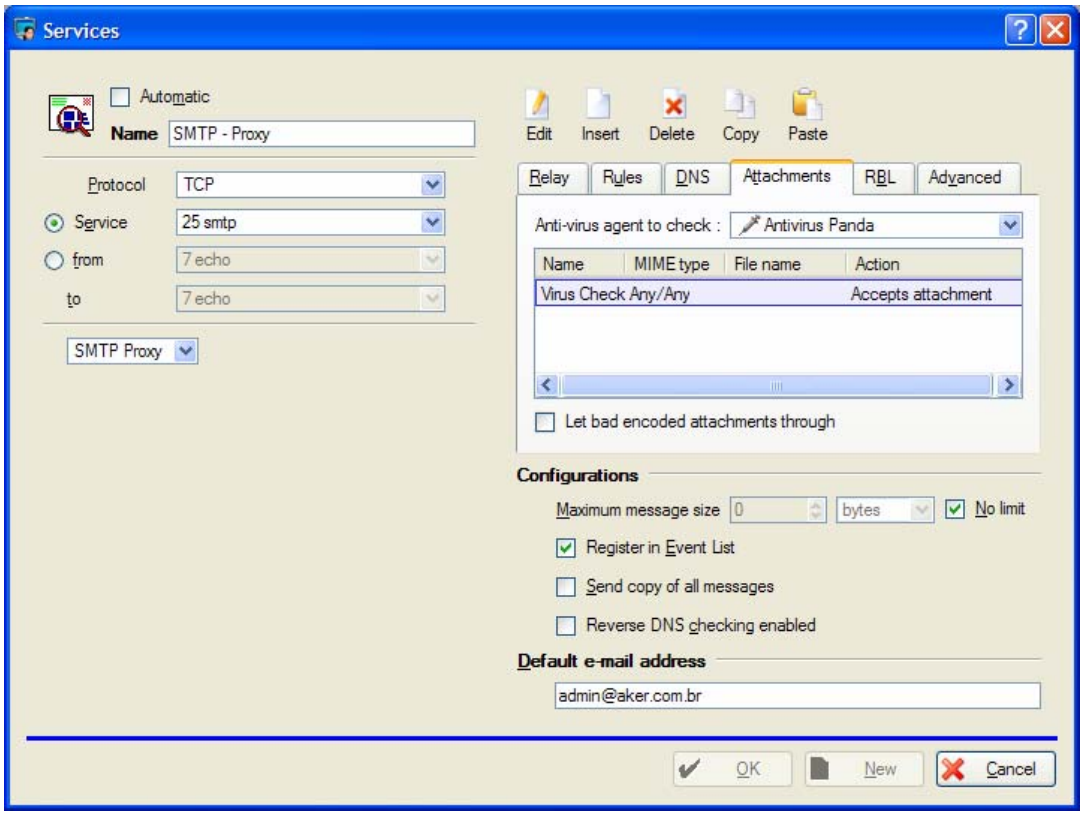
Search operator: The same operators used in the SMTP filtering rules can be used for reverse DNS filtering.

Text: Defines the text to be searched.

Check aliases: If this option is set, the firewall will compare all aliases returned by the DNS to see if any of them matches the rule.

Action: The field indicates if the messages that match the rule should be accepted or rejected by the SMTP proxy.

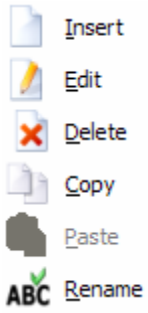
- **Attachments tab**



This tab is used to specify rules to deal with attachments. These rules allow that, if a message was accepted, its attachments to be removed or scanned for viruses. They also permit that a fully message be rejected if it contains an unacceptable file (with virus, for instance).

Antivirus agent to check: This field specifies the antivirus agent that will be used to scan files attached to e-mails. This agent must have been previously registered in the firewall. For more information, refer to chapter Registering entities.

In order to perform any operation on a specific rule, click the right mouse button on the rule. The following menu will appear: (this menu will be shown whenever the right button is clicked, even if there is no rule selected. In this case, only the options *Insert* and *Paste* will be enabled).



- **Insert:** This option allows the addition of a new rule in the list. If any rule is selected, the new one will be inserted in the position of the selected rule. Otherwise, the new rule will be added in the end of the list.
- **Delete:** This option removes the selected rule from the list.

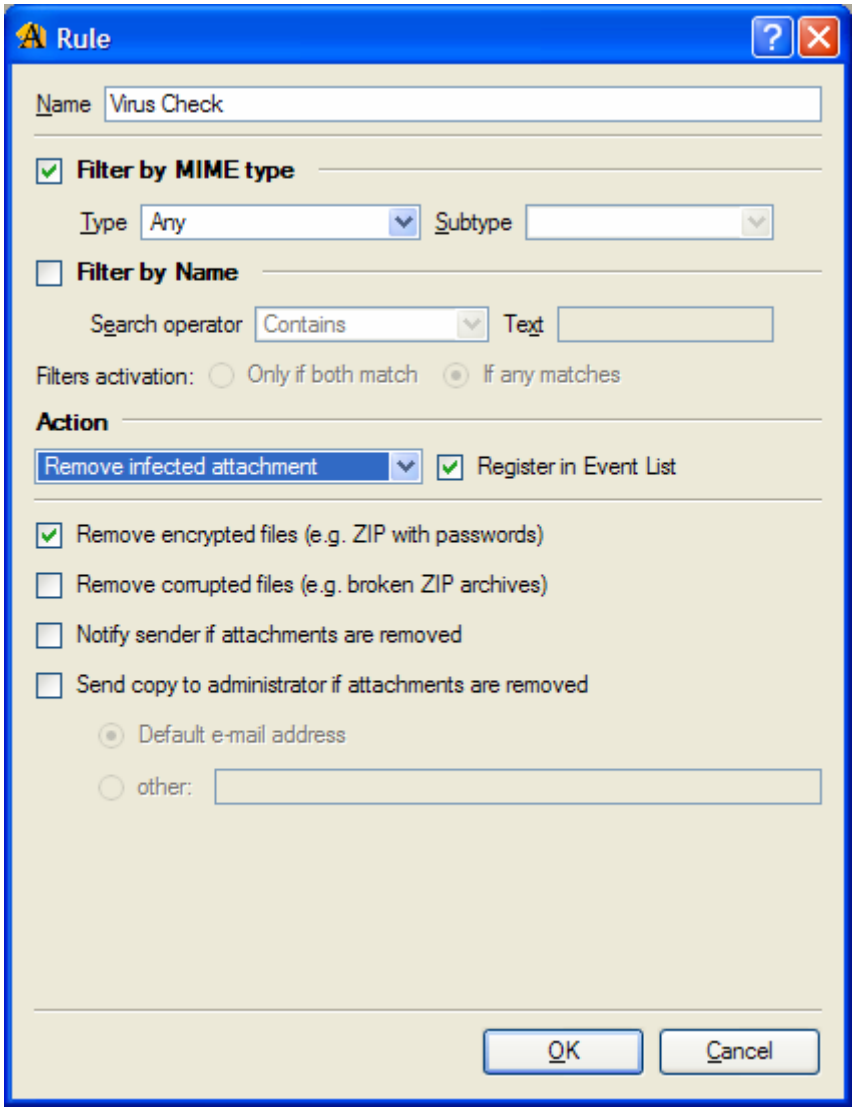
- **Edit:** This option opens the edition window for the selected rule.
- **Copy:** This option copies the selected rule into a temporary area.
- **Cut:** This option removes the selected rule from the list and copies it into a temporary area.
- **Paste:** This option copies the rule from the temporary area into the list. If a rule is selected, the new one will be copied in the position of the selected rule. If not, it will be copied to the end of the list.
- **Rename**: This option renames the selected rule

Hint: All these options can be accessed through the toolbar located right above the list. In this case, first select the rule, clicking on it with the left button, and then click on the desired option.

 The order of rules in the list is very important. For each attachment in a message, the firewall will search the list from the beginning looking for a rule that is matched. As soon as it is found, the action associated to it will be taken.

In the case of addition or edition of rules, the edit window, described in the section below, will be shown:

The edit window for attachments rules



All the parameters related to a filtering rule for attachments for a SMTP context are configured in this window. It consists of the following fields:

Name: Name that identifies the rule in the context. This name will be shown in the list of rules for attachments of the SMTP context. There cannot exist two rules with the same name.

Filter by MIME type: This field allows the creation of an attachment filtering rule based on the MIME type of the attached file. When it is checked, it is necessary to specify its type and subtype.

Filter by name: This field allows the creation of an attachment filtering rule based on (part of) the name of the attached file. When it is checked, it is necessary to specify the type of search to be performed and the text to be searched. These fields are equal to the fields of the same name of the SMTP filtering rule, described above.

Search operator: This field is equal to the field of the same name of a SMTP filtering rule, described above.

Action: Indicates which action will be taken by the firewall when a file matches the rule. It consists of three options:

- **Accept attachment**: If this option is selected the firewall will keep the attached file in the message.
- **Remove attachment**: If this option is selected the firewall will remove the attached file from the message.
- **Discard message**: If this option is selected, the firewall will reject the message.
- **Remove infected attachment**: If this option is selected the firewall will scan the attached file. If a virus is found the firewall will take one of the following actions: if the file can be disinfected, the virus will be removed and the file re-attached to the message. If the disinfection is not possible, the firewall will remove the file and add a message informing the recipient of this fact.
- **Discard infected message**: If this option is selected the firewall will scan the attached file. If a virus is found the firewall will take one of the following actions: if the file can be disinfected, the virus will be removed and the file re-attached to the message. If the disinfection is not possible, the firewall will reject the message.

 It is recommended the use of the actions that remove the attached files for incoming e-mails and the actions that reject the whole message in outgoing e-mails.

Remove encrypted files: If this option is checked, the firewall will remove the attachments that are encrypted and thus cannot be scanned.

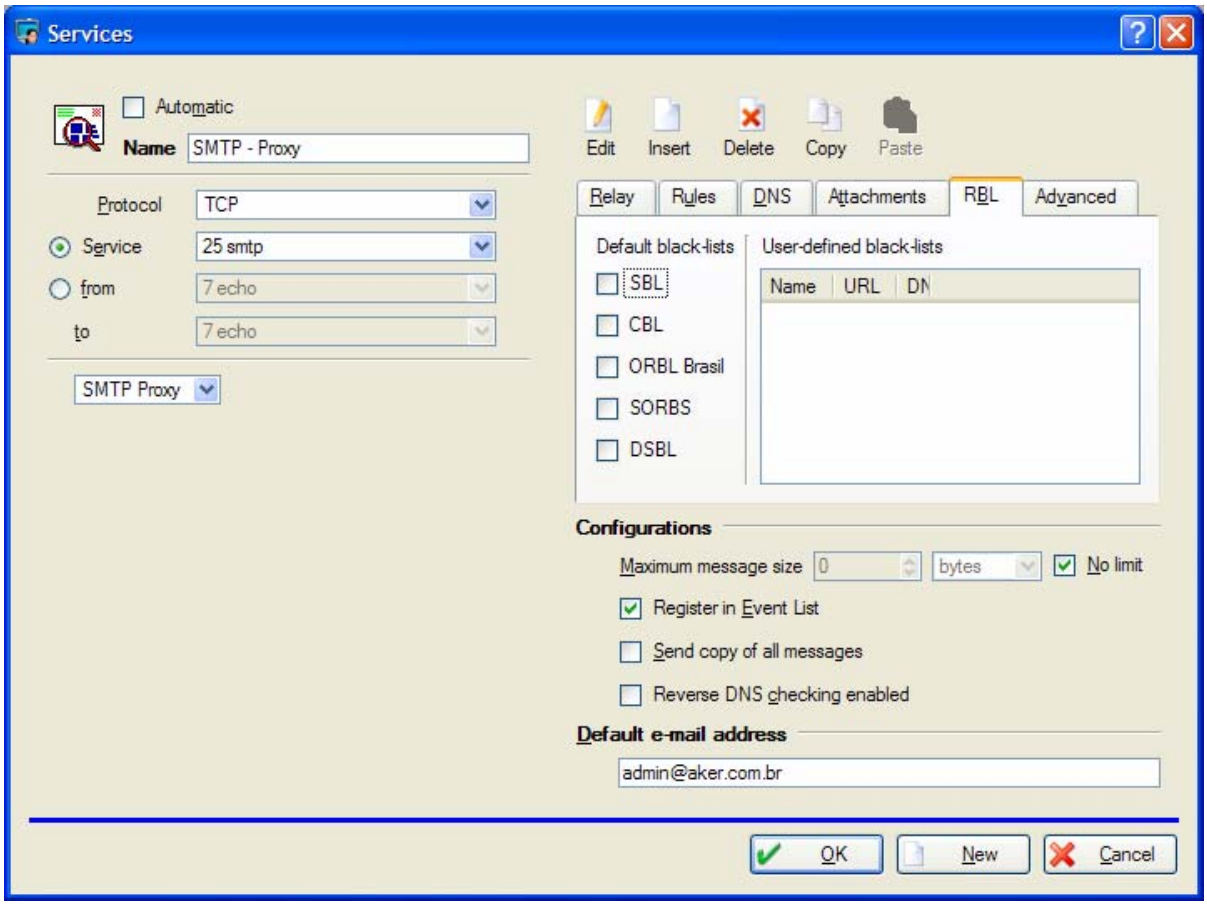
Remove corrupt files: If this option is checked, the firewall will remove the attachments that are corrupted.

Notify sender if attachments are removed: If this option is checked, the firewall will send a message to the sender of an e-mail every time one or more of its attached files are removed.

Send copy to administrator if attachments are removed: If this option is checked, the firewall will send a copy of all removed files to the administrator. If it is checked, one of the following sending options must be chosen:

- **Default e-mail address:** The copy of the message is sent to the default e-mail address.
- **Other:** The copy of the message is sent to the address specified in the field on the right.

- **RBL tab (Real-time Black List)**



This tab contains the blocking options for sites considered sources of SPAM. The blocking is performed on real-time, by consulting one or more dynamic blocking lists, maintained by third-parties. It consists of the following options:

Default black-lists: There are five black-lists that contain several hosts accused of being spammers. They are managed by organizations and the firewall just consults them before accepting each e-mail. Please enable the corresponding options if it is desired to use this feature.

- **SBL:** For more information, refer to http://www.spamhaus.com
- **CBL:** For more information, refer to http://cbl.abuseat.org
- **ORBL Brasil:** For more information, refer to http://www.globalmedia.com.br/orbl
- **DSBL:** For more information, refer to http://dsbl.org/

User-defined black-lists: These are black-lists configured by the firewall administrator. It consists of a list of black-lists, each one with the following fields:

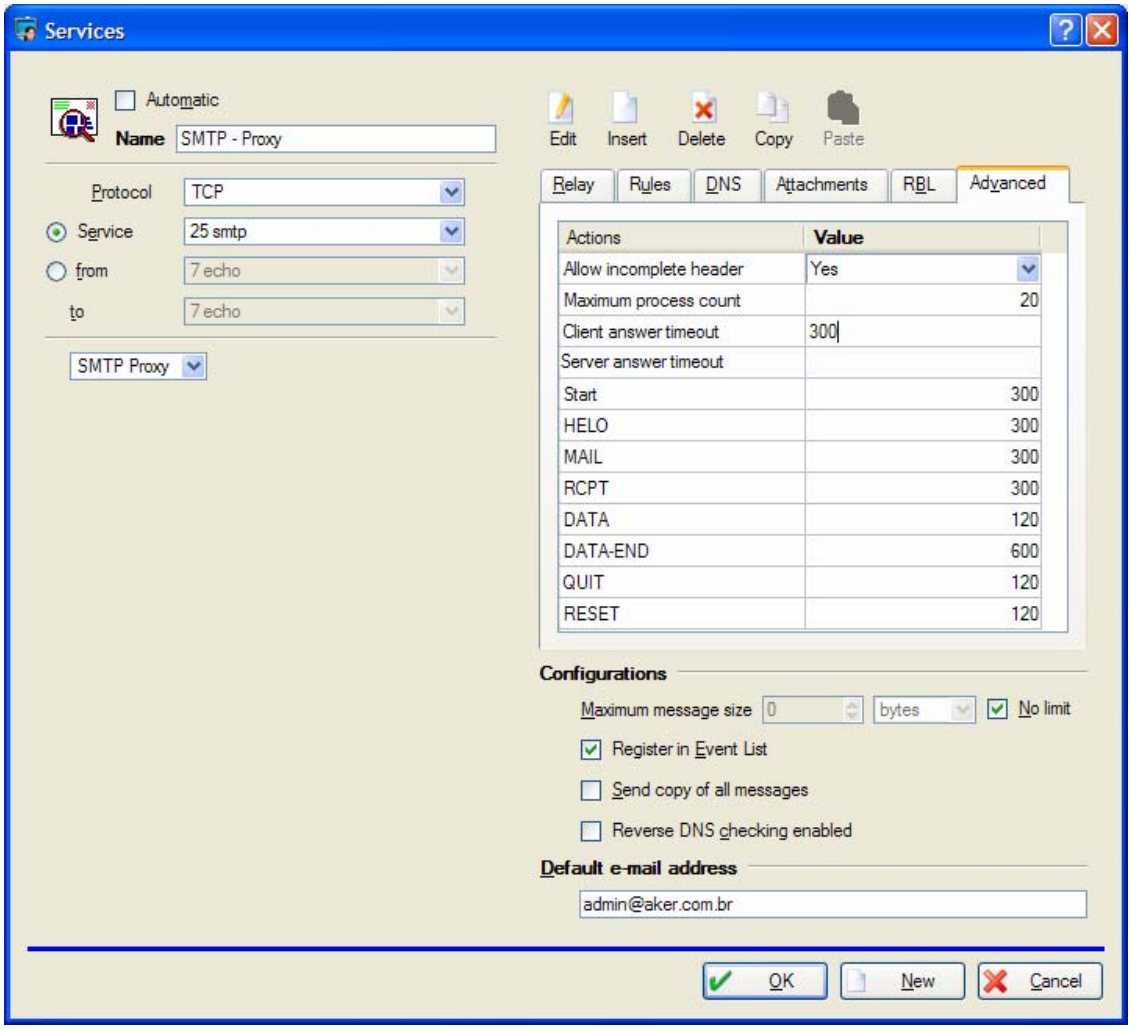
Name: Name of the black-list.

URL: It is the URL that will be shown to the users that have their messages refused, so they can gather more information.

DNS Zone: It is the complete DNS zone that will be consulted by the firewall. If an IP address is present in that zone, e-mails from it will be refused by the firewall.

Some black-list services usually have their operation interrupted temporarily due to legal issues. When this happen they become ineffective and may block more senders than they should. Please check the correct black-list functioning before using it

- **Advanced tab**



This tab allows access to the advanced configuration options of the SMTP proxy. They permit a fine tuning of the proxy. The options are:

Does not accept incomplete header: If this option is checked, messages whose headers do not contain all the mandatory fields of a SMTP message will be rejected.

Number of processes: This field indicates the maximum number of copies of the proxy that can be active in a specific moment. Since each process handles a connection, this number also represents the maximum number of messages that can be sent simultaneously to the given context. If the number of active connections reaches this limit, hosts trying to send new messages will be informed that the server is temporarily unable to accept new connections and that they should try later.

 It is possible to use this number of processes like a tool to control the maximum number of messages passing through the link.

Server response timeout: For each of the possible valid commands of the SMTP protocol, there is a maximum waiting time. If there is no answer within this period of time, the proxy assumes that the server has crashed and closes the connection. In this group it is possible to configure the maximum timeout, in seconds, for each one of these commands.

Client response timeout: This parameter indicates the maximum time, in seconds, that a proxy waits between each command of the client that is sending the SMTP message. If this time is reached, without receiving any command from the client, the proxy assumes that the host has crashed and closes the connection.

All the remaining settings refer to timeouts for each SMTP command and they shouldn't be modified unless there is a specific need to do so.

22-0 Configuring the Telnet Proxy

This chapter explains how to configure the telnet proxy to perform user authentication.

What is the Telnet proxy?

The Telnet Proxy is a special Aker Firewall program to work with the Telnet protocol. This protocol is used to emulate remote terminals. Its basic function is to enable user level authentication for telnet sessions. This type of authentication allows great flexibility and high security level.

It is a transparent proxy (for more information, see the chapter Working with proxies), therefore, neither the server, nor the client are aware of its existence.

Using the Telnet Proxy

To perform authentications in a communication using the Telnet Proxy, it is necessary to follow these 2 steps:

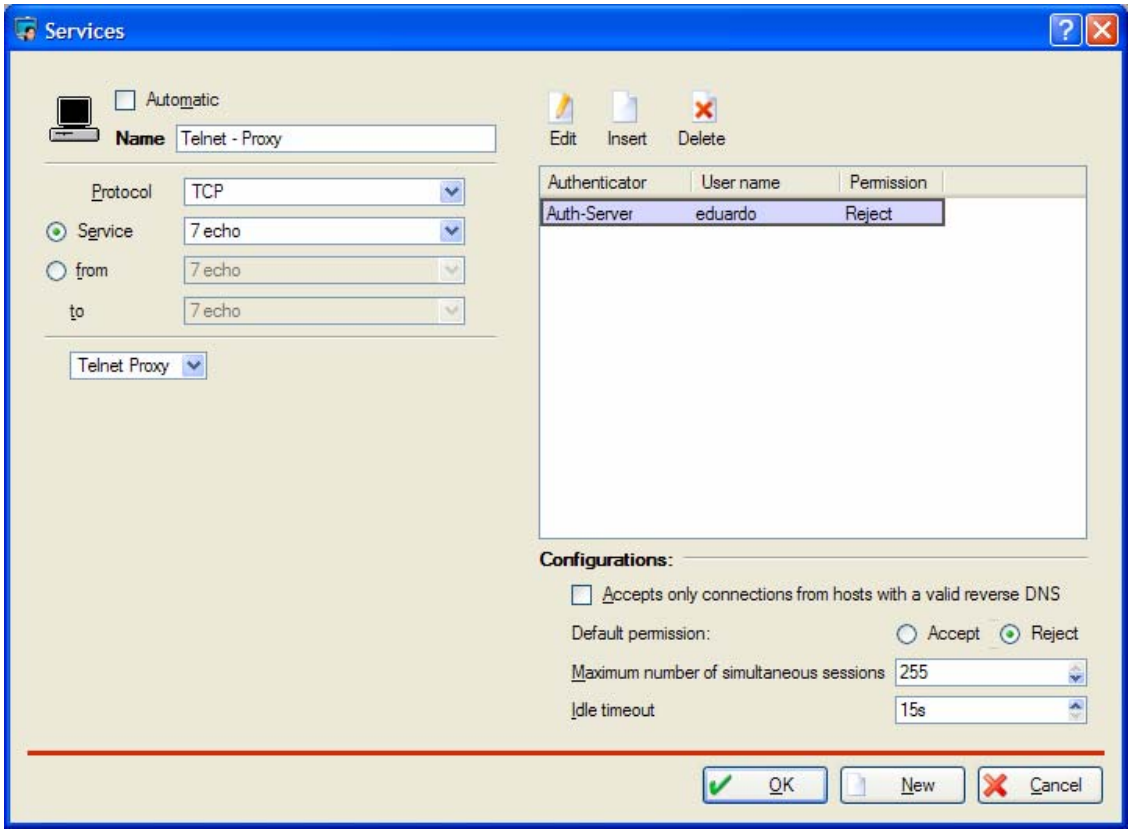
1. Create a service that will be redirected to the Telnet proxy and edit the context parameters that will be used by this service (for more information see the Registering Entities chapter).
2. Add a filtering rule allowing the use of this service by networks and desired hosts (for more information see The Stateful Filter chapter).

From now on, every time a Telnet session is established, matching the created rule, the firewall prompts for user identification and password. If identification and password are valid and the user does have permission, the session will be established. Otherwise, the user will be informed of the mistake, and the session canceled.

22-1 Configuring the parameters of a Telnet context

The properties window of a Telnet context will be displayed when the **Telnet Proxy** option is selected. The behavior of the Telnet proxy, when it is dealing with a service, is defined here.

The properties window of a Telnet context



In the properties window are configured all context parameters associated with a specific service. It has the following fields:

Accepts only connections from hosts with a valid reverse DNS: If this option is checked, only connections from hosts with configured reverse DNS pointing to a valid name, are going to be accepted.

Default Permission: This field indicates the permission applied to all users who are not present, and who are not included in any permission list group. There are two possible values. *Accept* allows establishment of Telnet session; *Reject* blocks it.

Maximum number of simultaneous sessions: This field defines the maximum number of Telnet sessions that may be simultaneously active in this context. If the number of open sessions reaches this limit, users trying to establish new connections will be informed about it and encouraged to try again later.

Idle timeout: Defines the maximum amount of time, in seconds, the proxy may remain idle without receiving data from the Telnet session, and still consider it active.

This field value must be less than, or equal to the value configured in the **TCP timeout** field, in the Global Configuration Parameters (for more information, see the chapter Configuring system parameters).

Permission List: This list defines individual user or group access permissions.

To execute any operation on a user or group in the Permission List, just right click on it. The following menu will show up: (this menu comes up every time the right mouse button is pressed, even if no user or group is selected. In this case, only the *Insert* and *Paste* options will be enabled.)

- **Insert:** This option adds a new user/group to the list. If any user/group is selected, the new one will be inserted in its position, moving it down one position on the list. Otherwise, the new one will be added to the end of the list.
- **Edit:** This option allows alteration of the selected user/group access permission.
- **Delete:** Removes selected user/group from the list.

Hint: All these options may be executed from the toolbar just above the list. In this case, first select the user/group by clicking on it, and then click on the desired toolbar option.

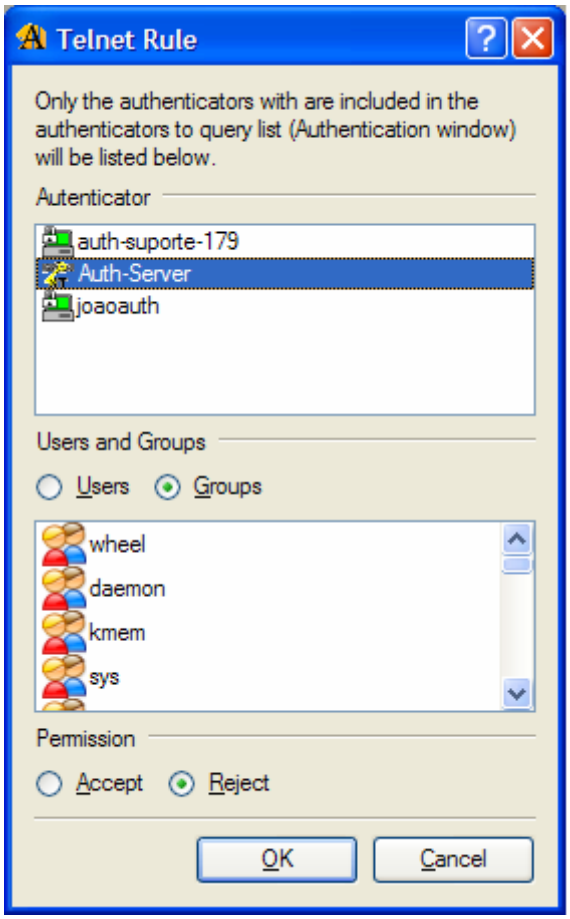
User/group order in the Permissions List is of fundamental importance. When a user is authenticated, the firewall searches the list from the beginning, looking for this user's name, or for a group to which he/she may belong. As soon as one is found, the associated permission is used.

To change a user/group position on the list, proceed as follows:

1. Select the user or group to change position.
2. Click on one of the arrow buttons, on the right. The up arrow button will move the user/group up one position. The down arrow button, one position down.

When adding users/groups, the following window will show up:

The User/Group Addition window



The inclusion window is used to configure access permission for a user or group of a specific authenticator. To do it, proceed as follows:

Select the authenticator from which a list of users or groups is desired, clicking on its name on the top list. (If it is not displayed on the list, first it is necessary to add it to the list of Authenticators to Query. For more information, see the Configuring authentication parameters chapter).

1. Select user or group list, clicking on the corresponding button located between the two lists..
2. On the bottom list, click on a user or group name you wish to add.
3. Choose the user/group access permission: accept (allows session establishment) or reject (blocks session establishment).
4. Click on **OK**. The window will be closed and the user/group will be added to the Permission List in the Context Properties window.

23-0 Configuring the FTP proxy

This chapter shows how to configure the FTP proxy to block specific file transfer commands

What is the FTP proxy?

The FTP proxy is a specialized program of Aker Firewall, designed to work with the FTP protocol, which is the protocol used for file transfers in the Internet. Its basic function is to allow the definition of commands that can be accepted and block, for example, the creation of new files or directories.

It is a transparent proxy (for further information refer to the chapter Working with proxies), thus, neither the server nor the client knows about its existence.

Using the FTP proxy

To use the FTP proxy to perform authentications in a communication, it is necessary to follow two steps:

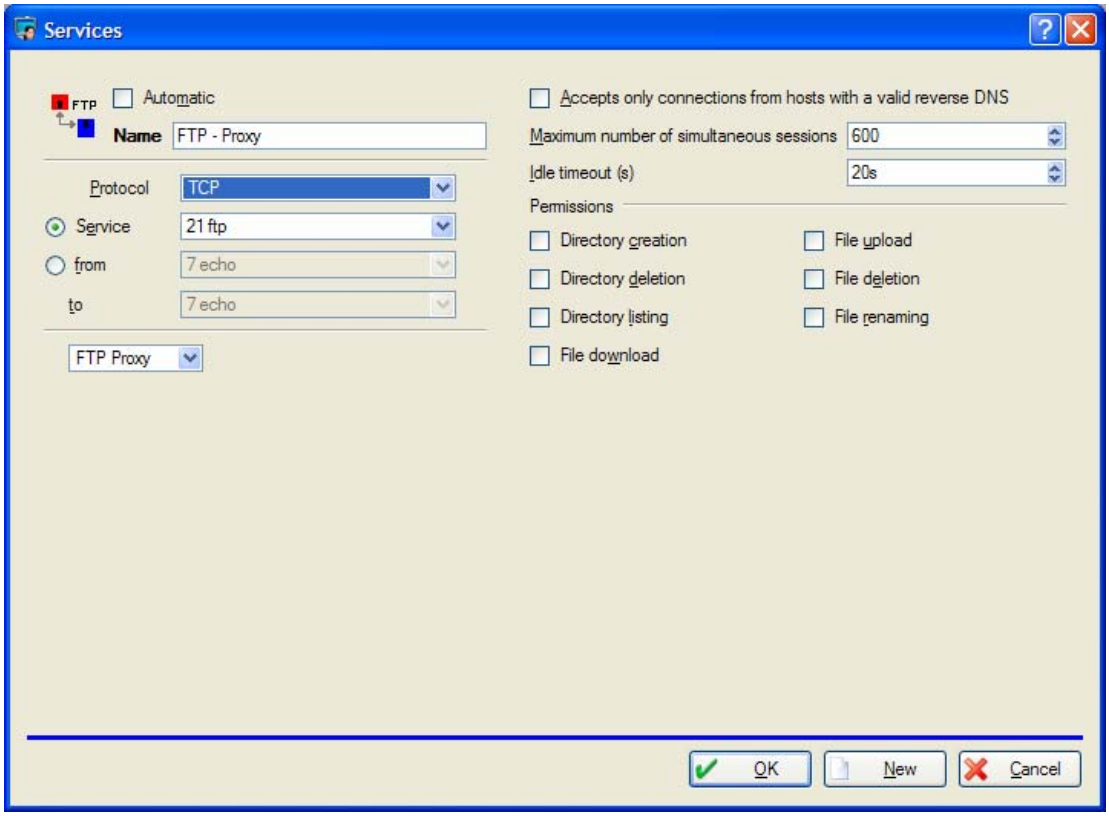
1. Create a service which will be redirected to the FTP proxy and edit the parameters of the context to be used for this service (for further information, refer to the chapter Registering Entities).
2. Add a filtering rule to enable the use of the service created in step 1, for the desired networks or hosts (for further information, refer to the chapter The Stateful Filter).

The FTP proxy does not perform user authentication. To allow certain users to have different privileges, it is necessary to create proxy FTP services with different contexts and associate each of these services with an access profile. For more information about access profiles, refer to chapter User access profiles.

23-1 Configuring the parameters of a FTP context

The properties window of a FTP context is shown when the **FTP Proxy** option is selected, in the services edition window. Through this window it is possible to define the behavior of the FTP proxy when dealing with a specific service.

The properties window of a FTP context



The properties window is where all parameters of a context, associated to a specific service, are configured. It consists of the following fields:

Accepts only connections from hosts with a valid reverse DNS: If this option is checked, only connections from hosts with a configured reverse DNS, pointing to a valid name, will be accepted.

Maximum number of simultaneous sessions: This field defines the maximum number of FTP sessions that can be simultaneously active in this context. If the number of open sessions reaches this limit, the users who try to establish new connections will be informed that the limit has been reached and that they should try again later.

Idle timeout: This item defines the maximum amount of time, in seconds, that the proxy can stay without receiving data from the FTP session and still consider it active.

The value of this field should be less or equal to the value configured in the **TCP Timeout** field, on the global configuration parameters. (for further information, refer to the chapter Configuring the system parameters)

Directory creation: If this option is unchecked, it will not be possible to create directories through FTP connections that belong to this context.

Directory deletion: If this option is unchecked, it will not be possible to remove directories through FTP connections that belong to this context.

Directory listing: If this option is unchecked, it will not be possible to view the contents of directories (`DIR` or `LS` commands) through FTP connections that belong to this context.

File download: If this option is unchecked, it will not be possible to download files through FTP connections that belong to this context.

File upload: If this option is unchecked, it will not be possible to upload files through FTP connections that belong to this context.

File deletion: If this option is unchecked, it will not be possible to delete files through FTP connections that belong to this context.

File renaming: If this option is unchecked, it will not be possible to rename files through FTP connections that belong to this context.

24-0 Configuring the POP3 Proxy

In this chapter, we will explain the POP3 proxy functions and configuration.

What is the POP3 Proxy?

The POP3 proxy is a special Firewall Aker program, designed to work with email (POP3 is an acronym for *Post Office Protocol*, which is the full name of the service that downloads email messages in the Internet). This proxy enables email filtering based on their attachment files. It also acts as a shield, protecting the POP3 server against several types of attacks.

It is a transparent proxy (for more information, see the Working with Proxies chapter), thus, neither the server nor the client are aware of its existence.

Attacks Against a POP3 Server

There are several types of possible attacks against a POP3 server:

- **Attacks that explore *bugs* in a server**

In this case, the attacker tries to use a command or command parameter that, knowingly, causes security failures.

Aker Firewall POP3 proxy avoids these attacks because it only allows utilization of commands considered secure, and it validates all commands parameters.

- **Attacks that explore buffers overflow**

These attacks consist of sending very long command lines to a server, which, when not correctly developed, will present security failures.

Aker Firewall POP3 proxy blocks these attacks by limiting command line length that may be sent to the server.

Using the POP3 proxy

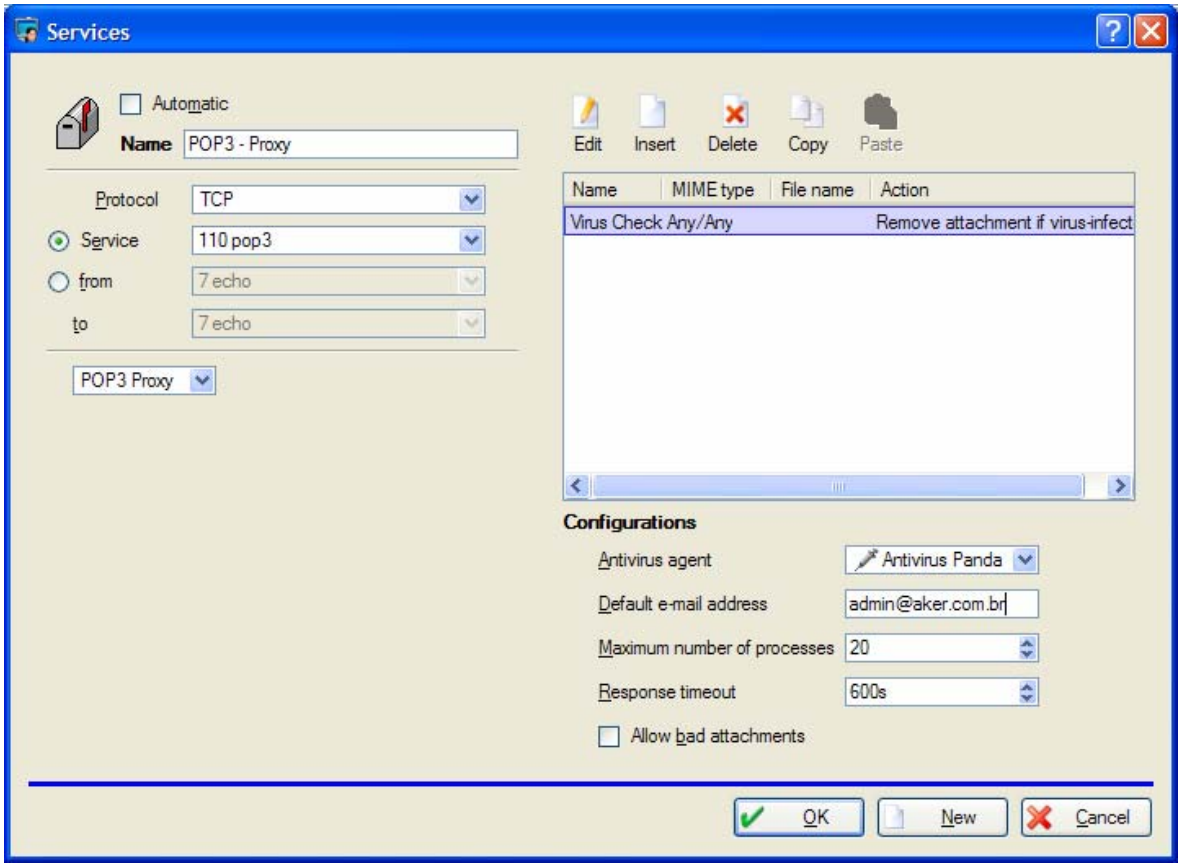
To use the POP3 proxy in a communication, two steps are necessary:

1. Create an Entity of the Service type, that will be redirected to the POP3 proxy, and edit the context parameters that will be used by this service (for more information, see the chapter Registering Entities).
2. Add a filtering rule allowing the use of the service created in step 1 by the networks or desired hosts (for more information, see the chapter The Stateful Filter).

24-1 Configuring the parameters of a POP3 Context

When the **POP3 Proxy** option is selected, the POP3 Context Properties window shows up. In this window, we configure the POP3 Proxy behavior for the service being created.

The POP3 Context Properties Window



All parameters of a context associated to a specific service are configured in the Properties window. They are:

Configurations: It is made up of several fields that indicate actions to be performed by the POP3 proxy.

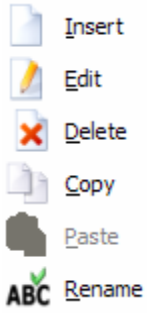
- **Antivirus agent:** This field identifies the antivirus agent that will be used to check e-mail attachments. This agent must have been previously registered in the firewall. For more information, see the chapter Registering Entities.
- **Default e-mail address:** Indicates the default e-mail address where copies of all messages that don't match any of the context rules will be sent to (if the option **Send Copy** is checked). This e-mail can also be used in any context filtering rule.
- **Maximum number of processes:** This field indicates the maximum number of proxy copies that can be active at a given time. Because each process deals with a connection, this number also represents the maximum number of messages that can be simultaneously transmitted to that specific context. If the number of

active connections reaches this limit, clients trying to send new messages will have to try again at a later time.

- **Response timeout:** This parameter indicates the maximum amount of time, in seconds, that the proxy waits for an idle connection. If this time is reached, the proxy terminates the connection.
- **Let bad attachments go through:** Allows corrupted attachments to pass through the firewall into mailboxes.

List of rules: In this list filtering rules for attachments are specified, determining whether a message will have its attachments removed or scanned for viruses.

To perform any operation on a specific rule, just right click on it. The following menu shows up: (This menu will always show up when the right mouse button is pressed, even if no rule is selected. In this case, just the *Insert* and *Paste* options will be enabled).



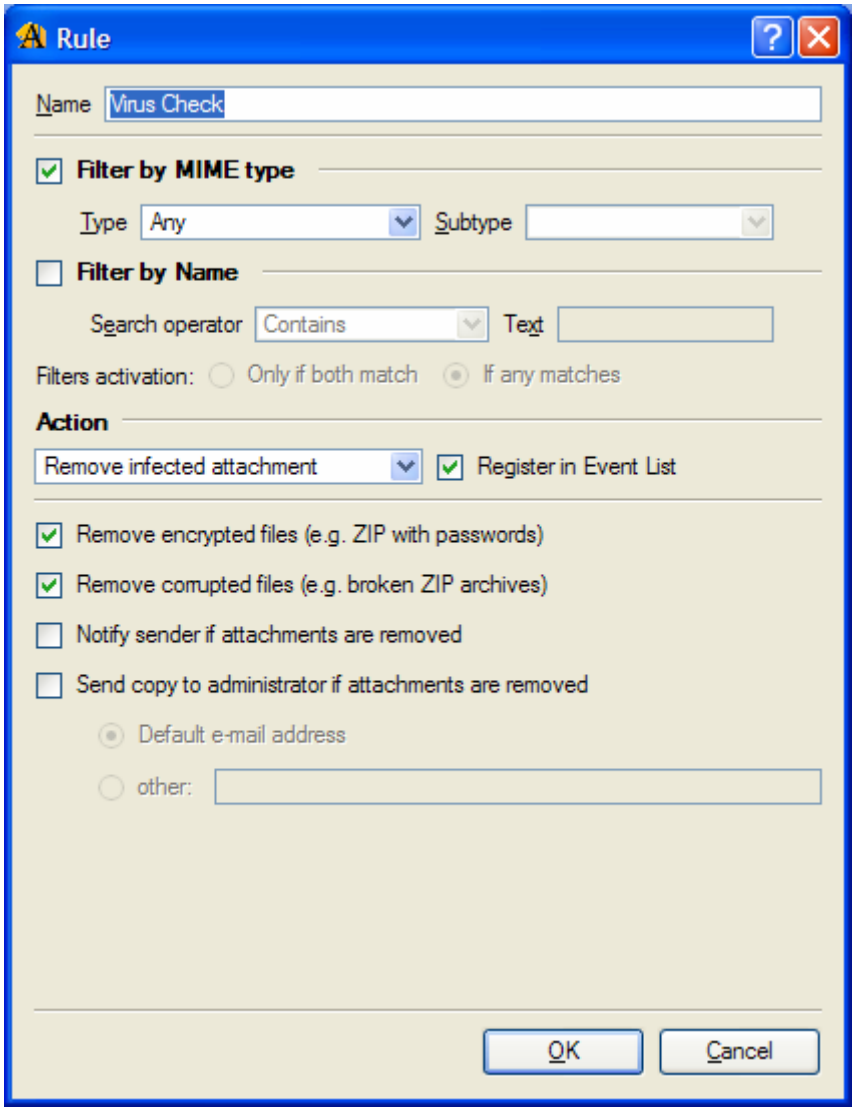
- **Insert**: This option adds a new rule to the list. If any rule is selected, the new one will be inserted in its position, pushing it down the list. Otherwise, the new rule will be added in the end of the list.
- **Edit**: This option opens the editing window for the selected rule.
- **Delete**: Removes the selected rule from the list.
- **Copy**: This option copies the selected rule into a temporary area.
- **Paste**: This option copies the rule from the temporary area into the list. If any rule is selected, the new one will be copied into its position, pushing it down. Otherwise, it will be copied at the end of the list.
- **Rename**: This option renames the selected rule.

Hint: All these options may be executed from the toolbar just above the list. First select the rule and then click on the desired option.

The order of the attachment filtering rules is extremely important. For each message attachment, the firewall searches the list from the beginning, looking for a matching rule. As soon as a match is found, the associated action is executed.

The window below shows up when rules are being added or edited:

The attachment rule editing window



All parameters concerning attachment filtering rules for a POP3 context are configured in this window. It has the following fields:

Name: Name that uniquely identifies the rule within the context. This name will be shown in the rules list. There cannot be two rules with the same name.

Filter by MIME type: This field allows definition of a file filtering rule based on its MIME type. When selected, type and subtype must be specified.

Filter by Name: This field allows filtering by the name of attached file (or part of it). When checked, the type of search to be performed and the text to be searched must be provided. The following search options are available:

- **CONTAINS**: The name must contain the supplied text in any position.
- **DOESN'T CONTAIN**: The name must not contain the supplied text.
- **IS**: The content of the name must be exactly equal to the supplied text.
- **IS NOT**: The content of the name must be different of the supplied text.
- **STARTS WITH**: The name must start with the supplied text.
- **DOESN'T START WITH**: The name must not start with the supplied text.

- **ENDS WITH**: The name must end with the supplied text.
- **DOESN'T END WITH**: The name must not end with the supplied text.
- **CONTAINS WORDS**: In this type of search, the supplied text is considered as formed by individual words (separated by spaces), instead of a continuous text. To match the search, the nzme must contain all the given words, regardless of their positions.

Filters Activation: If the option **Filter by MIME type** and **Filter by Name** have been selected, this field determines if the rule must be applied **Only if both match** (**AND** value) or **If any one matches** (**OR** value).

Action: Indicates action to be taken by the firewall when a file matches the rule. It has three options:

- **Accept attachment:** If this option is selected, the firewall will keep the file attached to the message.
- **Remove attachment**: If this option is selected, the firewall will remove the attached file from the message.
- **Remove infected attachment:** If this option is selected, the firewall will check the attachment for virus. If the file is infected, the firewall will either: if the file can be disinfected, remove the virus and attach the file back to the message. If the file cannot be disinfected, the firewall will remove the attachement and add a message informing the recipient of its action.

If the **Register in Event List** box is checked, rule matches will be registered in the events log.

Remove encrypted files: The firewall will remove zipped with passwords and encrypted attachments, because it won't be able to scan them for viruses.

Remove corrupted files: If this option is checked, the firewall will remove zipped attachments that are corrupted, once it won't be able to scan them for viruses.

Notify sender if attachments are removed: The firewall sends a message to the message sender every time one or more of its attachments are deleted.

Send copy to administrator if attachments are removed: The firewall sends a copy of all deleted attachments to the administrator. If this option is selected, one of the following options must be chosen.

- **Default e-mail address:** The copy of the message is sent to the default e-mail, defined in the Context Properties window.
- **Other**: The copy of the message is sent to the address specified in the field to the right.

25-0 Configuring the WWW Proxy

In this chapter, we will show the use and configuration of the WWW proxy.

25-1 Planning the Installation

What is Aker Firewall WWW Proxy?

Aker Firewall WWW proxy is a program specialized in working with protocols of the so-called WWW (*World Wide Web)*. Among these protocols, there are HTTP, HTTPS, FTP, and Gopher.

The main function of this proxy is to control internal user access to the Internet. It determines who can access which pages, or transfer files, for example. In addition, it can also block technologies considered dangerous to some installations, such as Active-X™, scripts (JavaScript), and even Java applets. Furthermore, it enables removal of banners from webpages, as a way to increase load speed and reduce link usage.

It is both a transparent (only for HTTP) and non-transparent proxy (for further information refer to chapter Working with Proxies) making system installation easier.

When used transparently, the proxy is usually faster than when used as a normal proxy, and it does not need extra client configuration. On the other hand, URL filtering capability for HTTPS, FTP, and GOPHER protocols only exists in the normal proxy.

In order for the non-transparent proxy to have the same performance as the transparent one, it is necessary that the browsers support HTTP 1.1 requests sent via proxies.

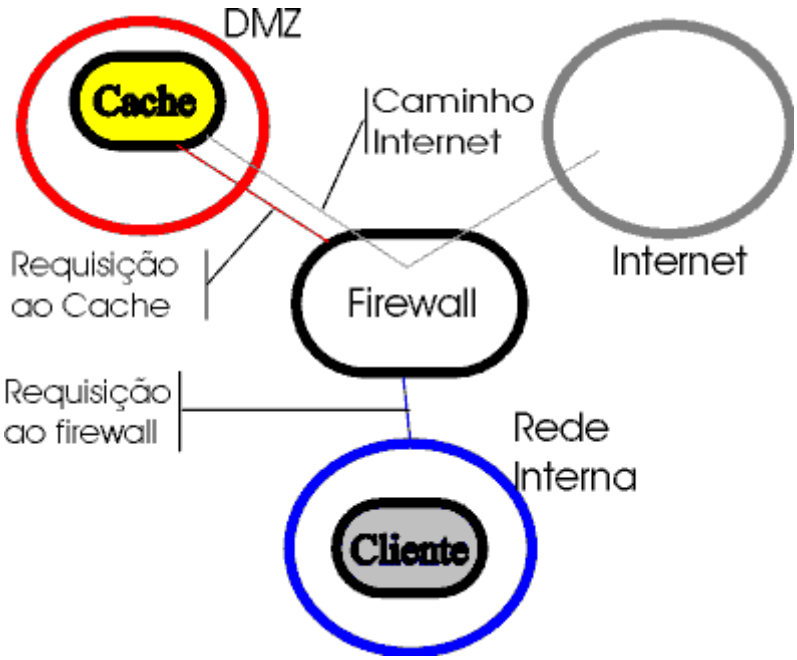
What is a WWW Cache Server?

A cache server is a program used to increase access speed to Internet pages. To do this, the program internally stores most pages commonly used by several client hosts, and every time it receives a new request, it verifies if the desired page is already stored. If available, the page is returned immediately, without the need to consult the external server. Otherwise, the page is regularly loaded from the server and stored, which will speed up responses to future requests of this page.

Aker Firewall WWW Proxy Working with a Cache Server

Firewall Aker, by itself, does not implement a cache server in its WWW proxy, however, it can be configured to work with any server that follows market standards. This cache server can run in the same machine where the firewall is, or in a separate one.

If a cache server is installed in a separate host (recommended), this host must be in a different subnet from the clients'. Otherwise, all security control can be easily bypassed. This type of configuration can be visualized in the following diagram:



To ensure total protection in this type of installation, it is just necessary to configure the stateful filter (for more information, see The Stateful Filter chapter) to only allow the host with the cache to access WWW services, and to prohibit client hosts to open connections with it. This done, next step is to configure all client hosts to use the firewall WWW proxy, and configure the firewall to use the cache in the desired machine.

Using the WWW Proxy

To use Aker Firewall WWW proxy in non-transparent mode (normal), take the following steps:

1. Create access profiles and assign them to desired users and groups. This procedure was described in the User Access Profiles chapter.
2. Edit the WWW proxy configuration parameters (which will be described in the Editing WWW Proxy Parameters session).
3. Create a filtering rule allowing client hosts to access the proxy (for more information, refer to The Stateful Filter chapter).

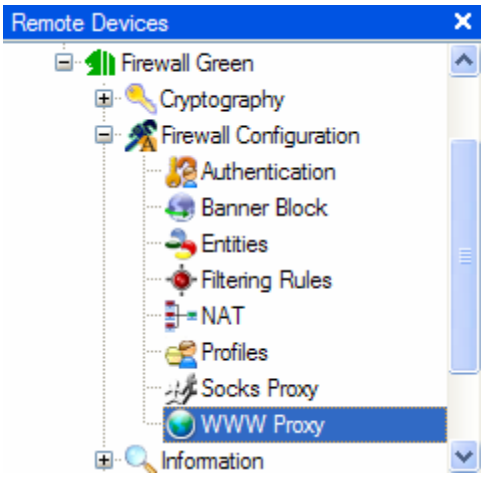
The non-transparent WWW proxy listens for connections to port 80, using the TCP protocol. If needed, this value can be altered to any port, just by adding the **-p *port#*** parameter, where ***port#*** is the number of the listened port, when initiated. This call can be found in **/etc/firewall/rc.aker** file and must be altered from **/etc/firewall/fwhttppd** to **/etc/firewall/fwhttppd -p 8080**, for example.

To use Aker Firewall WWW proxy in transparent mode (only with HTTP protocol) do the following:

1. Create a service that will be redirected to the transparent WWW proxy (HTTP), and edit the context parameters to be used by this service (for more information, see the Registering Entities chapter).
2. Add a filtering rule allowing the use of the service created in step 1 by desired networks or hosts (for more information see The Stateful Filter chapter).

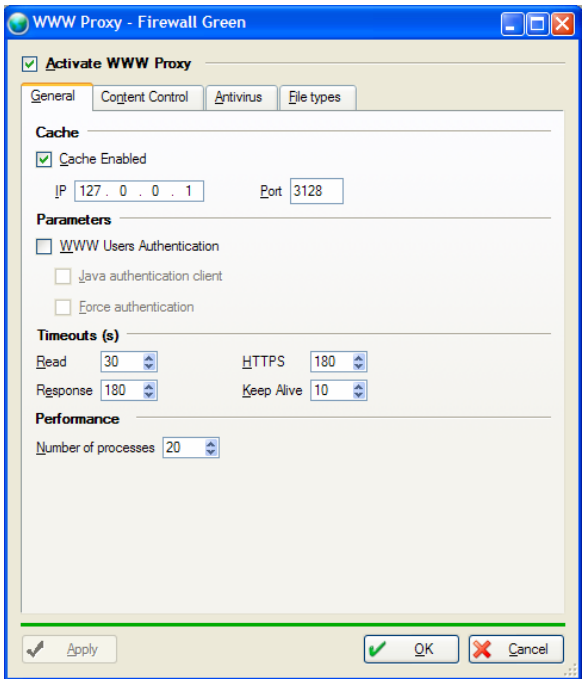
25-2 Editing the WWW Proxy Parameters

To use the WWW proxy, it is necessary to define some parameters that will determine basic characteristics of its operation. This definition is done in the WWW Proxy Configuration window. To access it:



- Click on the *Firewall Configuration* menu in the firewall window
- Select *WWW Proxy*

The WWW proxy parameters configuration window



- The **OK** button closes the WWW proxy configuration window and saves all modifications.

- The **Apply** button sends all modifications to the firewall and keeps the window open.
- The **Cancel** button discards alterations and closes the window.

General tab

- **Cache**

Cache enabled: This option defines if the WWW proxy will redirect its requests to a cache server. If enabled, all requests received will be redirected to a cache server, in the specified IP address and port. Otherwise, the WWW proxy will handle all requests.

IP: This field specifies the cache server IP address to where all requests will be redirected if the *Cache Enabled* option is active.

Port: This field specifies the port in which the cache server will wait for connections if the *Cache Enabled* option is active.

- **Parameters**

These fields allow adjustment of the WWW proxy for special situations:

WWW Users Authentication: This field activates or not WWW proxy user authentication. If checked, every time a user tries to initiate a session, a user identification and password will be requested. And the session will only be initiated if user is authenticated by one of the authenticators.

Java Authentication Client: This option tells the proxy to use the Java Authentication Client, even when operating in non-transparent mode. The advantage of this client is that it allows complete user authentication (as when using Authentication Client for Windows, and not only for the WWW proxy).

If Aker Authentication Client for Windows is being used and there is an open session with the Firewall, then name and password will not be requested, i.e., the proxy will behave as if it were not performing user authentication, when it is, in fact, doing it. If the Authentication Client session is finished, the proxy will request username and password for the next access. For more information on Aker Authentication Client, read Aker Authentication Client chapter).

To make the Java Authentication Client work in your browser, it must have Java support installed and enabled, and allow use of UDP protocol for Java applets. Only in Microsoft Internet Explorer this option comes disabled by default. To enable it, you must choose personalized security configurations for Java, and allow unsigned applets to have access to all network addresses.

Force Authentication: If this option is checked the proxy will enforce user authentication, that is, it will allow only access to authenticated users. If it is unchecked and an user decides to be authenticated (in order to be associated with an access profile

different from the default), he will be allowed to do so, but unidentified accesses will be allowed.

- **Timeouts**

Read: This parameter defines the maximum amount of time, in seconds, that the proxy will wait for a client request, from the moment that a new connection was established. If this time is reached without a client request, the connection will be canceled.

Response: This parameter defines the maximum amount of time, in seconds, that the proxy will wait for a response of a request sent to the remote WWW server, or to the cache server, in case the *Cache Enabled* option is active.

HTTPS: Defines the maximum amount of time, in seconds, that the proxy can wait without receiving data from the client, or the server, in an HTTPS connection, before it considers the connection inactive and cancels it.

Keep Alive: Defines how much time a user can maintain a "keep-alive" (HTTP 1.1) connection inactive, before the proxy terminates it, freeing process to another user. It is recommended to keep this time low enough, as to avoid unnecessary use of all system processes.

- **Performance**

Number of processes: This field defines the number of WWW proxy processes that will remain active waiting for connections. Because each process handles only one connection, this field also defines the maximum number of requests that can be simultaneously dealt with.

 To increase performance, WWW proxy processes will remain always active, independently if they are responding to requests or not.

 Generally, we should work with values ranging from 5 to 60 in this field, depending on the number of client hosts that will use the proxy (it is important to emphasize that a single host usually opens up to four simultaneous connections to access a single WWW page). The 0 (zero) value turns unfeasible the proxy utilization.

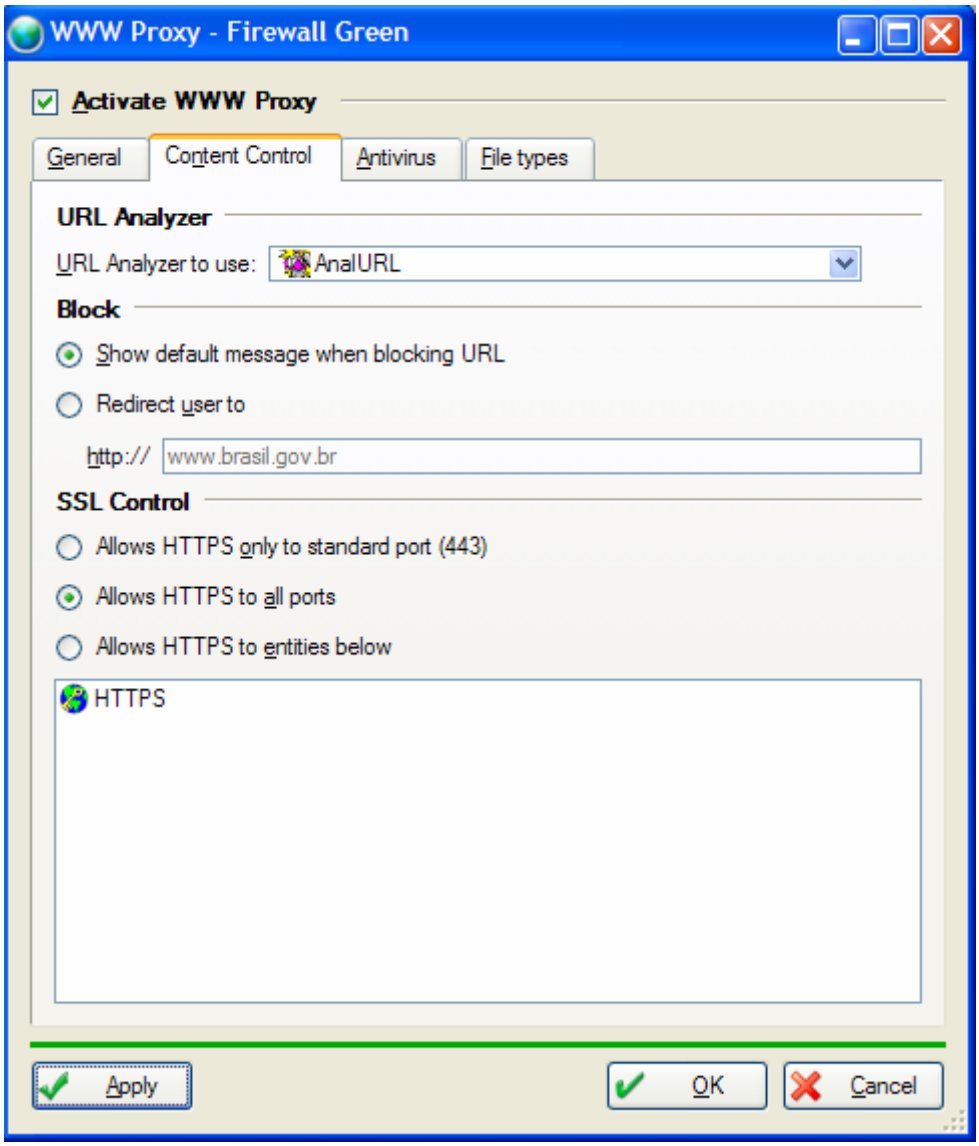
- **Block**

This option determines what the firewall should do when a user tries to access a non-authorized URL. The following options are available:

Show default message when blocking URL: If this option is checked, the firewall will display an error message informing that the desired URL is blocked.

Redirect user to: If this option is selected, the firewall will redirect all access attempts to blocked URLs to another URL specified by the administrator in the field below it (without the http:// prefix).

Content control tab



URL Analyzer: This field specifies the URL analyzer agent being used to categorize Internet pages. This agent must have been previously registered in the firewall. For more information, see the Registering Entities chapter.

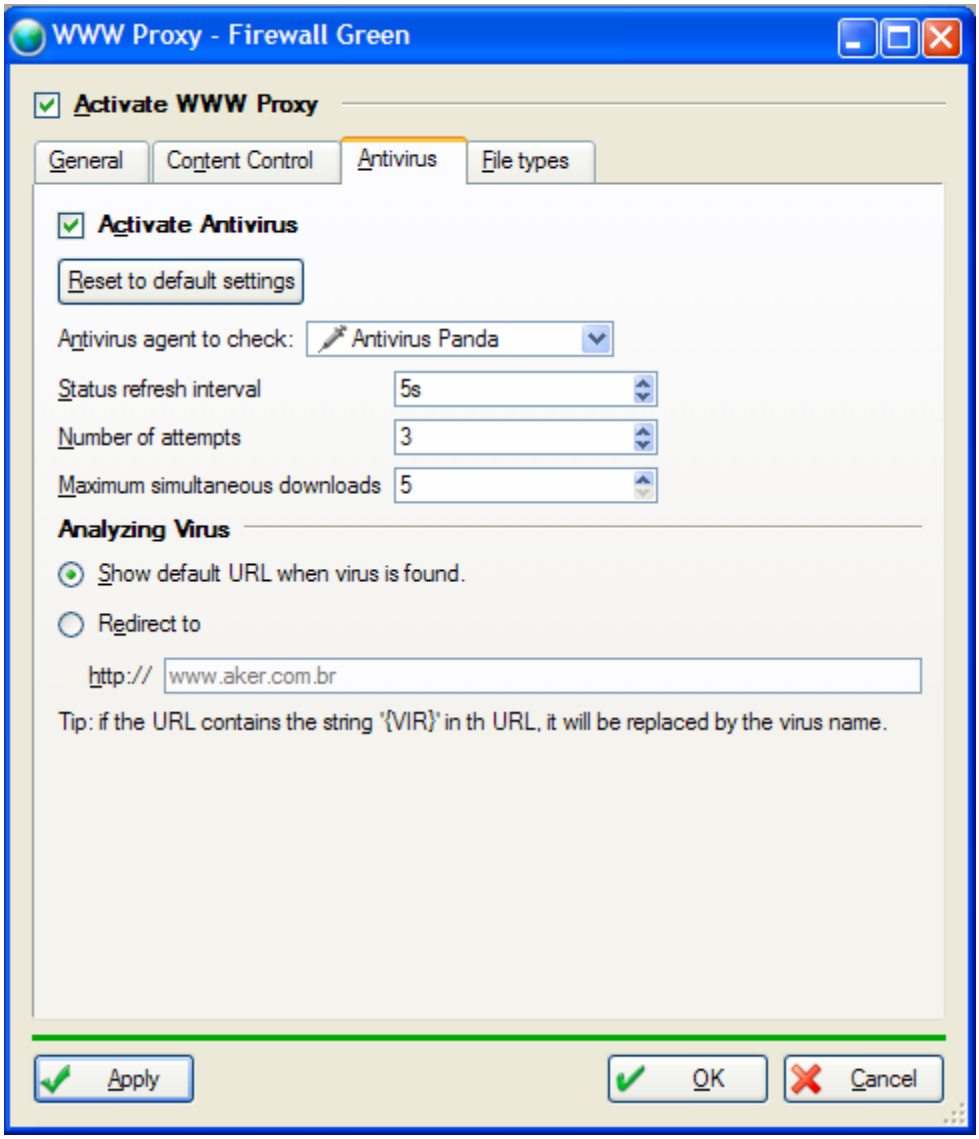
SSL Control: This parameter defines the secure connection ports (https) that will be accepted by the firewall. If a client tries to open a connection with a non-authorized port, the firewall will issue an error message and won't allow access.

In case only the default port (443) is to be used, the first option should be selected (**Allows HTTPS only to standard port (443)**). This is the configuration utilized by most firewalls.

The **Allows HTTPS to all ports** option indicates to the firewall that it must accept HTTPS connections to any port. This configuration is not recommended to environments that need reasonable security levels, since it is possible for a user to use the proxy to access non-authorized services by simulating an HTTPS connection.

The last option, **Allows HTTPS to entities below**, lets the administrator define exactly which ports will be accessible. In this case, entities corresponding to desired services must be registered. For more information, refer to chapter Registering Entities.

Antivirus tab



Activate Antivirus: When this box is checked, the firewall scans downloaded content for viruses.

The **Reset to default settings** button will restore the configuration of this tab to the original one.

Antivirus agent to check: Allows the selection of one antivirus agent previously registered in the firewall to be used for virus scanning. For more information, see the Registering Entities chapter.

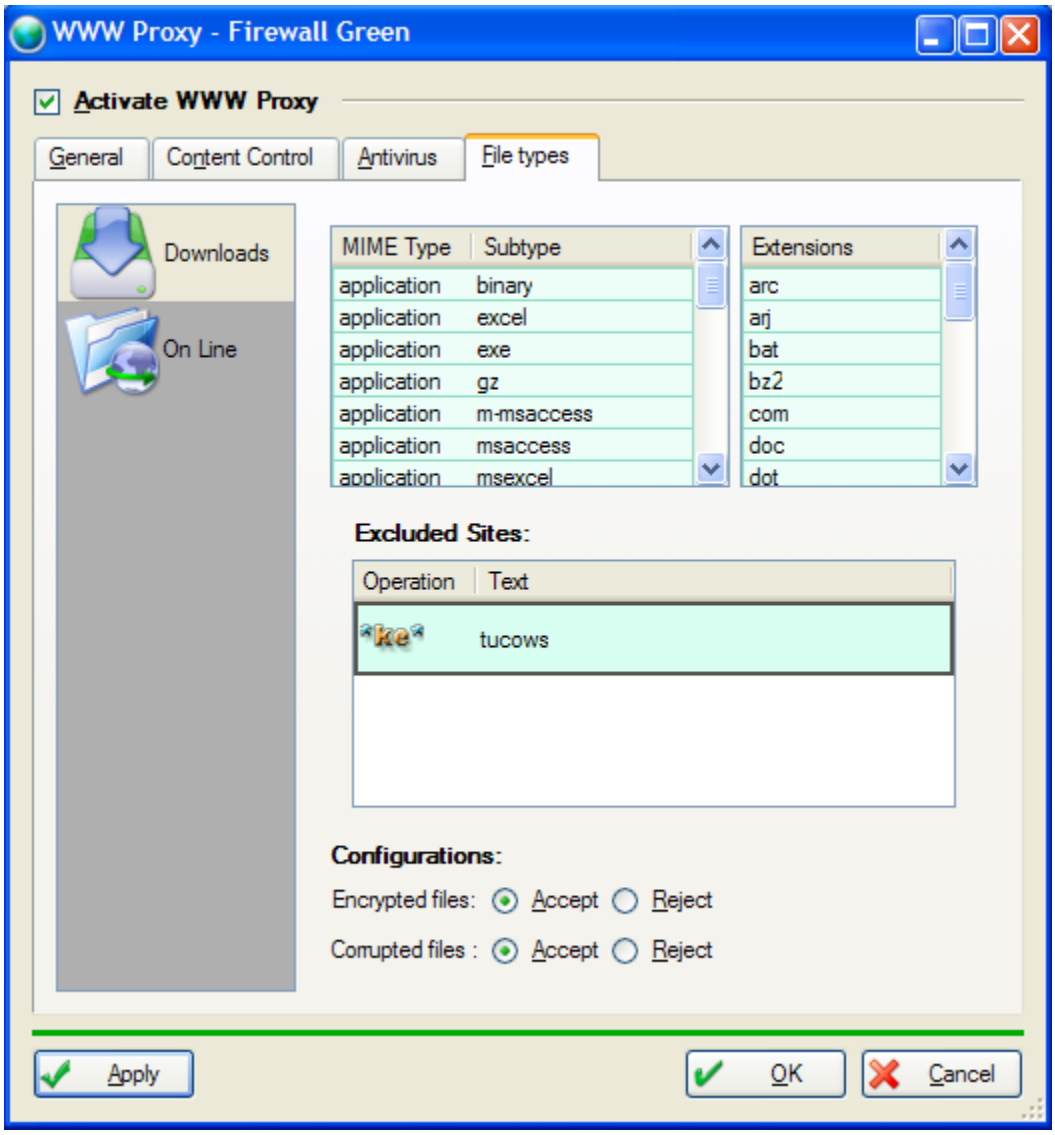
Status refresh interval: This option determines the time interval at which the downloaded page displayed by the firewall must be updated.

Number of attempts: Maximum number of download attempts for each file, if it is necessary to try more than once.

Maximum simultaneous downloads: Configures the maximum number of simultaneous downloads the firewall will allow.

Analyzing Virus: This field gives an option to show a URL other than the default one, if a virus is detected. The URL can be the firewall's or another one personalized by the user. It is also possible to personalize the message for each type of virus found, by using the {VIR} string that will be replaced by the name of the virus.

File types tab



- **Downloads** Option

This option is used to specify the files that will be scanned by Aker Firewall *Download manager*, that is, downloads that will be performed in background by the firewall and a web page with the status will be shown to the user. This option is interesting for

supposedly large files (compacted files, for instance) or for files that usually are not viewable by the browser.

It is possible to use two criteria to decide if a transferred file should be analyzed: the file **extension**, and its **MIME type**. If one of these criteria is met, i.e., if the file extension or the message MIME type is among those registered to be analyzed, then the file must be analyzed by the firewall.

The MIME type is used to indicate the type of data present in the response body, in HTTP protocol. It consists of two identifiers: the first one indicates the type, and the second, the subtype. The browser uses this information to decide how to display the information received in the same way the operating system uses filename extensions.

Excluded Sites:

In this field, the operation and text to be analyzed must be chosen. URLs that match one of the excluded ones will not analyzed.

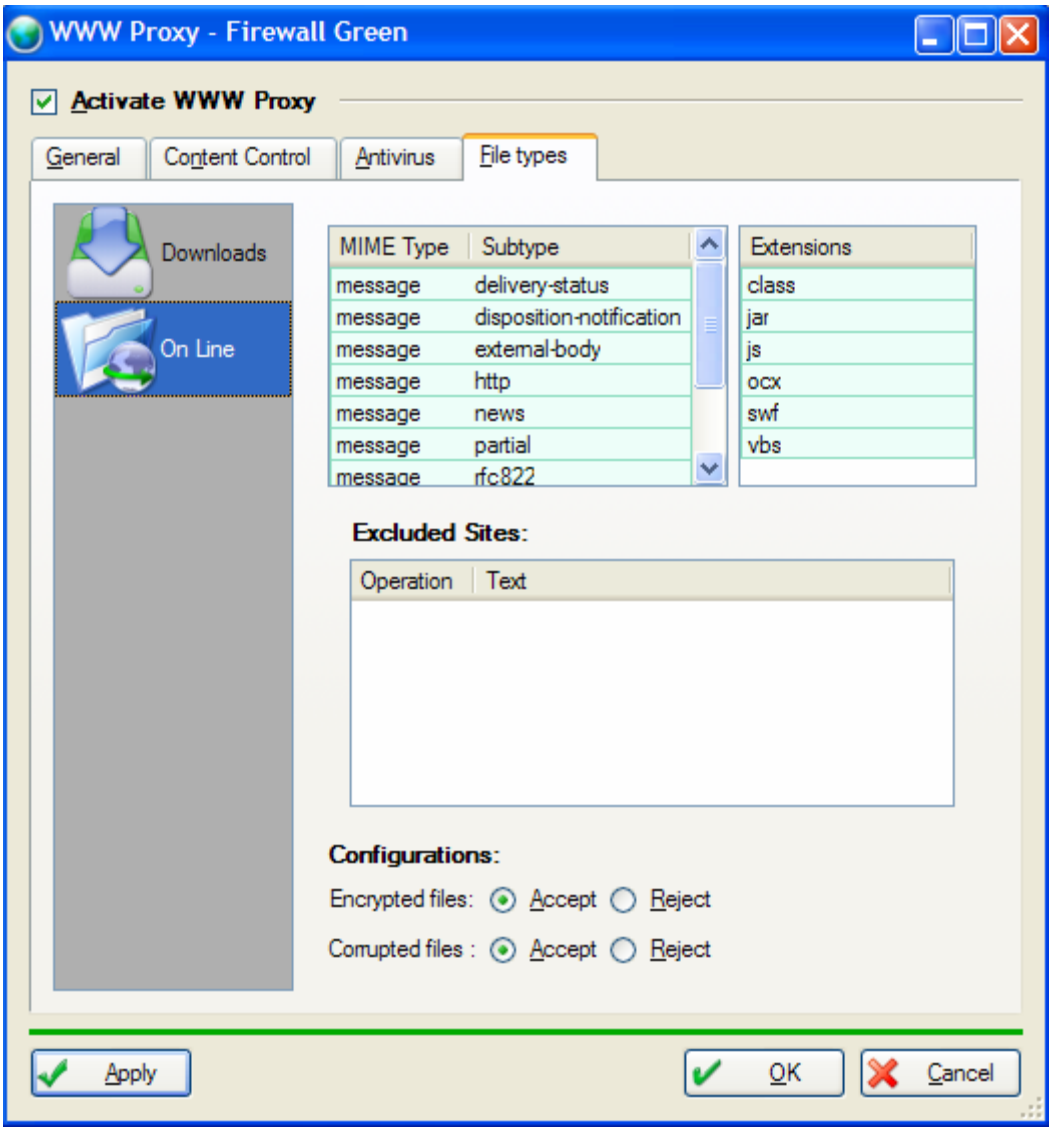
Configurations:

Encrypted Attachments: Choose between accepting or rejecting encrypted attachments.

Corrupted Attachments: Choose between accepting or rejecting corrupted attachments.

- **Online** Option

The same way as in **Downloads**, the firewall administrator must choose the MIME types and extensions. In the firewall default configuration, the following types are registered, as shown below:



Remaining items are similar to those in the **Downloads** option.

26-0 Configuring the SOCKS proxy

This chapter shows what is and how to configure the SOCKS proxy.

26-1 Planning the installation

What is the SOCKS proxy of Aker Firewall ?

The SOCKS proxy is a specialized program of Aker Firewall, designed to work with programs that support the SOCKS protocol, version 4 or 5.

The main function of SOCKS proxy is to provide a better security level for protocols to pass through the firewall, specially complex protocols which use more than one connection. It is possible, through the use of the SOCKS 5, to perform user authentication for any services that pass through the firewall, even without the authentication client.

It is a non transparent proxy (for further information, refer to the chapter Working with proxies), therefore, the clients that will use it must have proxy support and must be configured to use a proxy.

Using the SOCKS proxy

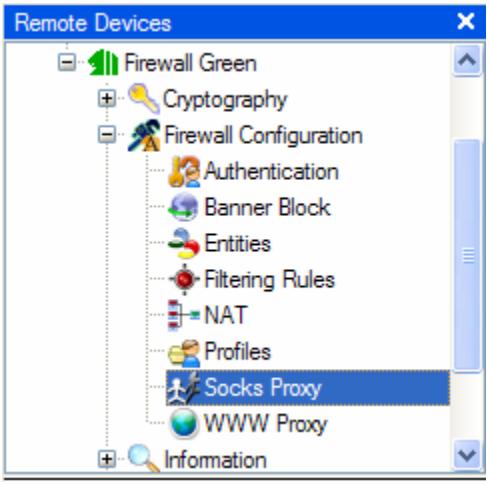
To use the SOCKS proxy of Aker Firewall, it is necessary to follow these steps:

1. Create the desired access profiles and associate them with the desired users and groups. This was explained in the chapter User access profiles)
2. Edit the configuration parameters of SOCKS proxy (this will be shown in the section Editing the parameters of the SOCKS proxy).
3. Create a filtering rule allowing the client hosts to access the proxy (for further information, refer to the chapter The stateful filter).

 The SOCKS proxy of Aker Firewall listens to connections on port 1080, using the TCP protocol. If necessary, this number can be changed to any port, by adding the parameter **-p *port***, where *port* is the number of the desired port, on the proxy startup. The proxy is started from the **/etc/firewall/rc.aker** file, and its initialization string may be changed from **/etc/firewall/fwsocksd** to **/etc/firewall/fwsocksd -p 8080**, for example.

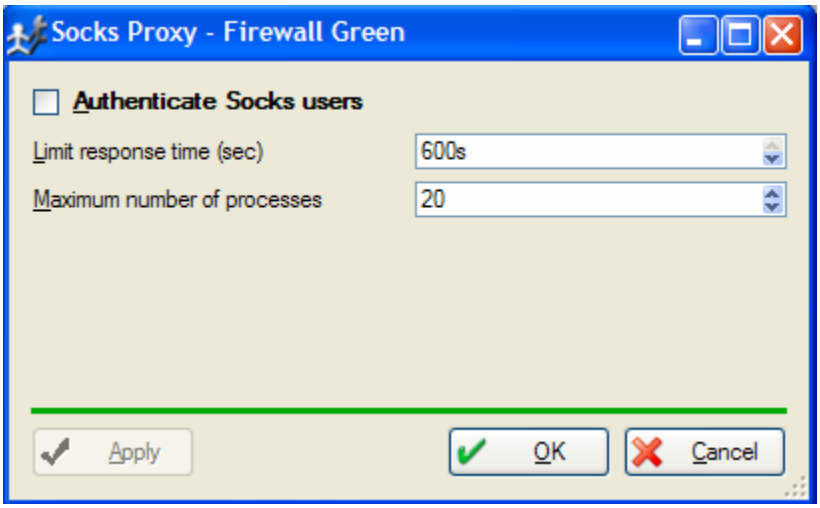
26-2 Editing the parameters of the SOCKS proxy

To use the SOCKS proxy, it is necessary to define some parameters that will determine the basic characteristics of its operation. This definition is made in the SOCKS proxy configuration window. In order to access it, follow these steps:



- Click on the menu *Firewall Configuration* on the firewall you want to manage
- Select the *Socks proxy* item

The SOCKS proxy parameters configuration window



- The **OK** button will close the SOCKS proxy configuration window and save all changes.
- The **Apply** button saves all modifications but keeps the window open
- The **Cancel** button will close the configuration window and discard all the changes done

The meaning of the parameters:

Authenticate SOCKS users: This field enables or not the user authentication of the SOCKS proxy. If it is checked, every time that a user tries to initiate a session, he will be asked for an identification and a password, and the session will only be started if the user is authenticated by any of the authenticators.

 If the user is using Aker Authentication Client and has an established session with the firewall, then no username and password will be asked, that is, the proxy will behave like no users authentication is being performed; however it is doing it. If the Aker Authentication Client session is closed, then the proxy will ask for an username and a password in the next access. For more information about Aker Authentication Client, refer to chapter Aker authentication client).

 The version 4 of the SOCKS protocol does not support user authentication, thus the only way to authenticate users using this protocol version is with the use of the authentication client. If this option is checked, the version supported by the client is 4 and there is no access profile session active, then the firewall will refuse all client's requests.

Limit response time: This parameter defines the maximum amount of time, in seconds, that the proxy waits for client data, from the moment that a new connection is established. If this time is reached without the necessary data from the client, the connection will be closed.

Maximum number of processes: This field defines the maximum number of processes of the SOCKS proxy can be active simultaneously. Since each process treats a single connection, this field also defines the maximum number of requests that can be treated simultaneously.

27-0 Using the GUI Tools

In this chapter, we will explain several Firewall Aker GUI tools.

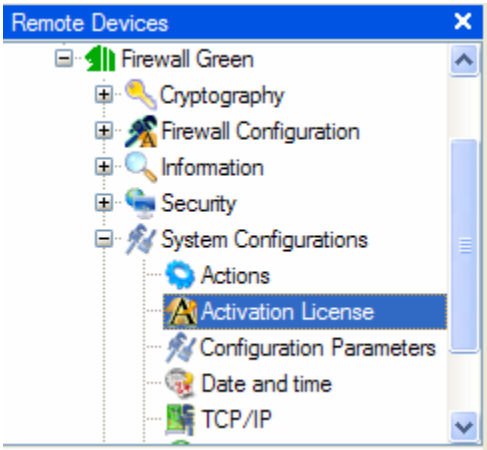
What are Firewall Aker GUI tools?

These are useful tools available only in the Firewall Aker Graphical User Interface. They facilitate firewall administration, supplying a series of very helpful functions for daily tasks.

27-1 Activation Keys

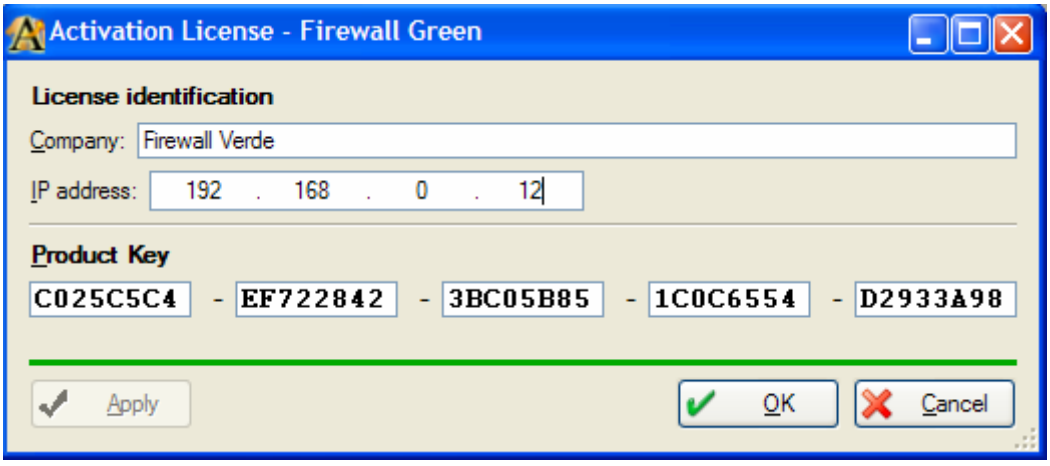
This options allows updating of Firewall activation key, and of additional licenses for encryption clients.

In order to update any of these keys through the GUI, do as follows:



- Click on the *System Configurations* menu in the firewall administration window
- Select *Activation License*

The activation license window



Initially, this window will show the activation and the additional licenses key, currently configured in the firewall. If the additional licenses key has not been typed in, then the field will be blank.

To modify any of these keys, just type in the new key value and click **OK**. Or click **Cancel** if you don't want to update the key.


The toolbar has a button to load the license from a file supplied by Aker.

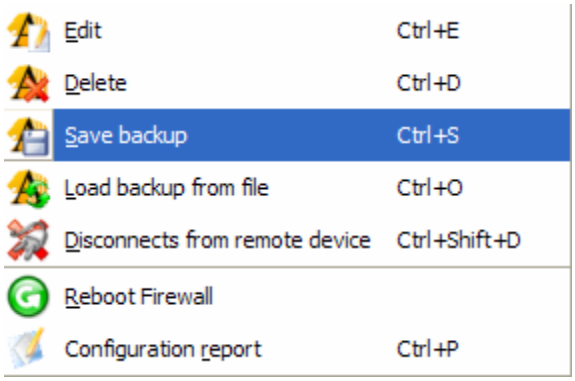
The company name, IP address, and the key(s) must be typed in exactly as directed by Aker Security Solutions, or its authorized representative. The company field is case sensitive.

If a recently updated key has different parameters from the previous key (for example, encryption enabling, or alteration in the number of licenses of encryption clients) it is necessary to finish the remote administration session, and reconnect to the firewall, so that the interface will detect the changes to these parameters.

27-2 Saving Configurations

This option allows saving the complete firewall configuration in the machine from where administration is being done. In case of an accident, this configuration can easily be restored at a later time.

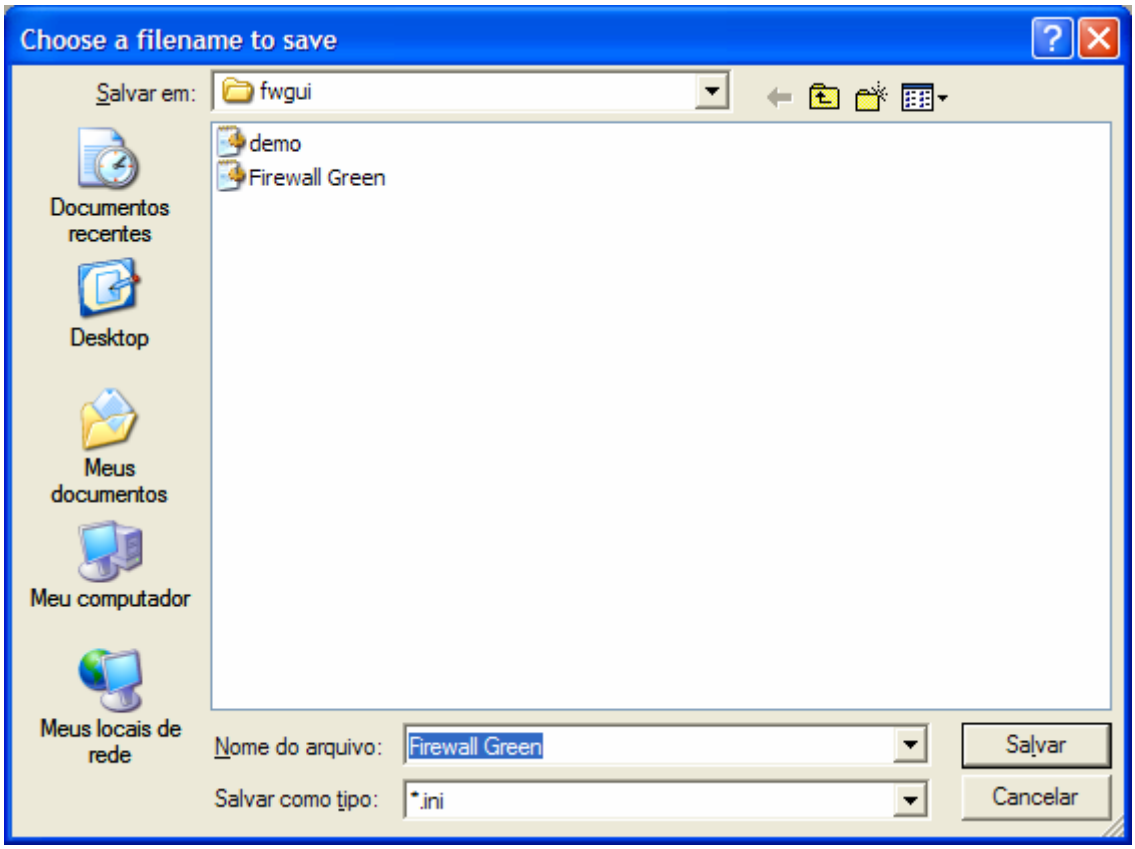
To make a backup copy:



- Click on the firewall to perform the backup copy
- Select *Save Backup* option on the toolbar or on the menu with the same name as the selected firewall

---

The save backup window

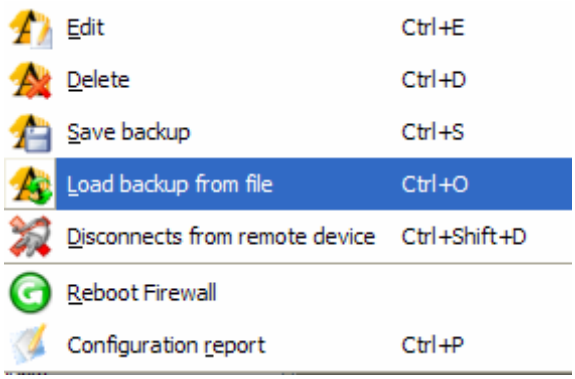


Type in the name and location of the file being saved and click on the **Save** button or press the **Cancel** button to cancel the save operation.

27-3 Restoring Configurations

This option allows restoration of the backup copy of the complete firewall configuration. Generation of backup copies were explained in the previous section.

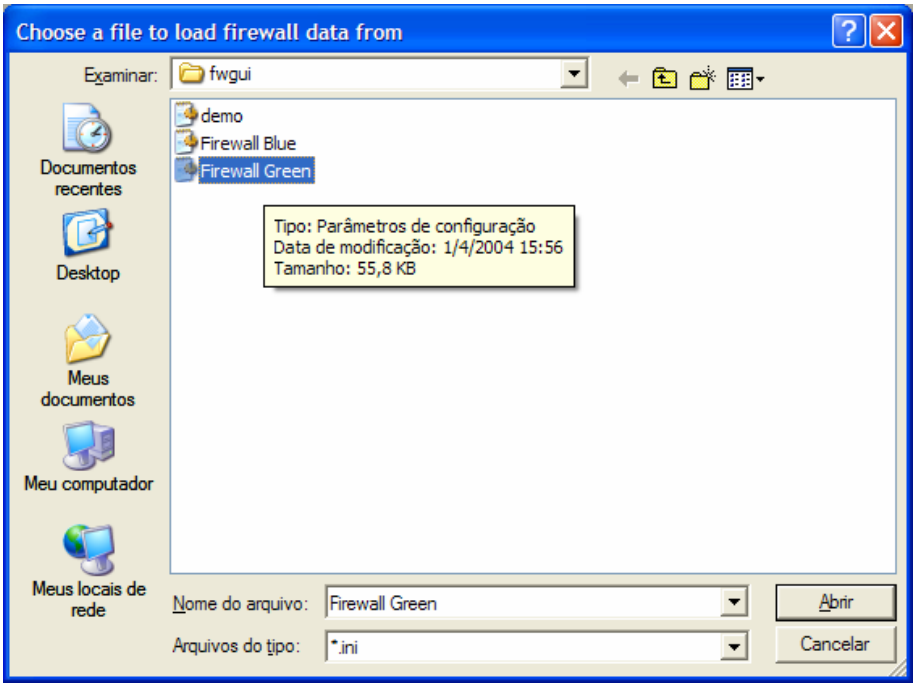
To restore a backup copy:



- Click on the firewall to load the backup copy
- Select *Load Backup from file* option on the toolbar or on the menu with the same name as the selected firewall

---

The load backup from file window:



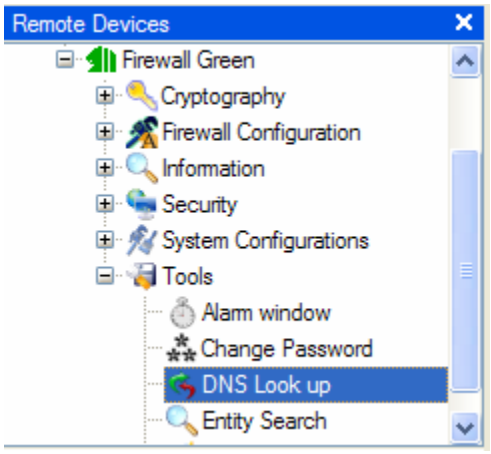
This window allows choosing the file name in which the configuration will be restored. After the file name is given, the firewall will read all its content, make several consistency tests, and if its content is valid, it will be loaded.

- The **Open** button will load the copy and immediately update the firewall configuration.
- The **Cancel** button closes the window but does not load the backup copy.

27-4 Reverse DNS

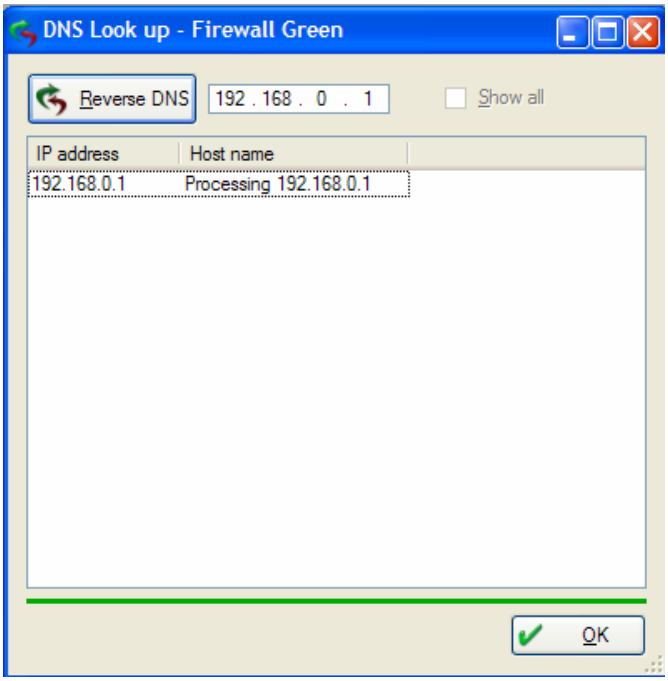
Reverse DNS is used to resolve hosts names from IP addresses. The Firewall Aker Reverse DNS Resolution Window provides address resolution without the need of additional programs.

To access the reverse DNS resolution window:



- Click on the *Tools* menu in the firewall administration window
- Select *DNS Look up*

The DNS look up window



This window has a field for the IP address to resolve and a list with the IP addresses previously resolved.

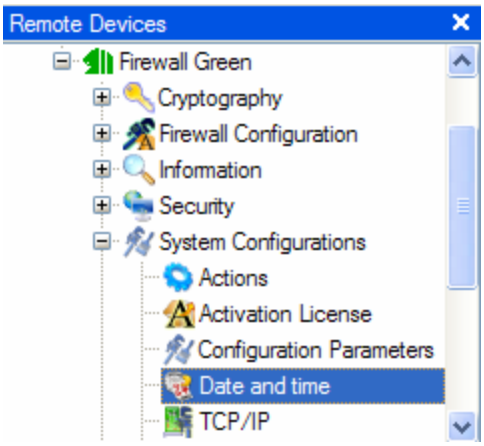
- The **OK** button will close the window.
- The **Show all** option, if checked, will show all previously resolved addresses in the window below.

To resolve an address, type it in the field and press the **Reverse DNS** button. The address will be displayed on the list, in the bottom part of the window, along with the resolution status. Soon after, either the host name corresponding to the address will be shown, or an indication that the given address does not have configured Reverse DNS.

27-5 Date and Time

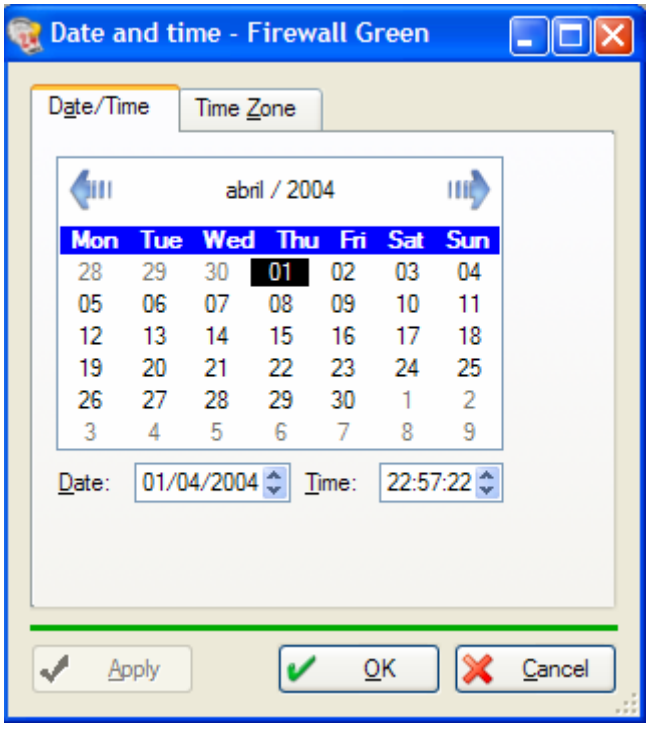
This option lets the administrator verify and modify firewall date and time. Correctly configured date and time are essential to the proper schedule operation of rules, WWW access profiles, key exchange using SKIP protocol, and log and events systems.

To access the Date and Time Configuration Window:



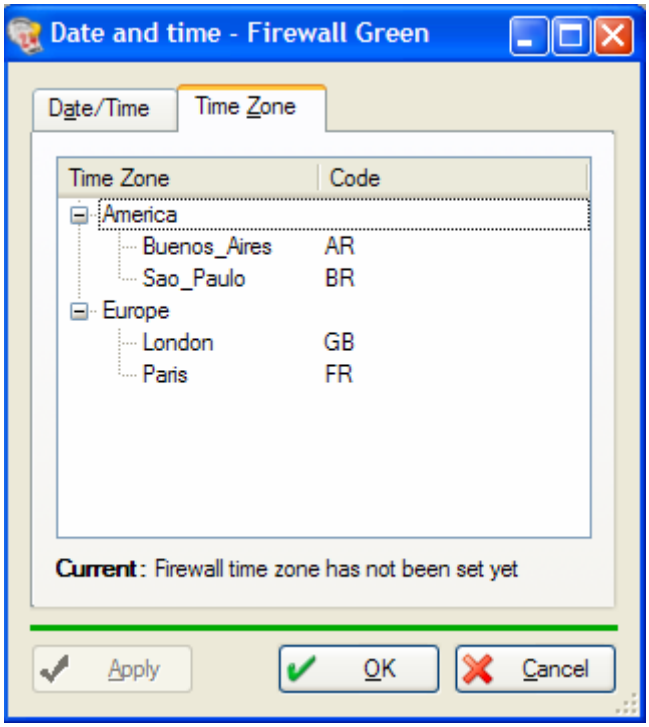
- Click on the *System Configurations* menu in the firewall administration window
- Select *Date and Time*

The date and time window



This window has two fields that show the date and time values configured in the firewall. To alter any of them, just input the desired value in the corresponding field. To choose a month, it is possible to use the navigation arrows.

The time zone Tab



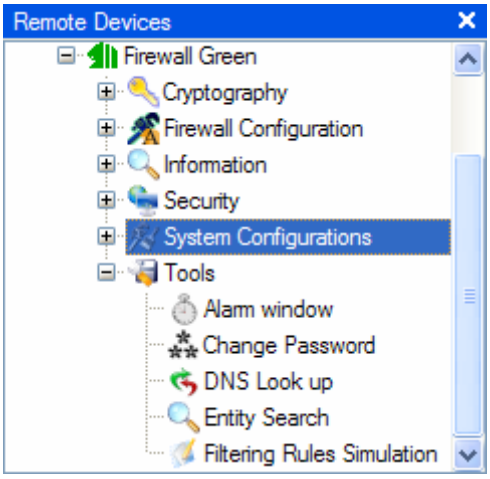
Choose the time zone of the nearest region to where the firewall will be installed.

- The **Apply** button modifies data and time and keeps the window open.
- The **OK** button saves the modifications and closes the window.
- **Cancel** closes the window and discards any modification.

27-6 Filtering Rules Simulation

Rule scanning allows the administrator to test firewall filtering rules configuration through a simulation of connection attempts. The analysis of the simulation result can tell if the firewall is really blocking the connections that should not be accepted, and letting through the ones that should.

To access the simultation window:



- Click on the *Tools* menu in the firewall administration window
- Select *Filtering Rules Simulation*

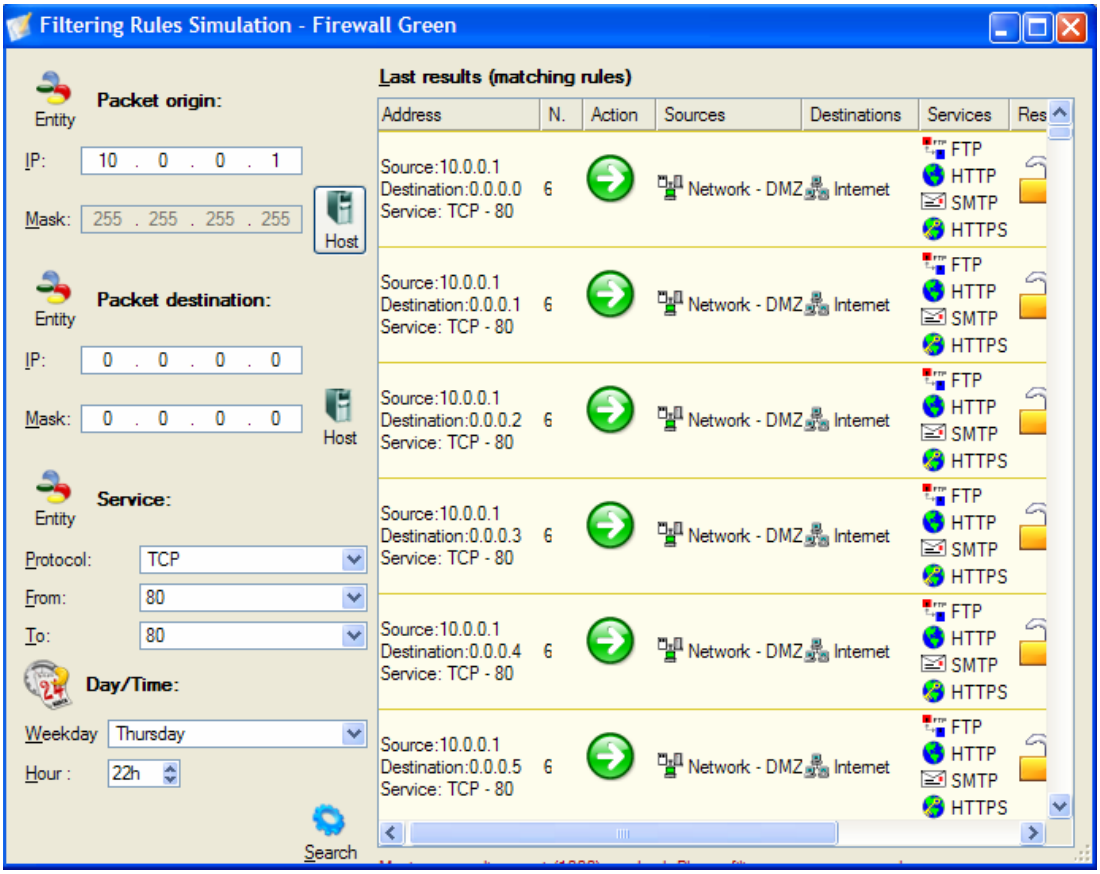
The filtering rules simulation window

It is possible to alternate between scanning by IP and by entities. The scan by entities is useful when all hosts, networks, and services to be used are already registered in the system. The scan by IP is the most indicated when these hosts, networks, or services are not registered and it is not desirable to register them (for example, external hosts that won't be used in any filtering rule).

It is possible to choose for source, destination and services, independently, if entities are to be used or not. To switch between the two modes, it is enough to click on the icons at the left of each field.

- **Scan by IP**

When the **Scan by IP** option is selected, the scanning window will have the following format:



The **Packet Origin IP** and **Mask** fields specify the range of hosts to be used as the sources for the simulated connections. The **Packet Destination IP** and **Mask** specify the range of hosts to be used as destinations.

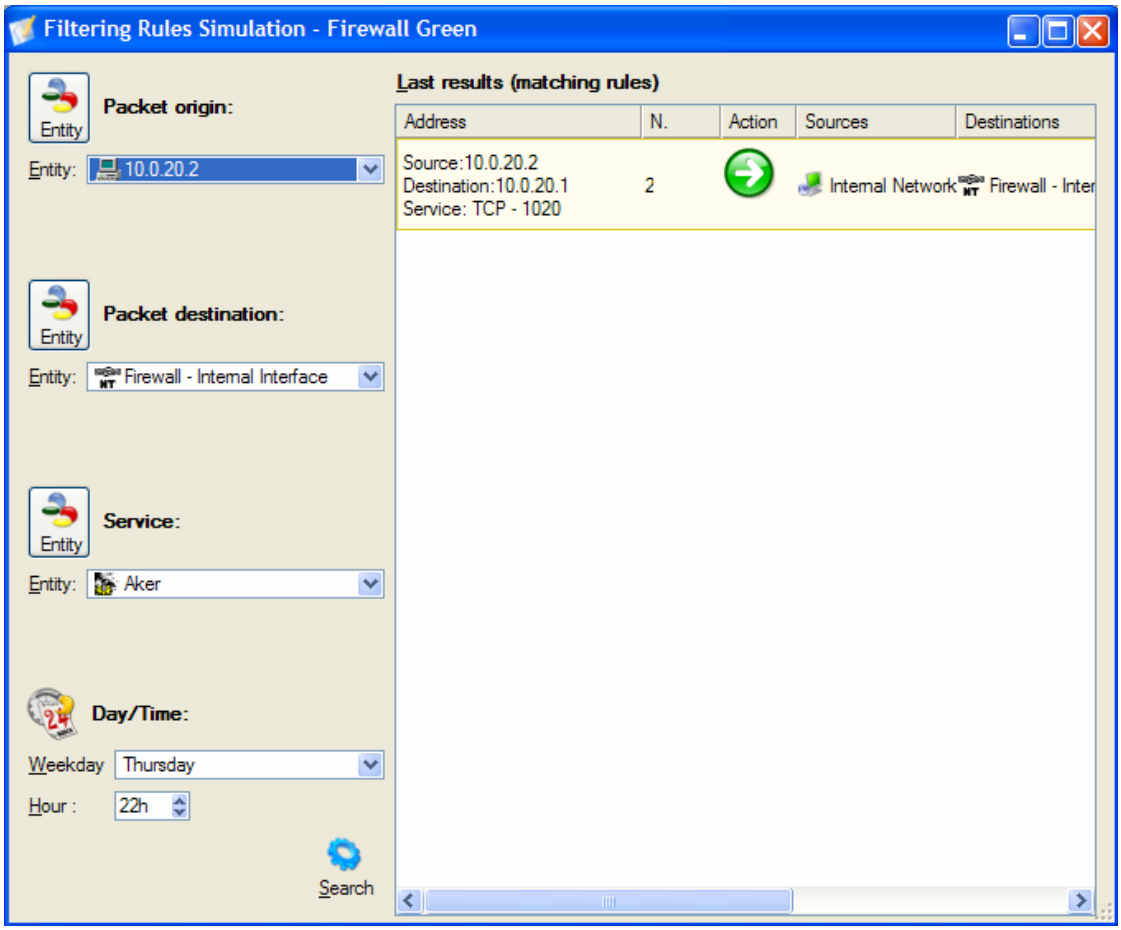
The **Service** field is used to specify the protocol and range of the ports to be tested.

For TCP and UDP protocols, the service value is the destination port. For ICMP, it's the type of service, and for other protocols, it's the value of the protocol.

The **Day/Time** field allows the administrator to test the rules in a specific weekday and time.

- **Scan by Entities**

When the **Scan by Entities** option is selected, the scanning window will look like this:



The field **Packet Origin** specifies the source entity that will be used in the simulated connections. The field **Packet Destination** specifies the entity to which the simulated connections must connect.

The **Service** field is used to specify the protocol and range of the ports to be tested, through an entity.

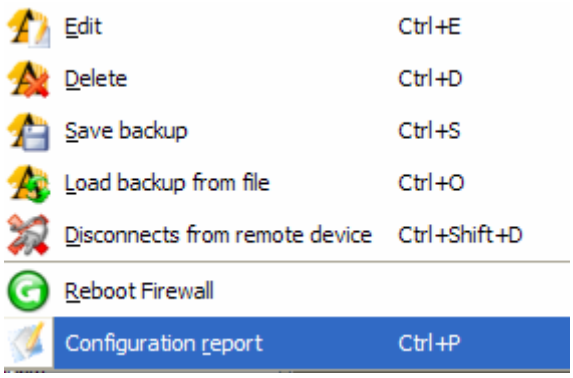
The **Day/Time** field allows the administrator to test the rules in a specific weekday and time.

It is only possible to select one entity as origin, one as destination, and one service.

27-7 Reports

This option gives the administrator the possibility to easily and quickly print a report of all Firewall configuration (or part of it). This report is very useful for documentation purposes and for configuration analysis.

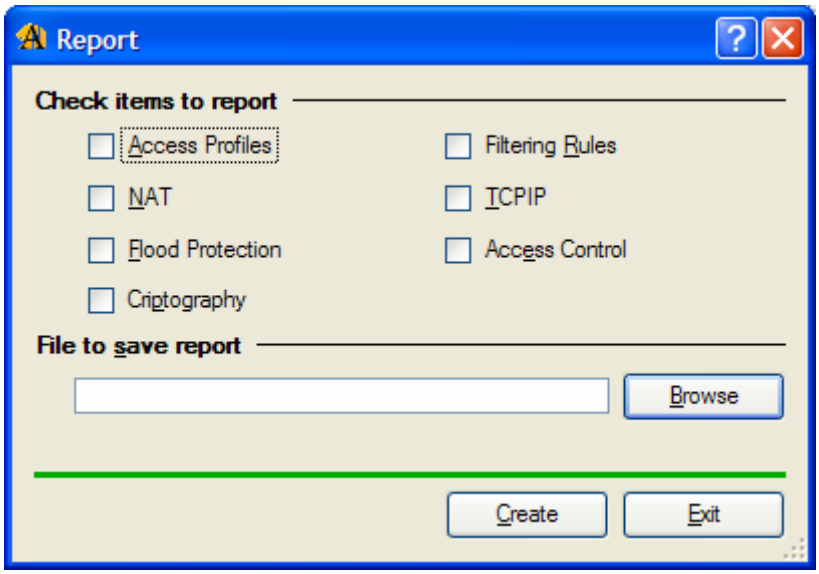
To access the Reports Window:



- Click on the firewall to generate the report
- Select *Configuration Report* in the menu with the same name as the selected firewall

---

The reports window



This window has several different options, one for each firewall configuration aspect, that may be independently selected. To generate a report, do as follows:

1. Check the items to be printed;

2. Click on the **Browse** button and choose the directory where the html pages will be stored;
3. Open the directory and select the html file to print your report.

To cancel the report, click on **Cancel**.

27-8 Patches and Updates

What are updates and how to obtain them ?

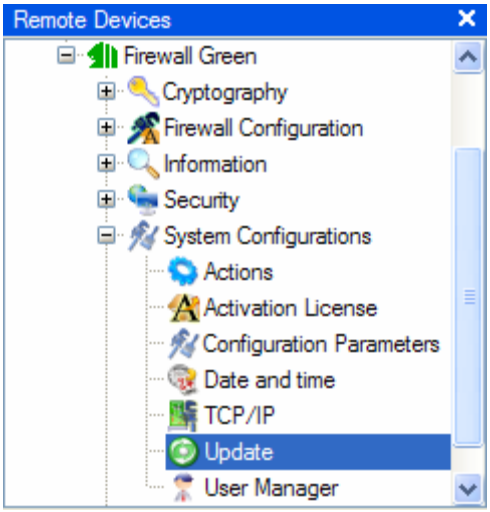
As all other software, Aker Firewall can eventually present bugs. As soon as these bugs are corrected, Aker produces a file that allows the updating of your firewall and the elimination of them. Sometimes new features are added in a existing version, in order to improve performance or enhance fexibility.

In both cases, the update files are made available for free in Aker website: find the *Download* menu and select *Patches and Upgrades*. These files are always cumulative, that is, it is necessary to download only the last available version and it will include all corrections present on all previous files.

The updates window

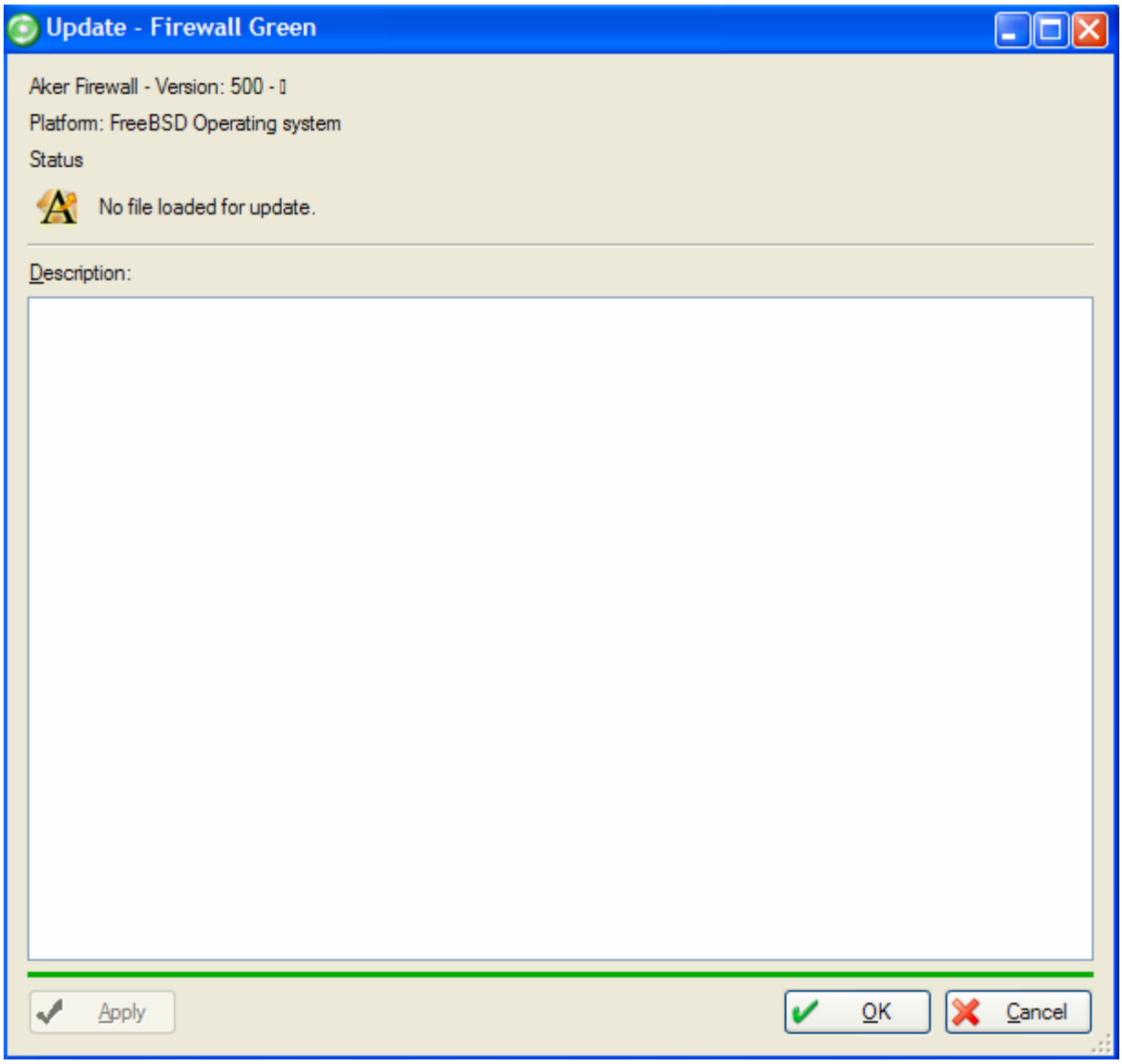
This option allows that an update or patch for Firewall to be applied remotely, through the GUI. It is even possible to completely update a firewall version using this option.

To access the update window:



- Click on the *System Configurations* menu in the firewall administration window
- Select *Update*

The update window



Initially, the update window will only show the firewall version, its correction level, and the platform (operating system and version) in which the firewall is running.

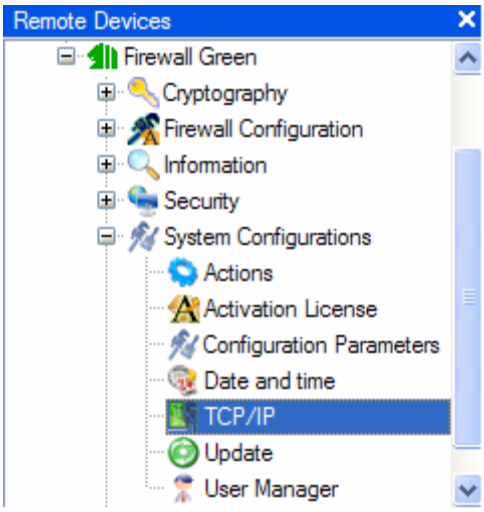
To apply an update or patch, just click on the **Load update file** button (the icon with Aker log). The patch or update description, the target firewall and the operating system versions will be displayed. Click on the **Apply** button to apply the update or patch.

If the update or patch is for a different firewall or operating system version, then the **Apply** button will be disabled, impeding its application.

27-9 TCP/IP Configuration

This options allows configuration of all firewall TCP/IP parameters through the GUI. It is possible to configure network interfaces addresses, DNS, and routing.

To access the TCP/IP Configuration Window, do as follows:

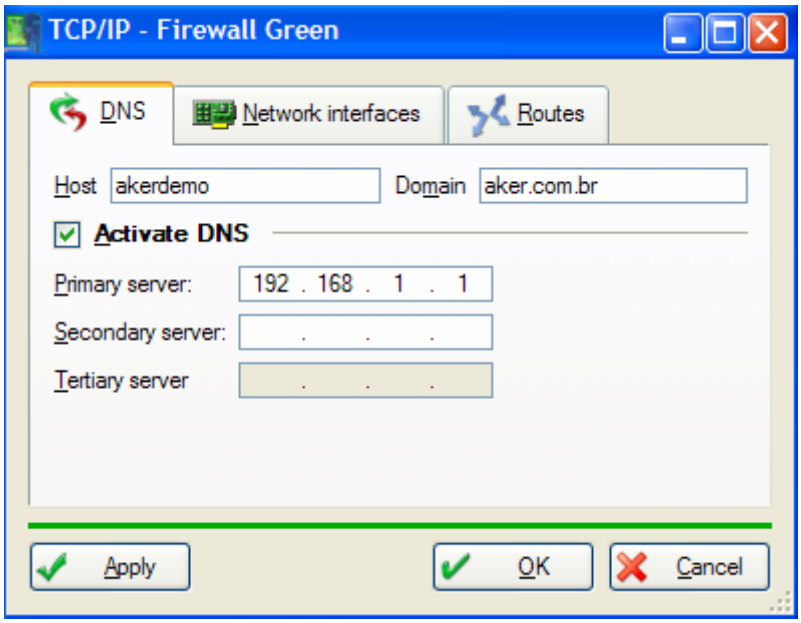


- Click on the *System Configurations* menu of the firewall administration window
- Select *TCP/IP*

The TCP/IP configuration window

This window consists of three tabs. Each one is associated to a different type of configuration. They are:

DNS



All options related to name or DNS resolution are configured in the DNS tab. It has the following fields:

Host: Name of the host in which the firewall is running.

Domain: Name of domain in which the firewall is running.

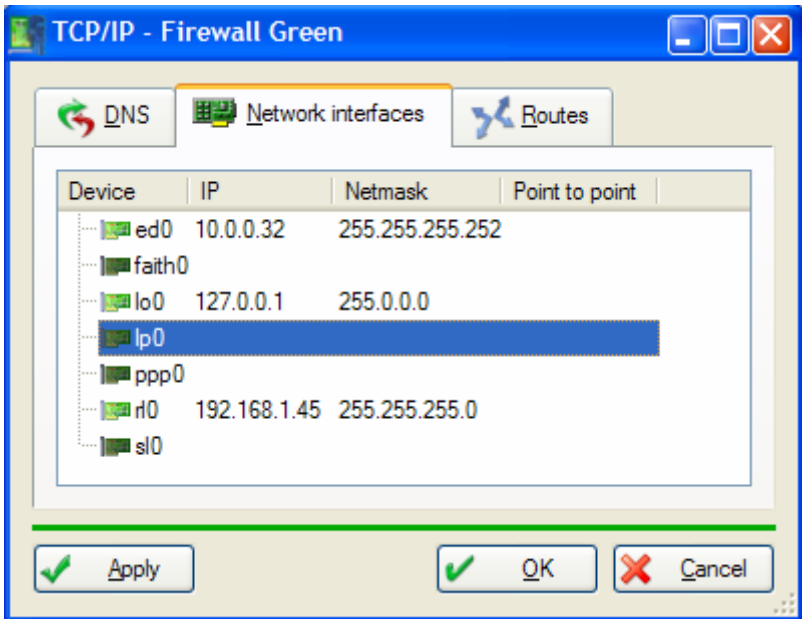
Activate DNS: This option must be checked to activate name resolution via DNS, and unchecked to deactivate it.

Primary server: This field defines the primary DNS server. It is mandatory if the *Activate DNS* option is checked.

Secondary server: This field defines the secondary DNS server, that will be consulted if the primary fails. It is optional.

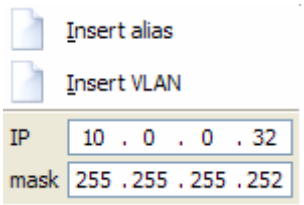
Tertiary server: This field defines the tertiary DNS server, that will be consulted if the primary and secondary fail. It is optional.

Network Interfaces



In this tab, it is possible to configure the IP addresses of all network interfaces recognized by the firewall. It has a list with all network interfaces, IP addresses, and masks (it is possible to configure up to 31 different addresses for each interface). If an interface does not have a configured IP address, its address and mask fields will be blank.

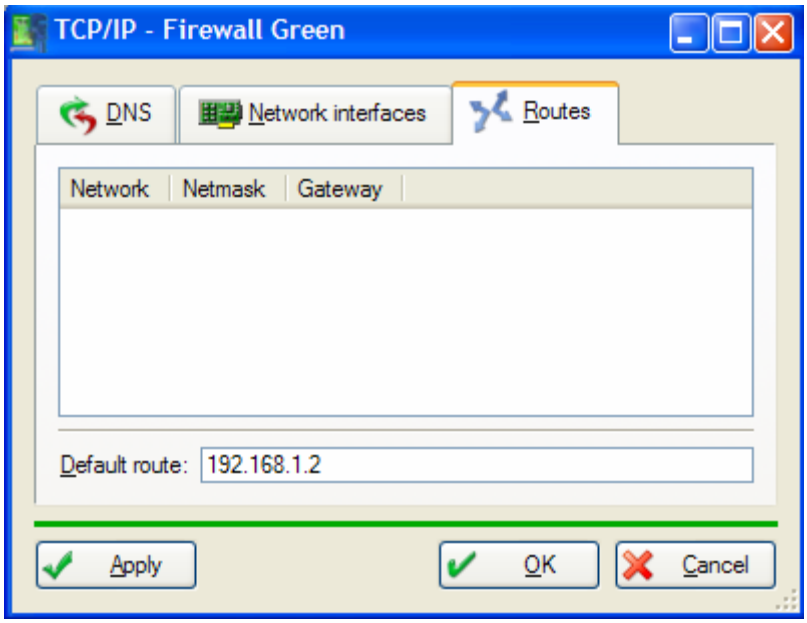
To configure or modify an interface IP address or mask, right-click on it, and use the menu that will show up.



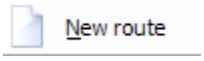
In the same menu, it is possible to give the interface an alias, and to create a VLAN associated to that interface.

It is only possible to configure IP addresses of network interfaces that are recognized by the operating system in which the firewall is running. If a new network address is added, and its name does not show on the interfaces list, it is necessary to configure the operating system to recognize it, before trying to configure it through this tab.

Routes



This tab enables IP routing configuration in the firewall. It has a field called **Default Route** where the default router is specified, and a list of several routes configured in the firewall.

To add a new route, right click anywhere inside the list area, and the 

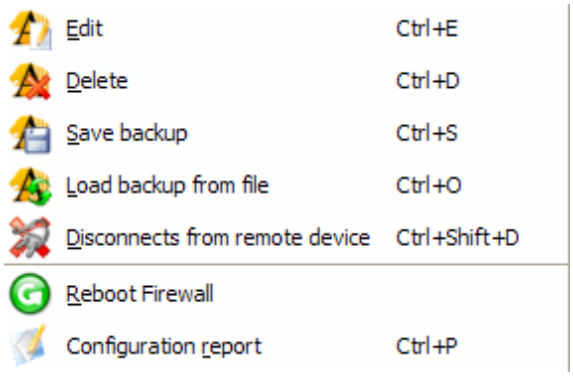
menu shows up.

To delete or edit a route, right click on it.

27-10 Rebooting the Firewall

This option is used to reboot the firewall, although it should not be used under regular operating conditions. The only operation that requires reinitialization of the firewall is the loading of an external encryption algorithm.

To reboot the firewall, do the following:

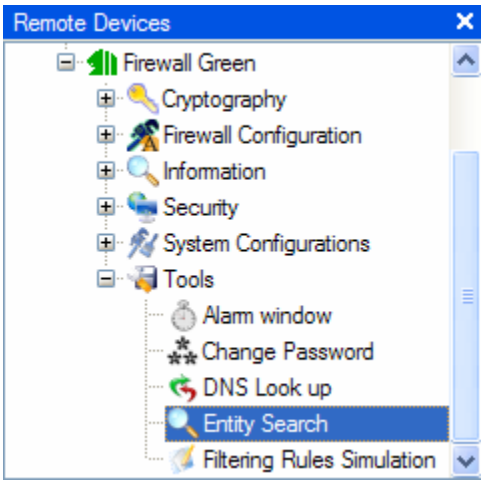


- Select the firewall to be rebooted
- Select *Reboot Firewall* option on the menu with the same name as the selected firewall

27-11 Entity Search

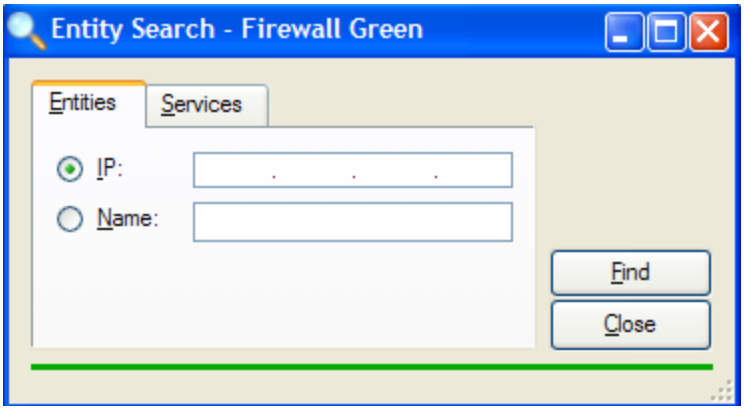
This option is used to locate entities that have a specific IP address, interface or service, as well as rules that contain a specific entity.

To access the Entity Search Window:



- Click on the *Tools* menu in the firewall administration window
- Select *Entity Search*

The Entity Search Window



This window has two tabs. Each for a different type of search.

- The **Entities** tab searches for entities by name or IP address.
- The **Services** tab searches for entities of the *service* type that contain the specified protocol or service.

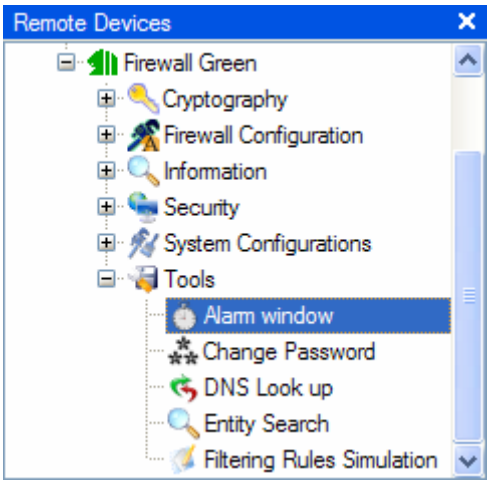
Regardless of the search used, tab operation is identical:

- The **Find** button starts the search using the data specified.
- The **Close** button closes the Entity Search window.
- By double-clicking on an entity or rule displayed as a search result, the corresponding editing window will be openned, allowing quick edition of its values.

27-12 Alarm Window

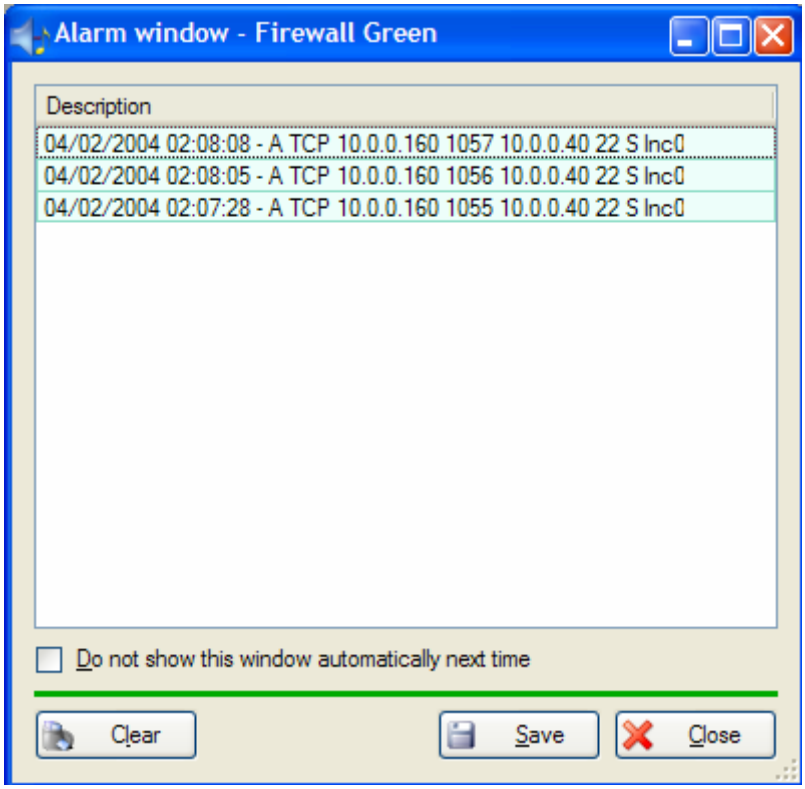
This option allows the viewing of all alarms generated by filtering rules or by the firewall actions.

To access the alarm window, do as follows:



- Click on the *Tools* menu in the firewall administration window
- Select *Alarm Window*

The alarm window



This window has a description field containing records of actions executed by the filtering rule.

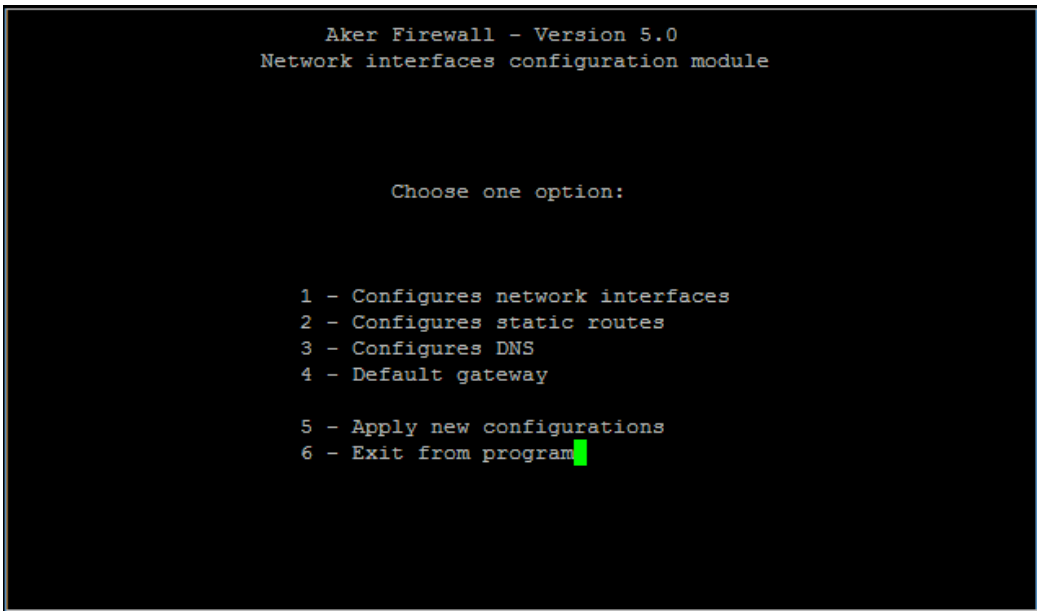
- The **Close** button closes the window.
- If the **Do not show this window automatically next time** option is checked, this window will not be automatically displayed when an event occurs.
- The **Save** button records the entries in a log text file.
- The **Clear** button clears the window of all entries.

27-13 Using the Command Line Interface for TCP/IP Configuration

It is possible to configure TCP/IP parameters through the command line interface.

Program location: `/etc/firewall/fwinterface`

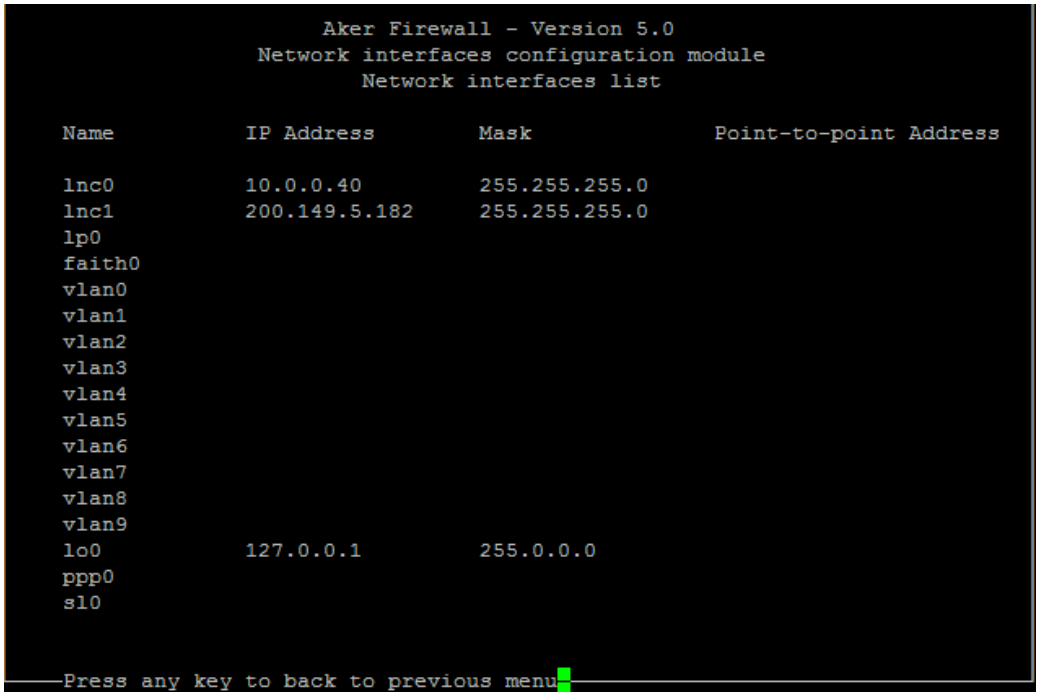
The program is interactive and the configuration options are described below:



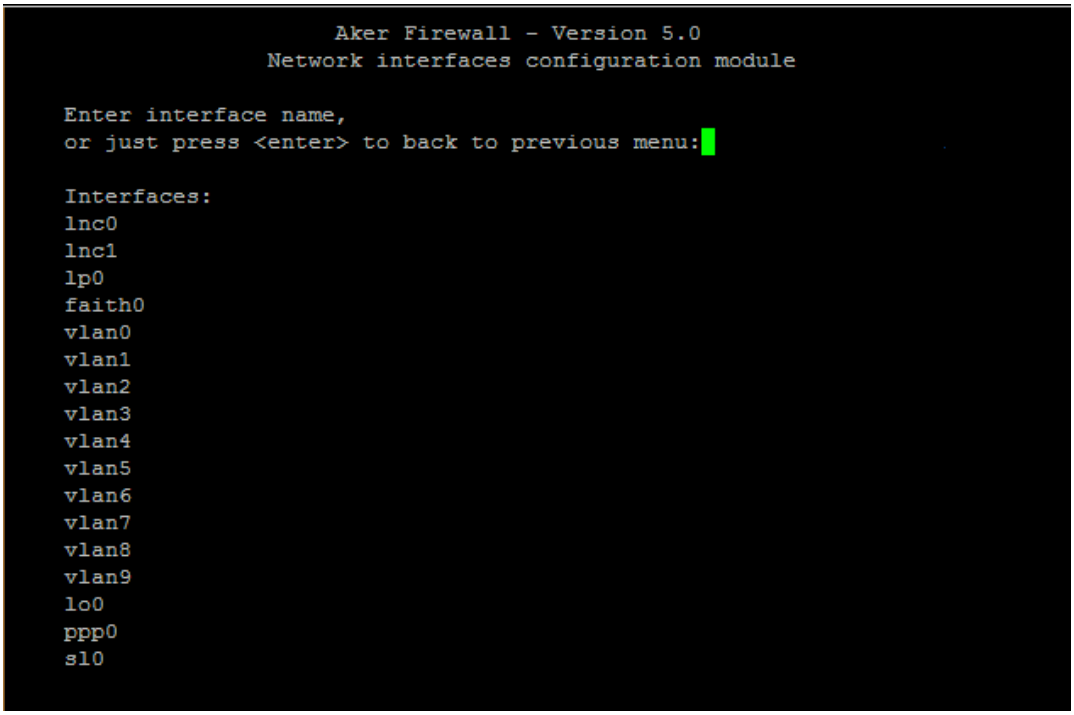
Similarly to the GUI, the command line interface has 6 options, as seen above.

In the window below, it is possible to view, configure and change configuration of a network interface.

The screen below shows the List of network interfaces.

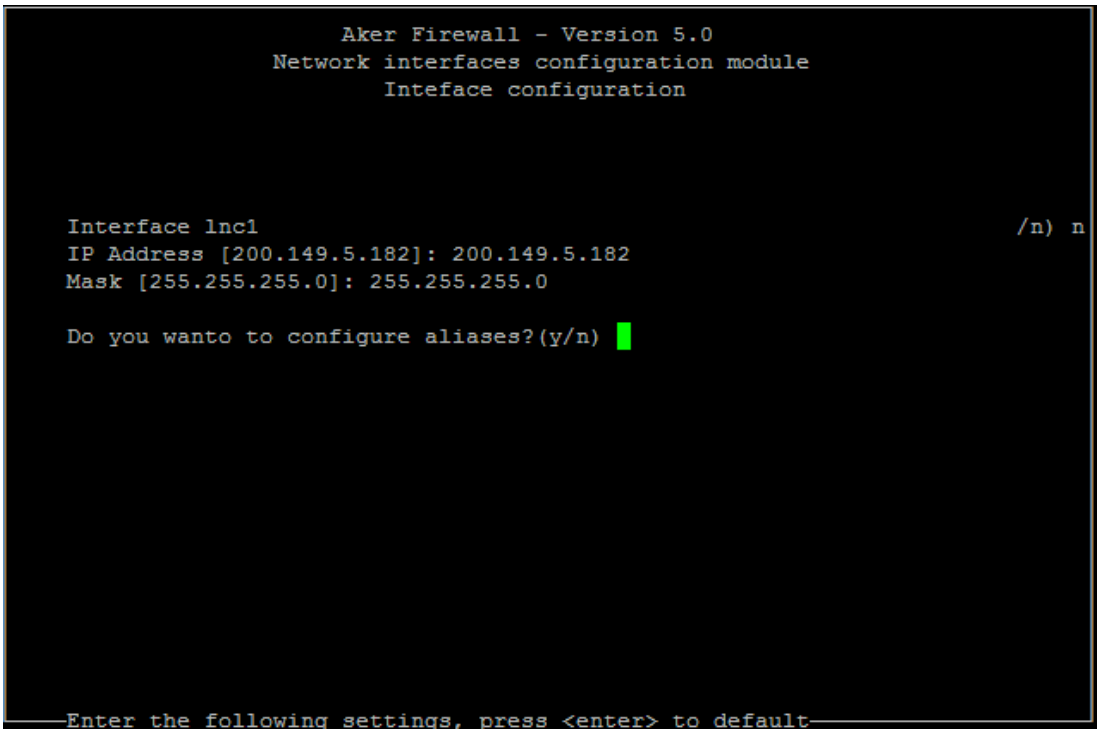


To configure an interface, just type its name. The <enter> key returns to the previous menu.

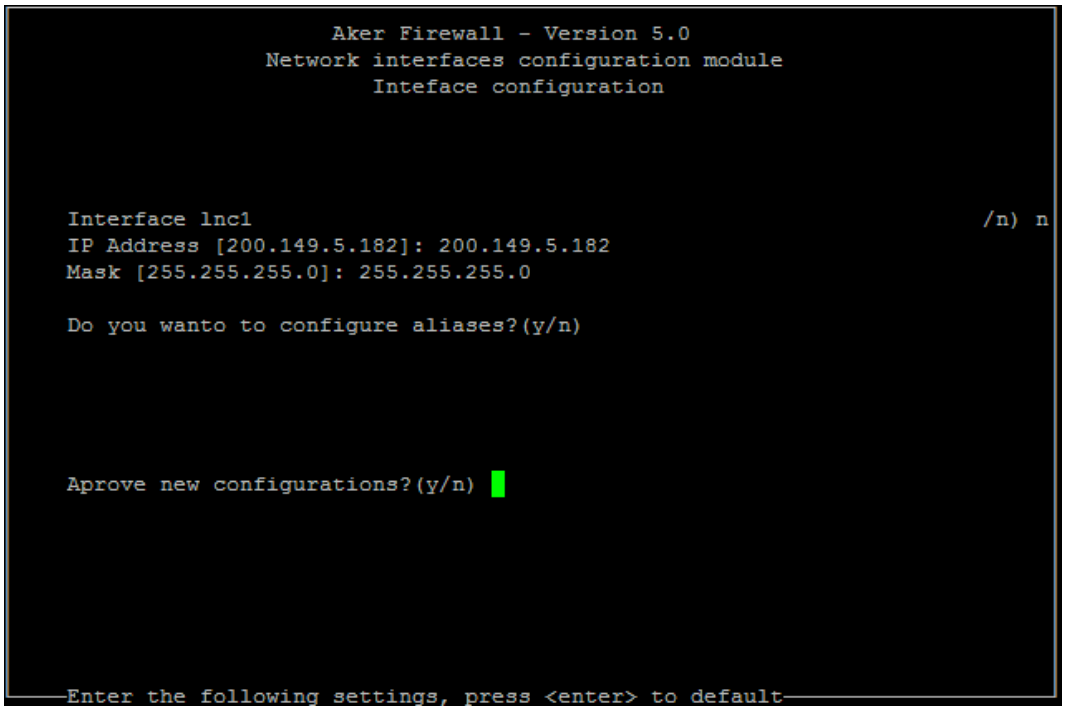


This screen shows the VLAN Registration option.

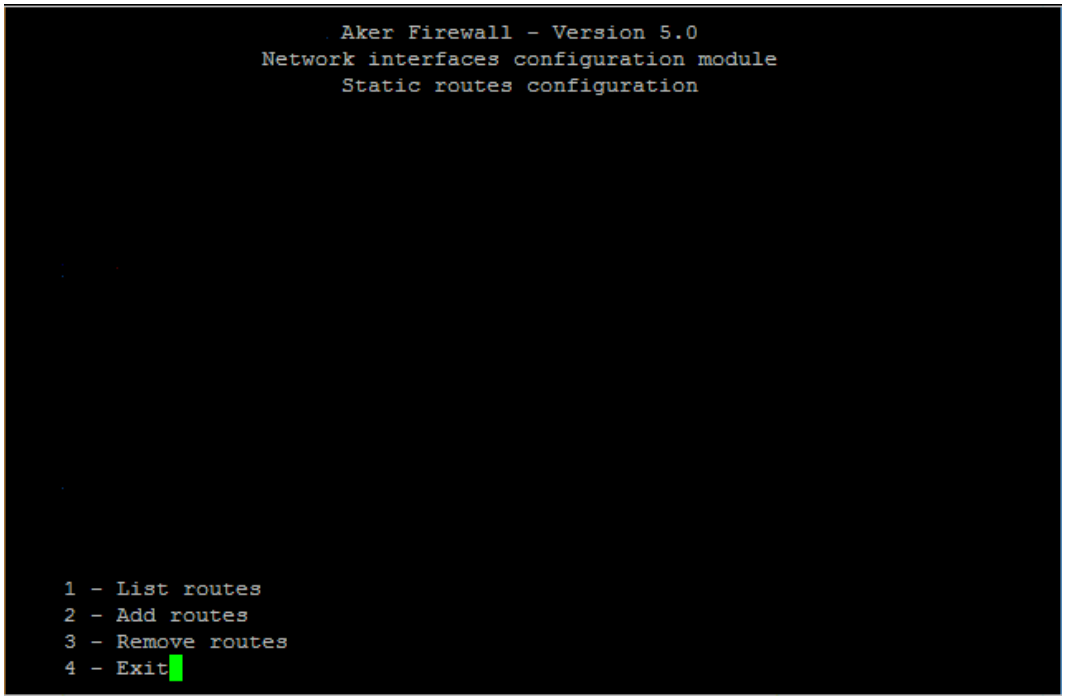
After configuration values are entered, it is possible to configure an alias for the interface.



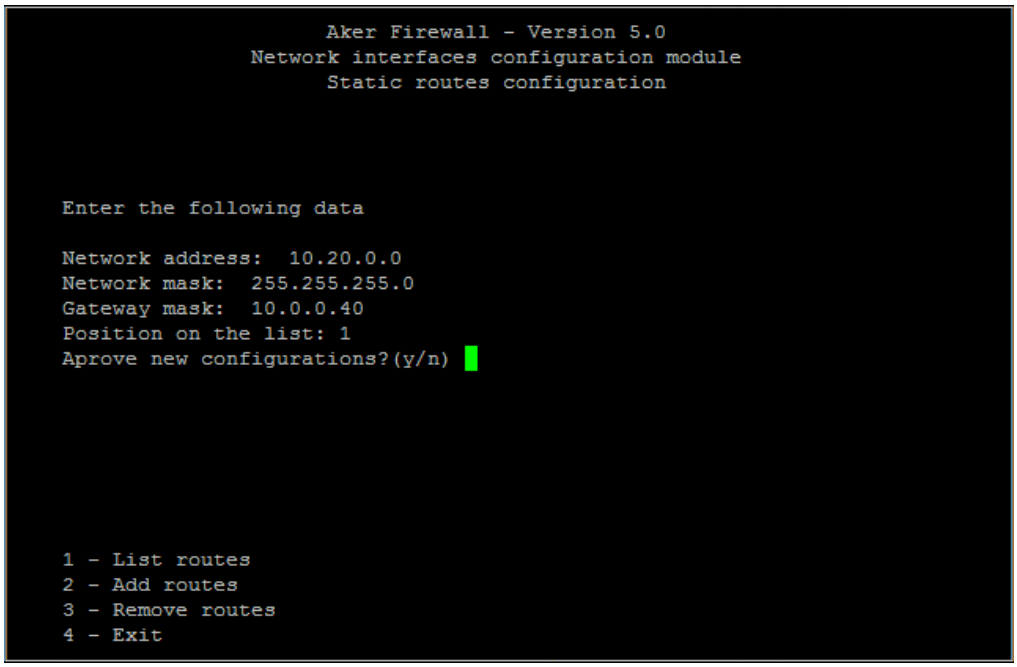
After data input, the program prompts for configuring an interface for the new values.



By choosing Option 2 in the main screen, it is possible to configure static routes.



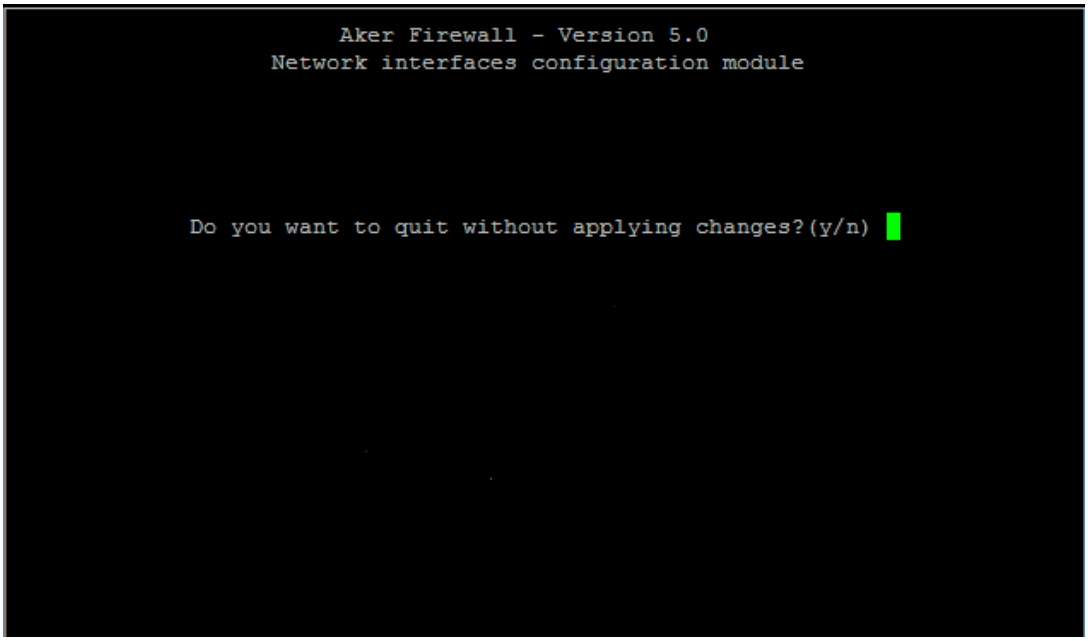
After information has been entered, the program prompts for confirmation of the new configuration parameters.



By choosing Option 3 in the main screen, it is possible to configure DNS Servers.

By choosing Option 4 in the main screen, it is possible to configure the default route.

Option 5 of the main screen saves the new configurations. If the user chooses Option 6, the firewall detects all modifications and asks if the user wants to exit without applying them.



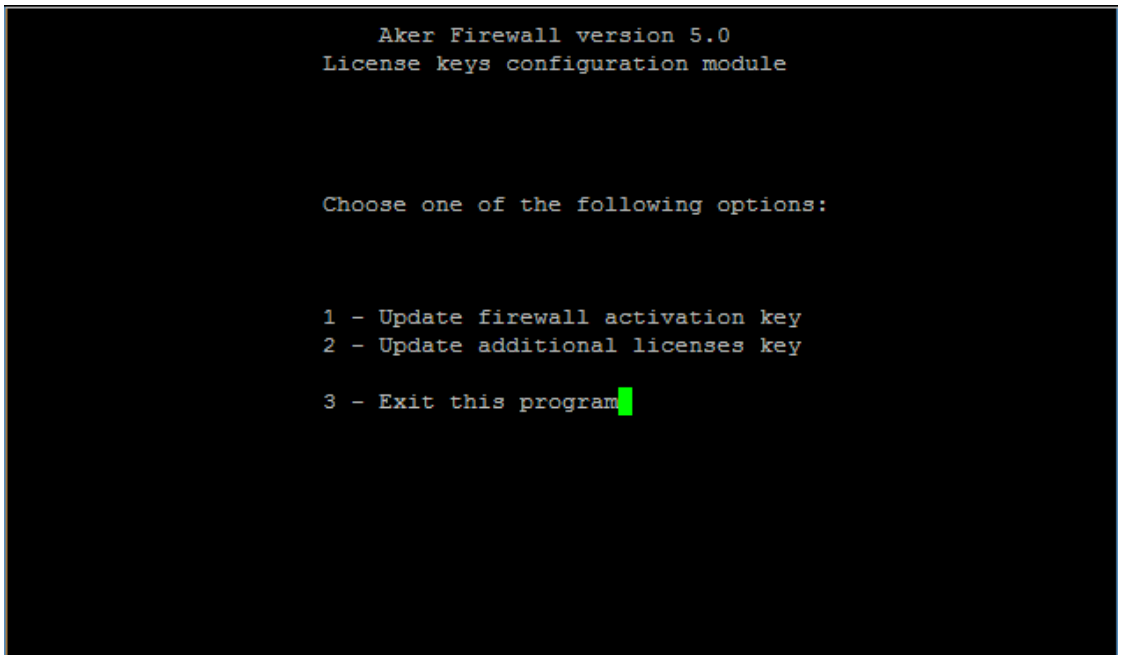
27-14 Using the Command Line Interface for Activation Keys

It is possible to configure Activation Keys through the command line interface.

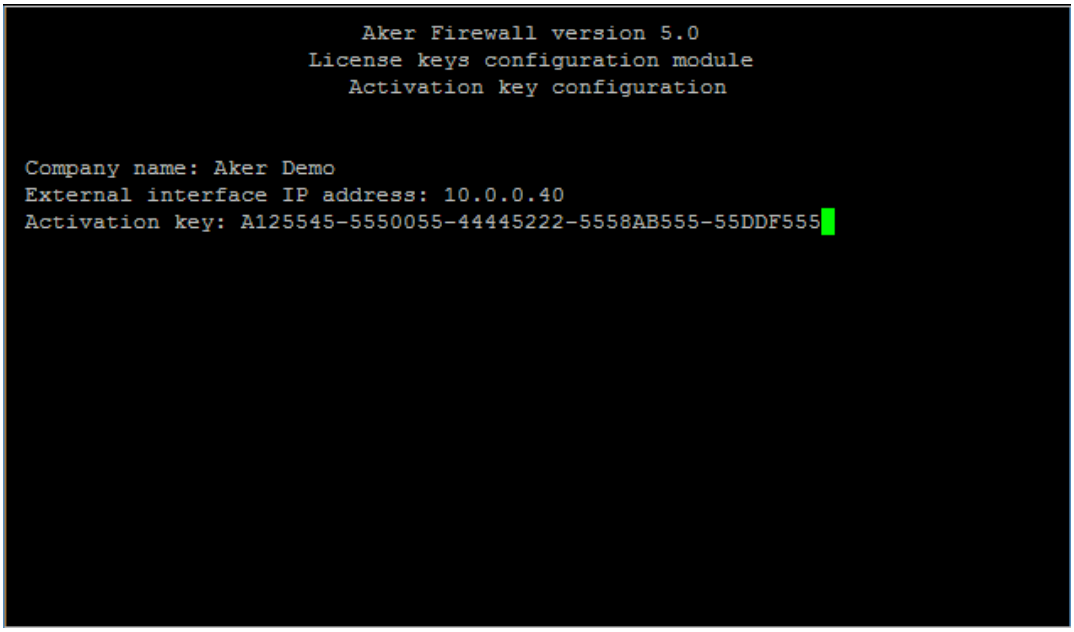
Program Location: `/etc/firewall/fwchave`

The program is interactive and the configuration options are described below:

By choosing the option 1, the same key entry program used during firewall installation will be shown.



Enter the data requested, according to your activation key.



By choosing Option 2, it is possible to add keys for additional licenses.

28-0 Configuring the Firewall in Cluster

This chapter shows how to configure the fault tolerance and the cooperative cluster of Aker Firewall

28-1 Planning the Installation

What is a fault tolerant system?

The more computers become prevalent in companies, offices and in the lives of people in general, the more we hear about "high availability". This is due to a simple good reason: no user wants a machine that stops working, or that network resources cannot be accessed. It is exactly high availability that will ensure continuous system operation of network services, storage and processing functions, even if there are failures in one or more elements.

Therefore, high availability is, increasingly, a subject of interest to users. And, without a doubt, it became a fundamental requirement for 24x7 systems, or for those which cannot be down for even a few minutes. After all, unplanned down time can compromise, at the very least, service quality, without mentioning the financial loss.

Fault tolerance is a group of resources that provide the illusion that the system is a single resource. The majority of its components, if not all of them, are duplicated so that, even if an individual component fails, service is not impacted. To enable this resource redundancy, a management mechanism is necessary to make its operation transparent.

What is a Cooperative System?

Under the fault tolerant system section above, high availability and group of resources were covered. In cooperative systems, besides these key features, there is the load balancing between systems. All firewalls remain active and, if their weight is equal, will handle connections and their processes, while balancing the load.

How does fault tolerance of Aker Firewall work?

Aker Firewall fault tolerance is composed of two connected systems with identical resources, that is, two connected machines with the same operating system, same network cards (NICS), and the same Firewall version. The same operating system is required to ensure that corrections made through the GUI are automatically duplicated in the other machine.

Besides being connected, through a network interface, to with each other, all network cards (NICS) of both machines should be connected to a hub or switch, so that both firewalls will have access to the same hosts and devices.

How does the Cooperative System of Aker Firewall work?

First of all, a basic configuration difference between the cooperative cluster and the failover is related to the licensing. A cooperative cluster license balances convergence evenly, according to the weights attributed to the firewalls. With a failover license, convergence occurs only in one of the firewalls.

What are the UNICAST and MULTICAST modes of Aker Firewall Cooperative System?

There are three basic types of IPv4 addresses: unicast, broadcast, and multicast. A unicast address is used to transport a packet to a single destination. A broadcast address, on the other hand, is used to send a datagram to an entire network. A multicast address, lastly, is used to deliver datagrams to a group of hosts, previously configured as members of a multicast group, possibly organized in geographically dispersed subnets.

Multicast is not connection-oriented. A multicast datagram is delivered to members of the target group with the same "best effort" that characterizes unicast IP datagrams. This means that datagram delivery is not guaranteed to arrive to all group members nor in the same order relative to other datagrams.

The only difference between a unicast IP packet and a multicast one is the presence of a group address in the destination address field of the multicast IP packet header. Instead of a class A, B or C address, multicasting uses class D addressing, with a format (224.0.0.0 239.255.255.255).

To transport a packet in a single transmission operation, UNICAST protocols imply only one transmitter and one receiver, while MULTICAST protocols involve one transmitter and multiple receivers.

Aker Firewall implements information exchange between cluster nodes in both protocols. The administrator should opt for one of both modes, noting that if the number of cooperative firewalls is large, MULTICAST is recommended.

When the cluster is active, any configuration change made in one firewall, through the GUI, will be automatically duplicated in the other firewall.

28-2 Using the Command Line Interface

Using the command line interface to configure fault tolerance is quite simple.

Program Location: `/etc/firewall/fwcluster`

Syntax:

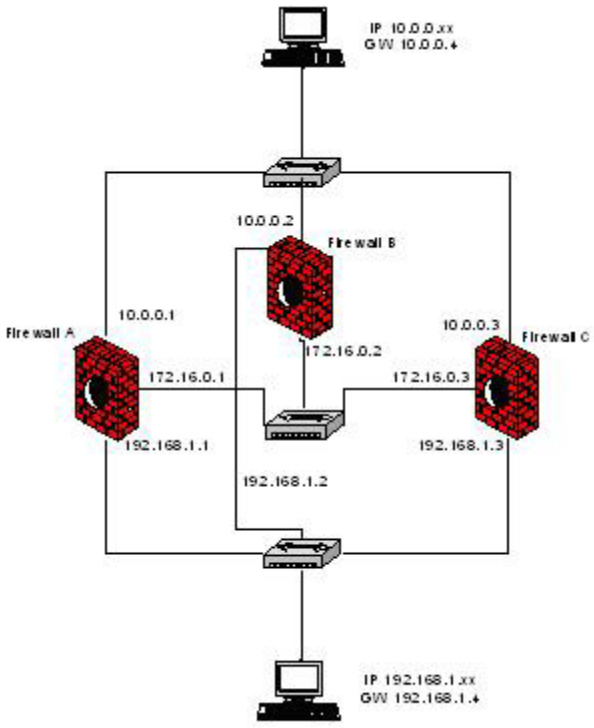
```
fwcluster [help | show]
fwcluster interface_control <if>
fwcluster weight <weight>
fwcluster <enable | disable>
fwcluster <include | remove> <if> [host | -f]
fwcluster <mode> <if> [multicast | unicast]
```

Program Help:

```
Aker Firewall - Version 5.0
Usage: fwcluster [help | show]
     fwcluster interface_control <if>
     fwcluster weight <weight>
     fwcluster <enable | disable>
     fwcluster <include | remove> <if> [host | -f]
     fwcluster <mode> <if> [multicast | unicast]
 where:
     if           : interface entity name
     weight       : this firewall weight within the cluster
     host         : virtual IP address to be included or removed (host
entity)
```

Example 1: (showing the configuration)

As a learning aid, we will explain the topology of a network with three clustered firewalls and two networks: 192 and 10.



Before setting up the cluster, initially, all interfaces should be registered reminding that, unlike firewall 4.5, here all firewalls have different IP addresses.

Examples: Firewall A - rl0 - if_external - 10.0.0.1 Firewall B - rl0 - if_external - 10.0.0.2
rl1 - if_internal - 192.168.1.1 rl1 - if_internal - 192.168.1.2
rl2 - if_control - 172.16.0.1 rl2 - if_control - 172.16.0.2

Firewall C – rl0 - if_external - 10.0.0.3
rl1 - if_internal - 192.168.1.3
rl2 - if_control - 172.16.0.3

Next, create a virtual entity for each network card (NICS), except for the control interface. These entities will have equal value for all clustered firewalls.

Examples: Firewall A - external_firewall (ip 10.0.0.4) Firewall B - external_firewall (ip 10.0.0.4)
internal_firewall (ip 192.168.1.4) internal_firewall (ip 192.168.1.4)

Firewall C - external_firewall (ip 10.0.0.4)
internal_firewall (ip 192.168.1.4)

To start configuring the cluster, first create the control interface:

```
/etc/firewall/fwcluster control_interface registered_interface
```

Then start registering each interface participating in the firewall:

```
/etc/firewall/fwcluster include registered_interface
registered_virtual_host
```

Define the weight of each Firewall or the default weight of 1 will be applied to all:

```
/etc/firewall/fwcluster weight weight_value
```

After applying these configurations to all participating firewalls, enable the cluster mode of each one:

```
/etc/firewall/fwcluster enable
```

 Cluster hosts don't have to be equal, but the network cards (NICS) do.

 For a fault tolerant, failover cluster, use only 2 firewalls, once that only one will handle all traffic.

29-0 System Files and Backup

In this chapter, we will show where the systems files that comprise version 5 of Aker Firewall are located and their use.

29-1 System Files

In this topic, the systems files and their location will be shown. This is very important for backups and troubleshooting

Directory Tree

- **`/etc/firewall`** - contains executable programs and sub-directories
- **`/etc/firewall/algs`** - external encryption algorithms for the encryption client
- **`/etc/firewall/x509`** - X.509 certificate files
- **`/etc/firewall/httpd`** - root of the file system of the local HTTP server of the WWW proxy. Do not remove the files already present in this directory.
- **`/etc/firewall/conf`** - firewall configuration files
- **`/etc/firewall/crls`** - list of the certificates which have been revoked by active Certification Authorities.
- **`/etc/firewall/snmpd`** - has the SNMP agent
- **`/etc/firewall/root`** - it has no files. It is used by a few Firewall processes.
- **`/etc/firewall/run`** - files needed for execution
- **`/var/log`** - log and event files of Aker Firewall
- **`/var/spool/firewall`** - used by the SMTP and POP3 proxies to store messages to be sent.
- **`/usr/src/sys/objs`** - contains pre-compiled firewall objects used to generate a new FreeBSD kernel for the system (for FreeBSD only).

Executable Programs

Programs that may be executed by the Aker Firewall administrators.

- **`/etc/firewall/fwadmin`** - command line interface for user administration
- **`/etc/firewall/fwaction`** - command line interface for configuring system's actions
- **`/etc/firewall/fwchave`** - command line interface for configuring the system's activation key
- **`/etc/firewall/fwcert`** - command line interface for configuring encryption certificates
- **`/etc/firewall/fwclient`** - command line interface for configuring encryption clients access
- **`/etc/firewall/fwcluster`** - command line interface for configuring fault tolerance
- **`/etc/firewall/fwcripto`** - command line interface for configuring encryption and authentication

- **/etc/firewall/fwdialup** - command line interface for configuring IP addresses for firewalls with a dynamic IP address (ADSL, for example)
- **/etc/firewall/fwent** - command line interface for creating entities
- **/etc/firewall/fwflood** - command line interface for configuring SYN flood protection
- **/etc/firewall/fwids** - command line interface for configuring IDS agent support
- **/etc/firewall/fwlist** - command line interface for accessing active connections and user sessions
- **/etc/firewall/fwlog** - command line interface for accessing firewall log and event files
- **/etc/firewall/fwnat** - command line interface for configuring network address translation (NAT)
- **/etc/firewall/fwpar** - command line interface for configuring general parameters
- **/etc/firewall/fwrule** - command line interface for configuring the intelligent packet filter
- **/etc/firewall/fwupgrade** - converts configuration files from version 4.5 to version 5.0 of Aker Firewall
- **/etc/firewall/fwipseccert** - command line interface for managing the X.509 certificates needed for IPsec encryption
- **/etc/firewall/fwstat** - command line interface for configuring and displaying Firewall stats
- **/etc/firewall/fwinterface** - command line interface for configuring the Firewall network interfaces
- **/etc/firewall/fwauth** - command line interface for configuring the Firewall global authentication parameters

Programs that SHOULD NOT be executed directly by the administrator

- **/kernel** - modified FreeBSD operating system Kernel with Aker Firewall support (only for FreeBSD)
- **/etc/firewall/aker_firewall_mod.ko** - Firewall kernel load module (only for FreeBSD)
- **/etc/firewall/2.2.x/aker_firewall_mod.o** - Firewall 2.2 kernel load module (only for Linux)
- **/etc/firewall/2.4.x/aker_firewall_mod.o** - Firewall 2.4 kernel load module (only for Linux)
- **/etc/firewall/fwauthd** - User authentication server
- **/etc/firewall/fwcardd** - X509 certificate validation module for smart cards
- **/etc/firewall/fwconfd** - Communication server for remote interface
- **/etc/firewall/fwclusterd** - Fault tolerance management server
- **/etc/firewall/fwcrld** - Download module for CRLs issued by active Certification Authorities
- **/etc/firewall/fwcryptd** - Encryption server
- **/etc/firewall/fwdnsd** - DNS - name resolution server for the remote interface
- **/etc/firewall/fwidsd** - program for integration with intrusion detection (IDS) agents

- **/etc/firewall/fwinit** - Aker Firewall initiation program
- **/etc/firewall/fwftppd** - Transparent FTP proxy
- **/etc/firewall/fwgkeyd** - Encryption keys generation server
- **/etc/firewall/fwhttppd** - Transparent HTTP proxy and non-transparent WWW proxy
- **/etc/firewall/fwlkeyd** - Encryption certificate server
- **/etc/firewall/fwmond** - Firewall process monitoring and reinitialization module
- **/etc/firewall/fwnatmond** - Machine monitoring module for load balancing
- **/etc/firewall/fwprofd** - User login server
- **/etc/firewall/fwrapd** - Real Player transparent proxy
- **/etc/firewall/fwsocksd** - Non-transparent SOCKS proxy
- **/etc/firewall/fwsmtppd** - Transparent SMTP proxy
- **/etc/firewall/fwpop3pd** - Transparent POP3 proxy
- **/etc/firewall/fwlogd** - Stats, events and log server
- **/etc/firewall/fwscanlogd** - Stats, events and log file query server
- **/etc/firewall/fwsyncd** - Synchronicity and encryption seed generation process
- **/etc/firewall/fwtelnetd** - Transparent telnet proxy
- **/etc/firewall/fwtrap** - Module for sending SNMP traps
- **/etc/firewall/fwurld** - Module for verification and analysis of URLs access permission
- **/etc/firewall/fwiked** - IPSEC encryption key negotiation module (IKE protocol)
- **/etc/firewall/libaker.so** - Firewall generic library
- **/etc/firewall/libconfd.so** - Firewall configuration library
- **/etc/firewall/snmpd/snmpd** - SNMP agent

Configuration Files

- **/etc/firewall/chave-500.fw** - Firewall activation key
- **/etc/firewall/conf/acesso.tab** - System access control list
- **/etc/firewall/conf/acesso.telnet** - Access control for the Telnet proxy contexts
- **/etc/firewall/conf/acl-500.tab** - Access profiles registered in the system
- **/etc/firewall/conf/ad_sites-500.http** - Banner blocking rules table
- **/etc/firewall/conf/auth-500.tab** - Global authentication parameters
- **/etc/firewall/conf/cert.fw** - Firewall local encryption certificate
- **/etc/firewall/conf/cert_ca.tab** - Certificates issued by certification entities
- **/etc/firewall/conf/cert_neg.tab** - Encryption negotiation certificates
- **/etc/firewall/conf/cert_rev.tab** - Revocation certificates
- **/etc/firewall/conf/cluster-500.fw** - Cluster configurations
- **/etc/firewall/conf/conf-500.tab** - General configuration parameters
- **/etc/firewall/conf/conjuntos-500.tab** - Entities of the group type registered in the system
- **/etc/firewall/conf/contextos-500.pop3** - Context list of the POP3 proxy
- **/etc/firewall/conf/contextos-500.smtp** - Context list of the SMTP proxy
- **/etc/firewall/conf/contextos.telnet** - Context list of the Telnet proxy

- **/etc/firewall/conf/contextos.ftp** - Context list of the FTP proxy
- **/etc/firewall/conf/cluster.fw** - Fault tolerance configuration
- **/etc/firewall/conf/crypt-500.tab** - Encryption/authentication table
- **/etc/firewall/conf/crypt_cl-500.tab** - Encryption client configuration table
- **/etc/firewall/conf/crypt_ex-500.tab** - Expanded encryption table
- **/etc/firewall/conf/entidades-500.crypt** - Encryption/authentication referenced entities
- **/etc/firewall/conf/entidades-500.tab** - Entities registered in the system
- **/etc/firewall/conf/entidades-500.filtro** - Entities referenced by filtering rules
- **/etc/firewall/conf/eqv_if-500.conf** - Interface configuration
- **/etc/firewall/conf/estatisticas-500.tab** - Statistics table
- **/etc/firewall/conf/filtros-500.pop3** - POP3 context filter list
- **/etc/firewall/conf/filtros-500.smtp** - SMTP context filter list
- **/etc/firewall/conf/flows-500.tab** - Load balancing internal control file
- **/etc/firewall/conf/groups_ca.tab** - Certification Authorities pseudogroup list
- **/etc/firewall/conf/ike_ex-500.tab** - IPsec configuration file
- **/etc/firewall/conf/nat-500.bal** - Load balancing configuration parameters
- **/etc/firewall/conf/nat-500.tab** - Network Address Translation rules (NAT)
- **/etc/firewall/conf/parametros-500.fw** - General system configuration parameters
- **/etc/firewall/conf/parametros-500.http** - WWW proxy configuration parameters
- **/etc/firewall/conf/parametros-500.ids** - IDS agent support configuration parameters
- **/etc/firewall/conf/prof_cert.tab** - Certificate for communicating with authentication clients
- **/etc/firewall/conf/regras-500.filtro** - Stateful filter rules
- **/etc/firewall/conf/regras-500.perfil** - Access profiles rules
- **/etc/firewall/conf/regras-500.socks** - SOCKS proxy rules
- **/etc/firewall/conf/sites-500.tab** - Web addresses used in access profiles
- **/etc/firewall/conf/syn-500.tab** - SYN flood protection address table
- **/etc/firewall/conf/usuarios.tab** - User table for remote user administration

Execution Files

- **/etc/firewall/run/fwauthd.pid** - Stores the authentication server process identification (PID)
- **/etc/firewall/run/fwclusterd.pid** - Stores the fault tolerance main process ID (PID)
- **/etc/firewall/run/fwcrld.pid** - Stores the CRLs download process ID (PID)
- **/etc/firewall/run/fwgkeyd.pid** - Stores the encryption key server process ID (PID)

- **`/etc/firewall/run/fwhttpd.pid`** - Stores the process ID (PID) of the HTTP proxy
- **`/etc/firewall/run/fwhidsd.pid`** - Stores the process ID (PID) of the communication with IDS agents
- **`/etc/firewall/run/fwlkeyd.pid`** - Stores the certificates server process ID (PID)
- **`/etc/firewall/run/fwnatmond.pid`** - Stores the machine monitoring process ID (PID)
- **`/etc/firewall/run/fwprofd.pid`** - Stores the user login server process ID (PID)
- **`/etc/firewall/run/fwsocksd.pid`** - Stores the SOCKS proxy process ID (PID)
- **`/etc/firewall/run/fwlogd.pid`** - Stores the log server process ID (PID)
- **`/etc/firewall/run/fwscanlogd.pid`** - Stores the log scan server process ID (PID)
- **`/etc/firewall/run/fwiked.pid`** - Stores IPsec key negotiation process ID (PID)
- **`/etc/firewall/run/fwurld.pid`** - Stores the URL validation process ID (PID)

Stats, Events and Log Files

- **`/var/log/fw-500-AAAAMMDD.fwlg`** - Stores firewall logs of date YYYY/MM/DD
- **`/var/log/fw-500-AAAAMMDD.fwev`** - Stores firewall events of date YYYY/MM/DD
- **`/var/log/stat-500-AAAAMMDD.fws`** - Stores firewall stats of date YYYY/MM/DD

29-2 Firewall Backup

Version 3.0 of Aker Firewall provided the option to remotely generate backup copies and completely recover its configuration. This was covered in the chapter entitled using GUI tools This remote procedure is recommended for the majority of installations as it is easy to use and allows storage of all firewall configurations in a remote machine. If desirable, however, a manual backup operation is possible, as with versions 2.0 and earlier.

In this topic, we will show the manual backup procedure to generate a complete security copy and how to recover the installation after a disaster.

Files to be copied

- The files that must be copied are the configuration files presented in the previous topic. This should be done every time the firewall configuration is changed.
- Other key files are the event and log files. Depending on the security requirements, daily, or even more frequent, copies of these files can be generated. Another option to increase security is to configure the Firewall to send log and event records to the syslogd (syslog Daemon process) and configure the syslogd to redirect these messages to another host of the internal network.

To generate backup copies, the FreeBSD and Linux **`tar`** utility tool can be used (commands below should be issued by the super user root):

- **`tar cvfz /conf.tgz /etc/firewall/conf`**
  (saves all firewall configuration into file /`conf.tgz`)

- **`tar cvfz /log.tgz /var/log/log-500.fw /var/log/events-500.fw`**
  (saves events and log files into the file /`log.tgz`)

After generating the copies, files `conf.tgz` and `log.tgz` can be transferred to other machines through, for example, FTP.

Recovery in case of disasters

In case of data loss, proceed as follows:

- In case only logs and configuration data were lost, just restore one of the backups mentioned above.

It is important that no firewall process is active when the files are being restored. To be sure of that, the machine can be reinitialized in single-user mode or all firewall processes can be killed with command: **`kill `ps -ax | grep fw | grep -v grep | cut -c 1-5``**).

To restore a security copy made with the **`tar`** command shown above, execute the following command sequence (which should be issued by the super user root):

1. **cd /**
2. **=tar xvfz /conf.tgz**
   (restores configuration files)
3. **tar xvfz /log.tgz**
   (restores log files)

- In case of total data loss, first verify if the operating system is intact. If there's doubt, initially re-install all FreeBSD or Linux. After that, re-install Aker Firewall, following all procedures described in the system installation chapter. With all components working properly, restore the configuration backup, the log and the event files, as shown above.

30-0 Aker Firewall Box

This chapters shows all commands that can be used in Aker Firewall Box shell

Aker Firewall Box

Aker Firewall Box is an appliance, that is, an integrated solution of hardware and software. The great advantage of this platform is that it does not require any knowledge of any operating system. Besides, by having all its configuration stored in a flash memory and because it is an industrial hardware, the platform presents more resistance against problems, specially those caused by energy problems.

Aker Firewall Box is available on several different models, that are designed to fulfill the needs of small, medium and large companies.

The complete list of all available models is frequently updated and can be viewed at:

http://www.aker.com.br/index.php?pag_cod=8&prod_cod=21&ling=en_us&cat_cod=8&itens=caracteristicas

How does Aker Firewall box shell work?

When a remote terminal configured at 9600 bps is connected to the corresponding serial interface on a Aker Firewall Box, it is possible to use its shell.

When this procedure is performed, it is first necessary to press the Enter key, until the password prompt appears. The initial password is '123456' and if it is type correctly, the following prompt will be shown:

```
Aker>
```

In case the local access password of the firewall is lost, it is necessary to contact the technical support in order to initiate the password reset procedure.

In the shell prompt, all standard commands of Aker Firewall can be typed, as described on the topics covering the command line interface on each chapter. In addition of those, there are specific commands of Aker Firewall box that are documented below:

 It is possible to type the firewall commands in the shell without the fw prefix, that is, `ent` instead of `fwent`.

To exit from the shell, it is enough to type in the commands `exit` or `quit` or simply to press the Ctrl + D keys.

Specific commands of Aker Firewall Box

Command	`quit` `exit`
Description	Finish the shell session

Command	`help` `?`
Description	Show a list with all valid commands

Command	`shutdown`
Description	Shuts down the firewall, so it can be turned off

Command	`reboot`
Description	Reboots the firewall

Command	`ping [-c n_pkt] [-i interv] destination_ip`
Description	Sends ping packets and waits for replies The `-c` option specifies the number of packets to be sent The `-i` option specifies the transmission interval between the packets in milliseconds (ms)

Command	`password`
Description	Changes the firewall local access password

Command	`date <show> | <mm/dd/yyyy>`
Description	With the `show` argument informs the system date. Otherwise sets the date to the informed value.

Command	`time <show> | <hh:mm[:ss]>`
Description	With the `show` argument informs the system time. Otherwise sets the time to the informed value.

Command	`hd <-enable | -disable >`
Description	Enables or disables the use of a hard disk.

Appendix A - System messages

Firewall log messages

All the messages below may appear in he firewall log. Whenever they appear, they will be preceding a record with the information about the packet that produced them. On the left, a number corresponding to each message is shown.

001 - Possible fragmentation attack

This message indicates that the packet filter received a TCP packet fragmented in the TCP header, probably resulted from an attempt of a fragmentation attack. For further information refer to RFC 1858

002 - Source routed IP packet

This message indicates that the packet filter received an IP packet with one of the following options: Record Route, Loose Routing or Strict Routing and it was configured not to accept source routed IP packets. For further information refer to RFC 791

003 - Land attack

A land attack consists of simulating a connection from a port to itself. It causes the crash of the attacked host in great part of the TCP/IP implementations.

This message indicates that the packet filter received a packet whose source address is the same as its destination address and whose source port is the same as its destination port, characterizing this kind of attack.

004 - Connection is not present in the dynamic table

This message indicates that the firewall received a TCP packet that was not a connection request and was addressed to a not open connection. It can be caused by an attack or, simply, by a connection that was inactive for longer than the TCP connections timeout.

005 - Packet was received from an invalid interface

This message indicates that the packet filter received an IP packet from an interface different from the one specified in the filtering rule which it fitted in. This may be caused by an attack of IP address spoofing or by a wrong filtering rule configuration.

006 - Packet was received from an unknown interface

This message indicates that the packet filter received a packet but could not determine its source interface. As a interface is specified in the corresponding filtering, the packet was rejected. This message will probably never be shown.

007 - Control connection not open

This message indicates that the firewall received a packet from a data connection (from a protocol which uses more than one connection, FTP and Real Audio / Real Video, for instance) and the corresponding control connection was not opened.

008 - Invalid TCP flags

This message indicates that the firewall received a TCP packet whose flags were invalid or contradictory (for example, SYN and FIN in the same packet). This may characterize an attack or a defective TCP/IP implementation.

009 - Invalid TCP sequence number

This message indicates that the firewall received a TCP packet whose sequence number was out of the expected values. This may characterize an attack.

010 - Possible SYN Flood attack

This message is generated by the Firewall when a connection is initiated to one of the addresses protected against SYN floods and the connection was not established in the maximum amount of time configured by the administrator. If this message occurs isolated, or with little incidence, then the interval of time configured in the SYN Flood protection (refer to The SYN Flood protection) probably is very small. If a high number of these messages appear successively, then a SYN flood attack was probably repelled by the firewall.

011 - Packet without authentication information

This message indicates that the given packet came without an authentication header and the configuration of the corresponding secure channel indicates that it could only be accepted if authenticated (refer to the chapter Creating secure channels). It may be caused by a wrong configuration of the authentication channels (configuring, probably, only one end of the communication) or by an attempt of IP address spoofing. For further information refer to RFCs 1825 and 1827.

012 - Packet has failed authentication

This message indicates that the given packet was not successfully validated by the firewall authentication module. It may be caused by an invalid authentication key configuration, by improper alterations in the packet contents while it was in transit or by an attack of IP address spoofing. For further information refer to RFCs 1825 and 1827.

013 - Packet without encryption information

This message indicates that the given packet did not come encrypted and the configuration of the corresponding secure channel indicates that it should have (refer to the chapter Creating secure channels). It may be caused by a wrong configuration of the secure channels (configuring, probably, only one end of the communication) or by an attack of IP address spoofing. For further information refer to RFCs 1825 and 1827.

014 - The size of the packet to be decrypted is invalid

This message indicates that the decryption module detected that the size of the packet to be decrypted is incompatible to the corresponding encryption algorithm. It is probably caused by a wrong configuration of the secure channels.

015 - Packet decryption has failed

This message indicates that the decryption module, after decrypting the packet and performing its consistence tests, detected that it is invalid. It is probably caused by a wrong secure channels table configuration or by a possible IP address spoofing attack.

016 - Invalid packet encapsulation type

This message indicates that the decryption module did not recognize the type of encapsulation used in this packet. It may be caused by a failure in the packet decryption (due to wrong keys) or by the use of an unsupported encapsulation. (Aker Firewall works exclusively with tunnel mode encapsulation, not accepting any other modes, for example, the transport mode).

017 - Packet without SKIP information

This message indicates that the given packet did not come with a SKIP header and the corresponding secure channel configuration indicates that it should have. This is probably caused by a wrong configuration of the secure channels table, where one of the ends is configured to use SKIP or Aker-CDP and the other one is not (refer to the chapter Creating secure channels).

018 - SA for the packet doesn't contain SKIP information

This message indicates that the decryption module received a packet with a SKIP header and the corresponding security association (SA) does not have information about SKIP (refer to the chapter Creating secure channels). This is probably caused by a wrong configuration in the secure channels table, where one of the ends is configured to use SKIP or Aker-CDP and the other one is not.

019 - Invalid SKIP protocol version

This message indicates that the version of the SKIP protocol indicated in the given packet, is different from the supported version. (Aker Firewall implements the version 1 of the SKIP protocol).

020 - Invalid SKIP protocol counter value

The SKIP protocol sends a counter in each packet, which is incremented every hour, to avoid attacks of sequence repetition. This message indicates that the value of the counter received in the given packet is invalid. It may have two distinct causes: either the difference of the internal clocks of the two communicating firewall is more than one hour or there was an attempt of a sequence repetition attack.

021 - Invalid SPI for SKIP authentication

This message indicates that a SKIP packet was received and the SPI number specified in the authentication header was invalid. (The SKIP protocol demands the SPI number to be 1).

022 - The next protocol in the SKIP header is invalid

This message indicates that the next protocol of the SKIP header of the given packet is not supported. (Aker Firewall demands that the authentication header comes SKIP header).

023 - Invalid SKIP authentication algorithm

This message indicates that the authentication algorithm specified in the SKIP header is not supported (Aker Firewall only supports the MD5 and SHA-1 authentication algorithms).

024 - Invalid SKIP encryption algorithm

This message indicates that the encryption algorithm specified in the SKIP header is not supported (Aker Firewall only supports the DES, Triple DES and Blowfish, with key sizes of 128 and 256 bits, encryption algorithms).

025 - Invalid SKIP key encryption algorithm

This message indicates that the encryption and key separation algorithm specified in the SKIP header is not supported (Aker Firewall only supports the algorithms DES with MD5 as key separator, Triple DES with MD5 as key separator and Blowfish, with MD5 as key separator).

026 - Data compression algorithm not supported

This message indicates that the data compression algorithm specified in the SKIP header is not supported (Aker Firewall does not support any data compression algorithms, since they are still not standardized).

027 - Invalid source name space identificator

The SKIP protocol allows the use of other name spaces, which are not the IP addresses, to select the corresponding security association (SA). The name space may be specified

for source and /or destination. This message indicates that the source name space is not supported. (Aker Firewall only supports IP addresses as name space).

028 - Invalid destination name space identificator

The SKIP protocol allows the use of other name spaces, which are not the IP addresses, to select the corresponding security association (SA). The name space may be specified for source and /or destination. This message indicates that the destination name space is not supported. (Aker Firewall only supports IP addresses as name space).

029 - Invalid Aker-CDP protocol version

This message indicates the firewall received a packet of the Aker-CDP protocol with an invalid version.

030 - Invalid packet length for Aker-CDP protocol

This message indicates the firewall received a packet of the Aker-CDP protocol with an invalid size.

031 - Invalid authentication for Aker-CDP control packet

This message indicates the firewall received an Aker-CDP control packet with an invalid authentication. The most probable causes are a modification of the packet during its transmission or a possible attack attempt.

032 - Number of firewall licenses has been reached

The Aker Firewall is licensed according to the number of hosts in the private(s) network(s) which is(are) being protected. This message indicates the firewall detected a number of internal hosts greater than the number of acquired licenses and, because of that, it didn't allowed this exceeding hosts to open connections through it.

Solution: Contact the Aker Security Solutions or its authorized representative and ask for a upgrade of the number of licenses.

033 - Packet discarded by an IDS blocking rule

This message indicates that the firewall received a packet that matched a temporary rule added by the intrusion detection agent e, due to this, was discarded (for more information, refer to chapter Configuring the Intrusion Detection Agent)

034 - Bad AH header in packet (length field)

This message indicates that the firewall has received an IPSEC encrypted packet with incorrect authentication information in AH header. Refer to RFC 2402 for more information.

035 - Simultaneous AH and ESP tunneling not allowed

This message indicates that the firewall has received an IPSEC encrypted packet, with double tunneling (ESP and AH). This is not allowed.

036 - SA for this packet not established

This message indicates that the firewall has received an IPSEC encrypted packet for a tunnel that hasn't been negotiated.

037 - Needed padding too big

This message indicates that the firewall has calculated a padding for the ESP protocol which is bigger than the maximum allowed size. Probably the algorithm block size is too large.

038 - Incorrect decrypted padding length

This message indicates that the firewall has decrypted an IPSEC packet that supposed was bigger than its actual size. Probably the packet is corrupted or errors when exchanging the keys have happend.

039 - Error starting authentication for specified algorithm

This message indicates that the firewall hasn't been able to authenticate the packet with HMAC algorithm. Probably the authentication algorithm is not working properly.

040 - Error finalizing authentication with chosen algorithm

This message indicates that the firewall hasn't been able to authenticate the packet with HMAC algorithm. Probably the authentication algorithm is not working properly.

041 - Connection end

This message is just a register of a connection ending and shouldn't appear in the firewall log.

042 - Configured conections from the same IP limit exceeded

This message happens when the maximum number of connections configured in the flood protection module has been reached. In order to check the configuration of this module, please follow the instructions present in chapter Flood protection.

Firewall event messages

043 - Aker Firewall 5 - Initialization complete

This is an informative message that will be produced every time the firewall is restarted.

044 - Memory allocation error

This message indicates that a firewall module tried to allocate memory and received an error. This message may occur in systems with a small amount of RAM memory using addresses translation with a high number of simultaneous connections or a high number of active connections going through the firewall proxies.

Solution: Install more RAM memory.

045 - TCP translation table full

The TCP address translation table is full. The only solution to this problem is to decrease the TCP timeout in the configuration parameters. For more information refer to chapter Configuring the system parameters.

046 - UDP translation table full

The UDP address translation table is full. The only solution to this problem is to decrease the UDP timeout in the configuration parameters. For more information refer to chapter Configuring the system parameters.

047 - Clients secure channels table full

This message indicates that an encryption client tried to establish and secure channel with the firewall, however, the number of already established sessions reached the system configured limit.

Solution: Increase the maximum number of simultaneous sessions for encryption clients. If necessary, contact the Aker Security Solutions or its authorized representative and ask for an upgrade of the number of encryption client licenses.

048 - Invalid authentication algorithm

The encryption module detected an invalid authentication algorithm in the security association (SA), when performing the authentication of a packet.

Solution: Contact the technical support

049 - Invalid encryption algorithm

The encryption module detected an invalid encryption algorithm in the security association (SA), when performing the encryption of a packet.

Solution: Contact the technical support

050 - Invalid data received by the firewall load module

This message indicates that invalid data was sent to the firewall modules that run in the FreeBSD or Linux kernel. The Invalid data must have been produced by a program running in a firewall machine

Solution: Try to verify which program produces this message when run it and do not run it again.

051 - Error when reading parameters file

This message is produced by any of the the external modules when trying to read the parameters file and detecting it does not exist or can't be read.

Solution: Restart the firewall for the initialization program will recreate the parameters file. If it does not work, contact the technical support.

052 - Error when loading access profiles

This message indicates that the authentication server or the users login server could not load the list of registered access profiles in the system.

Solution: Contact the technical support.

053 - Error when loading entities

This message indicates that a server process could not load the list of entites registered in the system.

Solution: Contact the technical support.

053 - Invalid access profile name

This message indicates that the authentication server, when trying to find the access profile of a user, discovered that the profile is not registered in the system.

Solution: Contact the technical support.

055 - Error when creating the connection socket

This message indicates that some external modules tried to create a socket and received an error message.

Solution: Verify the number of files that can be opened by a process and the total number for the system. If necessary increase these values. For further information on how to proceed, contact the technical support.

056 - Line with an excessive number of characters

This message indicates that a Aker Firewall proxy received a line with an excessive number of characters and due to it, closed the connection. The complementary information in parenthesis indicates the IP address of the host that caused the problem.

Solution: This message is caused by a server or a client out of the RFCs standard. The only possible solution to this problem is to contact the administrator of the host that caused the message.

057 - Error when loading context

This messages indicates that one of the transparent proxies could not load the specified context.

Solution: Contact the technical support.

058 - Error when loading secure channels table

This message indicates that one of the firewall daemons were unable to load the secure channels table.

Solution: Contact the technical support.

059 - Reverse DNS not configured

This message is produced by any of the proxies, if they were configured only to accept connections from hosts with a valid reverse DNS and could not resolve the name for the source IP address of a connection. The complementary message indicates the source IP address of the connection.

060 - Conflicting direct and reverse DNS

When a proxy of the firewall is configured to accept only connections from hosts with valid reverse DNS, it uses a technique to add more security: first it tries to resolve the name for the source IP address of the connection. If it can not do it, it indicates the error showing the preceding message and does not allow the connection to be established. If it resolves the name, it does another DNS lookup from the returned name, searching for its IP address. If it can not perform this second lookup or if the returned IP address is different from the source address, the connection is aborted and this message is produced.

061 - Possible protocol simulation attack

This message indicates that, during the inspection of a session of a protocol with multiple connections (FTP and Real Audio / Real Video, for instance), the firewall detected an attempt to open a connection to a port lower than 1024 or to an address different from the expected one. It is probably caused by an attack or by a defective protocol implementation.

062 - Invalid Command

This message indicates that one of the proxies received a command considered invalid from the client and, due to it, did not transfer it to the server. The complementary messages indicate which was the invalid command and which were the source and destination hosts (only in case of a transparent proxy) of the connection.

063 - SMTP message accepted

This message indicates that the transparent SMTP proxy accepted a message and sent it to the server. The complementary messages indicate which were the source and destination hosts of the connection.

064 - SMTP message refused

This message indicates that the transparent SMTP proxy rejected a received message. It was caused because the message matched some filter that indicated it should be rejected or for being bigger than the maximum allowed size.

065 - SMTP connection refused by DNS rule

This message indicates that the transparent SMTP proxy rejected a received message. It was caused because the message matched a DNS rule.

066 - SMTP connection refused by RBL

This message indicates that the transparent SMTP proxy rejected a received message because it was found in at least one RBL

067 - SMTP connection refused by server or server down

This message indicates that the transparent SMTP proxy tried to establish a connection with the destination SMTP server, however it was refused or the server is down.

068 - Line size exceeded by SMTP client

The SMTP client has sent a line too lengthy, which cannot be handled by the SMTP proxy. Check that the client is following RFC standards or configure it do to so.

069 - SMTP connection closed by client

The SMTP client has unexpectedly closed the connection. This may have happen due to user intervention or by client problems. Usually those connections are restarted automatically.

070 - Line size exceeded by SMTP server

The SMTP server has sent a line to lengthy, which cannot be handled by the SMTP proxy. Check that the server is following RFC standards or configure it do to so.

071 - SMTP connection closed by server

The SMTP server has unexpectedly closed the connection. This may have happen due to user intervention or by client problems. Usually those connections are restarted automatically.

072 - SMTP server had trouble handling requisition

This message indicates that the SMTP server could not process the SMTP transaction.

073 - Invalid email address received from SMTP client

This message indicates that the SMTP client has supplied an invalid e-mail address.

074 - Relay attempt blocked

This message indicates that a relay attempt has been denied by the firewall. Please refer to chapter configuring the SMTP proxy for more information.

075 - Out of disk space while analysing message

This message indicates that the firewall hard disk or file system is full and, due to this fact, the SMTP proxy couldn't handle the message.

076 - Message maximum size exceeded

This message indicates that the SMTP message size was bigger than the maximum allowed size. Please refer to chapter configuring the SMTP proxy for more information.

077 - Bad message: syntax error

This message indicates that the SMTP proxy has received an incorrectly encoded message. This is usually generated by SPAM programs.

078 - Attachment with virus removed from message

This message indicates that a message attachment contained virus and has been removed. The message complement indicates who were the sender and the recipient of the message, as well as the name of the virus found.

079 - Attachment removed from message

This message indicates that a message attachment has been removed. The message complement indicates who were the sender and the recipient of the message.

080 - Message dropped because of its attachment

This message indicates that a SMTP message had an unacceptable attachment (due to the configured rules) and has been blocked by the SMTP proxy of the firewall. The message complement indicates who were the sender and the recipient of the message.

081 - Attachment with virus desinfected

This message indicates that a SMTP message attachment contained virus and has been disinfected. The message complement indicates who were the sender and the recipient of the message, as well as the name of the virus found.

082 - Bad coded attachment (bad message)

This message indicates that a SMTP message attachment has been incorrectly encoded, or presents MIME encoding problems. Usually this attachment can be discarded by the firewall if the administrator configures it to to so. Please refer to chapter configuring the SMTP proxy for more information.

083 - URL accepted

This message indicates that the WWW proxy accepted an URL request made by an user. The complementary message inside parenthesis indicates the user that made the request. The second message line indicates the IP address of the host from which the request was made and the third line indicates the URL that was accessed.

This message will only be generated for URLs of the HTTP protocol when they result in HTML code. For the FTP and Gopher protocols, it will be generated for each accepted request, regardless of its type.

084 - Local file download accepted

This message indicates that the WWW proxy has accepted a URL request made by an user. The complementary message indicates the username where the request came from. The remaining messages indicate the IP address of the host where the request came from and the URL.

This message refers only to files stored locally in the firewall, that was requested using the WWW proxy as a web server.

085 - URL refused

This message indicates that the WWW proxy rejected an URL request made by an user. The complementary message inside parenthesis indicates the user that made the request. The second message line indicates the IP address of the host from which the request was made and the third line indicates the URL that the user tried to acess.

086 - Banner Removed

This message indicates that the WWW proxy has replaced a banner by a blank image, due to the fact that the URL matched a banner filtering rule. The complementary message indicates the username where the request came from. The remaining messages indicate the IP address of the host where the request came from and the URL.

087 - Packet did not match any SOCKS proxy rule

This message indicates that the SOCKS proxy received a request to establish a TCP connection or to send an UDP packet and the request did not match any rule of the corresponding access profile. Due to this, the request was denied.

The complementary messages indicate the login of the user that sent the request (if user authentication is enabled), the client address, the destination address and its protocol.

088 - UDP packet accepted by SOCKS proxy

This message indicates that the SOCKS proxy received a request to send an UDP packet and it was sent, due to the existence of a rule in the corresponding access profile allowing the proxy to do so.

The complementary messages indicate the login of the user that sent the packet (if user authentication is enabled), the client address and the destination address.

089 - UDP packet refused by SOCKS proxy

This message indicates that the SOCKS proxy received a request to send an UDP packet and it was refused, due to the existence of a rule in the corresponding access profile indicating that the proxy should not accept such a request.

The complementary messages indicate the login of the user that tried to send the packet (if user authentication is enabled), the client address and the destination address.

090 - TCP connection established through SOCKS proxy

This message indicates that the SOCKS proxy received a request to establish a TCP connection and it was established, due to the existence of a rule in the corresponding access profile allowing the proxy to do so.

The complementary messages indicate the login of the user that established the connection (if user authentication is enabled), the client address and the destination address.

091 - TCP connection finished through SOCKS proxy

This message is generated each time a TCP connection is closed through the SOCKS proxy.

The complementary messages indicate the login of the user that had established the connection (if user authentication is enabled), the client address and the destination address.

092 - TCP connection refused by SOCKS proxy

This message indicates that the SOCKS proxy received a request to establish a TCP connection and it was refused, due to the existence of a rule in the corresponding access profile indicating that the proxy should not accept such a connection.

The complementary messages indicate the login of the user that tried to establish the connection (if user authentication is enabled), the client address and the destination address.

093 - Incorrect data received by SOCKS proxy

This message is generated when the SOCKS proxy receives data from a client that are not according to SOCKS protocol specification. Example of such invalid data can be a protocol version different from 4 or 5, a blank destination address, among others.

094 - Error when communicating with the authentication server

This message indicates that one of the proxies could not communicate with the authentication server when trying to perform an user authentication. Due to it, the user was not allowed to continue and the connection was refused.

Solution: Verify if the process of the authentication server is active on the firewall. To do it, execute the command #**`ps -ax | grep fwauthd | grep -v grep`**. If the process does not appear, start it with the command **`/etc/firewall/fwauthd`**. If the process is active or if this problem persists, contact the technical support.

095 - Error when connecting to the authentication agent

This message indicates that the authentication server was not able to connect to the authentication agent that would be running on a specific host. The complementary message indicates the name of the authentication agent that could not be connected and the IP address where it is supposed to be running.

Solution: Verify if the IP address, in the authenticator definition, of the host where the agent is supposed to be running is correct (for further information, refer to the chapter Registering entities), and that the agent is really running on that host.

096 - Error when communicating with the authentication agent

This message indicates that the authentication server connected to the authentication agent, but could not establish a communication. The complementary message indicates the name of the authentication agent that caused the problem and the IP address of the host where it is running on.

Solution: Verify if the access password in the definition of the authenticator is equal to the password in the configuration of the authentication agent. For further information, refer to the chapter Registering entities

097 - Error when connecting to IDS agent

This message indicates that the firewall was not able to connect to the IDS agent that would be running on a specific host. The complementary message indicates the name of the IDS agent that could not be connected and the IP address where it is supposed to be running.

Solution: Verify if the IP address, in the entity definition, of the host where the agent is supposed to be running is correct (for further information, refer to the chapter Registering entities), and that the agent is really running on that host.

098 - Error when communicating with IDS agent

This message indicates that the firewall connected to the IDS agent, but could not establish a communication. The complementary message indicates the name of the IDS agent that caused the problem and the IP address of the host where it is running on.

Solution: Verify if the access password in the definition of the entity is equal to the password in the configuration of the IDS agent. For further information, refer to the chapter Registering entities

099 - IDS blocking rule added

This message indicates that the intrusion detection agent added a temporary blocking rule in the firewall due to the occurrence of an event.

The complementary messages indicate the kind of blocking that was added (source, destination and/or service) and the addresses and/or services blocked.

100 - Error when connecting to anti-virus server

This message indicates that the firewall was not able to connect to the anti-virus server that would be running on a specific host. The complementary message indicates the name of the anti-virus server that could not be connected and the IP address where it is supposed to be running.

Solution: Verify if the IP address, in the entity definition, of the host where the server is supposed to be running is correct (for further information, refer to the chapter Registering entities), and that the anti-virus server is really running on that host.

101 - Error when communicating with anti-virus server

This message indicates that the firewall connected to the anti-virus server, but could not establish a communication. The complementary message indicates the name of the anti-virus server that caused the problem and the IP address of the host where it is running on.

Solution: Verify if the access password in the definition of the entity is equal to the password in the configuration of the anti-virus server. For further information, refer to the chapter Registering entities

102 - Error when connecting to URL analyzer

This message indicates that the firewall was not able to connect to the URL analyzer that would be running on a specific host. The complementary message indicates the name of the URL analyzer that could not be connected and the IP address where it is supposed to be running.

Solution: Verify if the IP address, in the entity definition, of the host where the analyzer is supposed to be running is correct (for further information, refer to the chapter Registering entities), and that the URL analyzer is really running on that host.

103 - Error when communicating with URL analyzer

This message indicates that the firewall connected to the URL analyzer, but could not establish a communication. The complementary message indicates the name of the URL analyzer that caused the problem and the IP address of the host where it is running on.

Solution: Verify if the access password in the definition of the entity is equal to the password in the configuration of the URL analyzer. For further information, refer to the chapter Registering entities

104 - New host detected in the cluster

105 - Cluster host is down

106 - Invalid heartbeat packet

107 - Cluster convergence completed successfully

108 - Firewall activation key repeated

109 - Proxy authentication failure

This message indicates that a user entered an invalid password, when trying to be authenticated in a specific proxy. The complementary messages indicate the user name and the source and destination hosts (only in case of a transparent proxy) of the connection.

110 - User unregistered for proxy

This message indicates that an unregistered user tried to be authenticated in a specific proxy. The complementary message indicates the source and destination hosts (in case of a transparent proxy only) of the connection.

111 - User lacks permission to open telnet sessions

This message indicates that a user was authenticated correctly in the telnet proxy, but was not allowed to open the desired connection. The complementary messages indicate the name of the user and the source and destination hosts of the connection.

112 - Telnet session established

This message indicates that a user was authenticated correctly in the telnet proxy and was allowed to open the desired connection. Due to it, the connection was established. The complementary messages indicate the name of the user and the source and destination hosts of the connection.

113 - Telnet session finished

This message indicates that a user closed a telnet session. The complementary messages indicate the name of the user and the source and destination hosts of the connection.

114 - Error when sending data to the firewall kernel

This message indicates that some external module tried to send information to the firewall modules that run in the kernel and received an error message. If there is a complementary message in parenthesis, it will indicate which information was being sent

Solution: Verify if the Aker Firewall module is loaded in the kernel. In FreeBSD use the command **`kldstat`** and in Linux the command **`lsmod`**. In both cases a module named **`aker_firewall_mod`** must appear.

115 - Error when saving certificates

This message indicates that the firewall was unable to save a certificates list in the hard disk.

Solution: Verify if there is free space in the filesystem '/' of the firewall. This can be done through the command **`"$df -k"`**. If this command shows the directory '/' with 100% of used space, then this is the cause of the problem. If there is free space and this error still appears, consult the technical support.

116 - Error when loading certificates

This message indicates the firewall was unable to load a certificates list.

Solution: Contact the technical support

117 - Invalid received certificate

This message indicates the firewall certificates server received an invalid certificate. This can have one of the following causes:

- Invalid certificate signature
- Unknown certification authority
- Expired certificate

The complementary messages indicate which of these possible errors happened and which firewall emited the invalid certificate.

118 - Certificate received and validated correctly

This message indicates the firewall certificates server received a valid negotiation or revogation certificate. The complementary messages indicate the type of the received certificate and which firewall emited it.

119 - Invalid encryption client request

This message indicates the certificates server received an encryption client request and this request was considered invalid. This can have one of the following causes:

- The firewall certificate was updated and the client is still using an old one
- The request came from a host non-authorized to establish secure channels with the firewall.

The complementary messages indicate the cause of the problem and the addresses of the source and destination hosts (the destination is the IP address of the host behind the firewall which the client tried to communicate with).

120 - Encryption session user authentication failure

This message is shown when the user authentication for the encryption clients is active and indicates that an user registered in an authenticator tried to establish a secure channel with the firewall, however, his password was incorrect. The complementary messages show the username and the addresses of the source and destination hosts (the destination is the IP address of the host behind the firewall which the client tried to communicate with).

121 - User unregistered for encryption session

This message is shown when the user authentication for the encryption clients is active and indicates that an user not registered in an authenticator tried to establish a secure channel with the firewall. The complementary message shows the username and the addresses of the source and destination hosts (the destination is the IP address of the host behind the firewall which the client tried to communicate with).

122 - Encryption session with client established

This message is generated by the certificates server when a user is authenticated correctly in an encryption client and a secure channel is established. The complementary messages show the username and the addresses of the source and destination hosts (the destination is the IP address of the host behind the firewall which the client tried to communicate with).

123 - Encryption session with client finished

This message indicates that a client closed a secure channel. The complementary message indicates the source address of the session.

124 - Encryption client communication error

This message, which has several causes, indicates that the encryption server received an invalid encrypted packet from an Aker Encryption Client.

The complementary messages indicate the cause of the problem and the addresses of the source and destination hosts (the destination is the IP address of the host behind the firewall which the client tried to communicate with).

125 - Error when loading encryption algorithm

Aker Firewall can work with encryption algorithms developed by third parties, called external algorithms. This message indicates that the encryption server was unable to load one of these external encryption algoritms. This is caused by a failure in the algorithm implementation.

The complementary messages show the name of library from which the firewall tried to load the algorithm and the error that caused the problem.

Solution: Contact the algorithm developer and pass the complete message to him.

126 - User's profile session authentication failure

This message indicates that a user entered an invalid password, when trying to logon in the firewall using Aker Authentication Client. The complementary messages indicate the user name and the source host of the request.

127 - User unregistered for user's profile session

This message indicates that an user not registered tried to logon in the firewall using Aker Authentication Client. The complementary message shows the addresses of the source host.

128 - User's profile session established

This message indicates that a user successfully logged in the firewall using Aker Authentication Client. The complementary messages indicate the name of the user who established the session and the host from which the session was established.

129 - User's profile session finished

This message indicates that a user finished a session in the firewall established through the Aker Authentication Client. The complementary messages indicate the name of the user who finished the session and the host from which the session was closed.

130 - Invalid user's profile request

This message, which has several causes, indicates that the firewall user login server received an invalid request from an Aker Authentication Client.

The complementary messages indicate the cause of the problem and the source address of the request.

131 -Error when loading pseudo-groups

This message indicates that the firewall was unable to load the certification authorities pseudo-groups list.

Solution: Contact the technical support

132 - Error when downloading CRL

This message indicates that the firewall was unable to download the revoked certificates list (CRL) from a certification authority. The complementary messages indicate the reason of the failure and the URL that was tried to download the CRL.

Solution: Make sure the URL informed in the certification authority entity is correct and that the service is running. It is possible to check this by typing the URL in a browser and checking if it is possible to download the file.

133 - The number of processes in the system is too high

This message indicates that any external firewall module, when trying to create a new instance of itself to deal with a connection, detected that the number of processes running in the system is close to the maximum allowed limit. Because of this, the creation of the new process was canceled and the connection that should be treated by the new process was aborted.

Solution: Increase the maximum number of processes in the system. For further information, contact the technical support.

134 - 1-N translation host down

This message indicates that one of the hosts participating of a 1-N translation (load balancing) is down. The complementary message shows the IP address of that host.

135 - 1-N translation host up

This message indicates that one of the hosts participating of a 1-N translation (load balancing) that was down is now up. The complementary message shows the IP address of that host.

136 - Administrative session request

This message is generated by the Aker Firewall remote administration module every time it receives an administrative connection request. In the complementary message the IP address of the host that requested the connection is shown.

137 - Administrative session established

This message is generated by the Aker Firewall remote administration module when a user is authenticated correctly and an administrative session is established. In the complementary message the login of the user that established the session and his rights are shown.

The user rights are represented by three different anagrams. If the user has a specific right, the corresponding anagram will be shown, otherwise, the value "--" will be shown instead. The anagrams and their meanings are:

- **CF** - Configures Firewall
- **CL** - Configures Log
- **MU** - Manage Users

138 - Administrative session closed

This message indicates that the administrative session that was established was ended on a user's request .

139 - Administrator not registered

This message indicates that a user not registered in the system tried to establish an administrative section.

140 - Administrative session confirmation error

This message indicates that a user registered in the system tried to establish a remote administrative session, but his password was wrong. The complementary message shows the name of the this user.

141 - Firewall is being administrated by another user

This message indicates that a user was authenticated correctly to establish a remote administration session, but there was another user with an opened section for the same host and therefore the connection was refused. The complementary message indicates which user had his session refused.

142 - Parameter modification

This message indicates that the administrator, who was with the administrative session active, changed a configuration parameter of the system. The complementary message indicates the name of the changed parameter.

143 - Filtering rules modification

This message indicates that the administrator, who was with the administration session active, changed the filtering rules table of the firewall.

144 - Address translation modification

This message indicates that the administrator, who was with the administrative session active, changed a network address translation parameter or the server translation table. The complementary message indicates exactly what was changed.

145 - Secure channels modification

This message indicates that the administrator, who was with the administrative session active, changed the secure channels table of the firewall.

146 - SYN Flood configuration modification

This message indicates that the administrator, who was with the administrative session active, changed a parameter of the SYN Flood protection. The complementary message indicates exactly what was changed.

147 - Contexts modification

This message indicates that the administrator, who was with the administrative session active, changed the contexts of one of the transparent firewall proxies. The complementary message indicates which proxy had its contexts changed.

148 - SNMP configuration modification

This message indicates that the administrator, who was with the administrative session active, changed the configuration parameters of the SNMP agent.

149 - Access profiles modification

This message indicates that the administrator, who was with the administrative session active, changed the access profiles list.

150 - Access control list modification

This message indicates that the administrator, who was with the administrative session active, changed the access control list.

151 - Authentication parameters modification

This message indicates that the administrator, who was with the administrative session active, changed the global authentication parameters.

152 - Entities modification

This message indicates that the administrator, who was with the administrative session active, changed the entities list of the system.

153 - WWW parameters modification

This message indicates that the administrator, who was with the administrative session active, changed the WWW parameters.

154 - SOCKS proxy configuration modification

This message indicates that the administrator, who was with the administrative session active, changed any of the SOCKS proxy configuration parameters.

155 - Active connection removal

This message indicates that the administrator, who was with the administrative session active, removed one of the active connections The complementary message indicates if the removed connection was TCP or UDP.

156 - Active user session removal

This message indicates that the administrator, who was with the administrative session active, removed one of the user sessions that was established through the Aker Authentication Client.

157 - Operation on the log file

This message indicates that the administrator, who was with the administrative session active, performed an operation on the log file. The possible operations are *Compact* and *Clear*. The complementary message indicates which one these operations was performed.

158 - Operation on the events file

This message indicates that the administrator, who was with the administrative session active, performed an operation on the events file. The possible operations are *Compact* and *Clear*. The complementary message indicates which one these operations was performed.

159 - Operation on the users file

This message indicates that the administrator, who was with the administrative session active, performed an operation on the events file. The possible operations are *Add*, *Delete* and *Change*. The complementary message indicates which one of these operations was performed and on which user.

160 - Firewall date/time modification

This message indicates that the administrator, who was with the administrative session active, modified the date and/or time of the firewall.

161 - Local negotiation certificate loaded

This message indicates that the administrator, who was with the administrative session active, loaded or changed the firewall local negotiation certificate.

162 - Certificates modification

This message indicates that the administrator, who was with the administrative session active modified the certification authorities certificates or revocation certificates lists.

163 - TCP/IP configuration modification

This message indicates that the administrator, who was with the administrative session active modified the TCP/IP firewall configuration (hostname, DNS configuration, interface configuration or routes).

164 - Administrative session dropped by error

This message indicates that the administration session that was active, was interrupted due to a protocol communication error.

Solution: Try to establish the connection again. If the problem persists, consult the technical support.

165 - Administrative session dropped by timeout

When a remote interface establishes an administrative connection, it starts to send packets to the firewall, periodically, indicating that it is active. These packets are sent even if the user does not perform any operation.

This message indicates that the administrative session that was active, was interrupted because server did not receive any packet from the remote interface within the maximum allowed time. The most probable causes are a crash on the host that was running the graphic user interface or a network failure.

166 - Error in the previous operation

This message indicates that the last operation performed by the remote communication server was not successfully completed.

Solution: Verify if there is free space in the filesystem '/' of the firewall. This can be done through the command **`"$df -k"`**. If this command shows the directory '/' with 100% of used space, then this is the cause of the problem. If there is free space and this error still appears, consult the technical support.

167 - User without access right

This message indicates that the user tried to perform an unauthorized operation.

Solution: This message probably will never appear under normal conditions of Aker Firewall functioning. If it appears, contact the technical support.

168 - Unrecognized packet

This message indicates that the firewall communication server received an unknown service request.

Solution: Contact the technical support.

169 - Too many negotiations in progress

170 - Non-IPSEC SA

171 - Specified cryptographic algorithm not implemented

172 - Cryptographic key expansion failed

173 - Kernel sent an invalid packet

174 - Failed to insert SA in kernel

175 - Establishing IPSEC VPN for the traffic

176 - failure initializing fwiked

177 - Error processing configuration

178 - Kernel communication failure

179 - Kernel sent a bad request

180 - Attempt to install a non-negotiated SA

181 - Cryptographic algorithm not supported

182 - Error sending ike rule to the packet filter

183 - SA activation succesfull

184 - IKE negotiation failed (see complementary messages)

185 - Error reading state change notification from cluster

186 - Error sending state change notification to cluster

187 - fwiked notification (see complementary messages)

188 - fwiked warning (see complementary messages)

189 - receiving pipe number from kernel

190 - Error reading statistics configuration file

191 - Error loading entity table

192 - Counter entity not found

193 - Daemon suspended: bad configuration

194 - Error receiving statistics from kernel

195 - Error saving statistics

196 - Error receiving statistics lifetime

197 - Requested flow not found

198 - Requested pipe not found

199 - Erasing log system registers

200 - Error loading shell

201 - Error loading license information

202 - Login attempt (console) failed due to bad password

203 - Severe system problem. Contact your reseller

204 - Console login successfull

205 - Response line too big

206 - Error receiving data from POP3 server

207 - Error receiving data from POP3 client

208 - Error sending data to POP3 client

209 - Error sending data to POP3 server

210 - Invalid answer from POP3 server

211 - Error connecting to POP3 server

212 - Connection refused by POP3 server

213 - Invalid POP3 command or sintax error

214 - Error openning spool file

215 - Error writing to file

216 - Out of space writing to file

217 - Sintax error parsing POP3 email message

218 - Entering STLS mode - no further analysis possible

219 - Error receiving data from server firewall

220 - Error sending data from server firewall

221 - Server firewall processing error

222 - Error updating firewall configuration

223 - Error when cloning cluster's state

224 - Error when sending file to cluster

225 - Error when grouping data from cluster

226 - Virus-infected file cleaned

227 - Virus-infected file blocked

228 - Corrupted file could not be analysed

229 - Encrytped file could not be analysed

230 - Host answered and was marked as up

231 - Host did not answer and was marked as down

232 - Link was marked as up

233 - Link was marked as down

Appendix B - Questions and Answers

Stateful Filter

I'm trying to perform a file transfer using FTP from the host where the firewall is installed. I'm able to connect and be validated by the rInote FTP server, however when I try to transfer a file I receive a message saying it was not possible to open the data connection. How can I solve this problIn ?

The only way to perform a file transfer using FTP from the firewall is by using the passive mode. To do this, just type the command **`passive`** in the FTP command line, after being validated by the rInote server. From this moment on, all file transfers will be successfully completed.

All browsers already use the passive mode for all FTP file transfers.

Remote administration

I am using the remote administration through the Internet. Is there any risk of having my password intercepted?

No. A user's password will never be sent unencrypted through the network. The authentication method is based on a challenge-response, where the firewall is able to authenticate the user without receiving his password and the rInote interface is able to authenticate the firewall.

I've lost the password of the only administrator that was registered in the system. Is there any way to recover it?

There is no available way to recover a lost password, however, it is possible to use a local module of the users administration and create another administrator or change the password of the existing administrator to a known password. The local module can only be run by the root user, and have the following name: **`/etc/firewall/fwadmin`**

Encryption

I'm configuring a secure channel betweeen two Aker Firewalls, one with version 3.01 and other with 3.10 or 3.50. I've configured SKIP key exchange and put the same shared secret in both firewalls, however I receive the *Packet has failed authentication* message everytime I try to make the two firewalls communicate. What is wrong ?

The version 3.10 of Aker Firewall has suffered modifications in some points of the SKIP algorithm, caused due to compatibility problIns with other operating systIns, and thus became incompatible with the previous versions.

The solution to this problIn is to update all versions before 3.10 to 3.10 or superior (which are totally compatible)

SNMP

I realized that when I administrate Aker Firewall running on Linux Platform, the SNMP read and write communities, in the configuration parameters window, are disabled. What does it happen ?

The Linux operating systIn already comes with a pre-installed SNMP agent. Because of that, we chose not to install Aker Firewall SNMP agent.

To learn how to set up Linux SNMP agente read and write communities, please refer to its documentation.

Other services

How to configure MS Exchange servers to operate through Aker Firewall ?

To allow the correct operation of Exchange Servers through firewalls it is necessary to force the use of specific ports that will be used by those servers. In order to do that, it is necessary to include the following keys in the registry of the servers (all keys are case-sensitive):

In
`HKLM\SYSTIn\CurrentControlSet\Services\MSExchangInTA\Parameters`
Add **DWORD TCP/IP port for RPC listens** with the port to be used (for example, 30001).

In
`HKLM\SYSTIn\CurrentControlSet\Services\MSExchangeSA\Parameters`
Add **DWORD TCP/IP port** with the port to be used (for example, 30002).

In
`HKLM\SYSTIn\CurrentControlSet\Services\MSExchangeDS\Parameters`
Add **DWORD TCP/IP port** with the port to be used (for example, 30003).

In
`HKLM\SYSTIn\CurrentControlSet\Services\MSExchangeIS\ParametersystIn`
Add **DWORD TCP/IP port** with the port to be used (for example, 30004).

Obs1: After the modifications above it is necessary to restart the Exchange servers.
Obs2: In case the Exchange version is 5.5, it is necessary to apply Service Pack 2 or superior so this can work

Aker Firewall Configuration for the above example:

1. Register entities for the above services (30001, 30002, 30003 and 30004)
2. Create a rule allowing access to the above services and to Windows RPC (135/TCP).
3. If you are using LDAP, it is also necessary to add service 389/TCP

Appendix C - Copyrights e Disclaimers

In this appendix the disclaimers of the libraries and third party source codes used in Aker Firewall are listed. These disclaimers apply only to the explicit mentioned parts and not to Aker Firewall as a whole. They are mentioned here due to requirements of the developers:

DES Library

This library and applications are FREE FOR COMMERCIAL AND NON-COMMERCIAL USE as long as the following conditions are aheared to.

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this code is used in a product, Eric Young should be given attribution as the author of the parts used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentations and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
This product includes software developed by Eric Young (eay@mincom.oz.au)

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA,
OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

libcrypto Encryption Library

This package is an SSL implementation written
by Eric Young (eay@cryptsoft.com).
The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as
the following conditions are aheared to. The following conditions
apply to all code found in this distribution, be it the RC4, RSA,
lhash, DES, etc., code; not just the SSL code. The SSL documentation
included with this distribution is covered by the same copyright terms
except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in
the code are not to be removed.
If this package is used in a product, Eric Young should be given attribution
as the author of the parts of the library used.
This can be in the form of a textual message at program startup or
in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:
1. Redistributions of source code must retain the copyright
notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright
notice, this list of conditions and the following disclaimer in the
documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software
must display the following acknowledgement:
"This product includes cryptographic software written by
Eric Young (eay@cryptsoft.com)"
The word 'cryptographic' can be left out if the rouines from the library
being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from
the apps directory (application code) you must include an acknowledgement:
"This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND
ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE
IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE

ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE
FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL
DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS
OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION)
HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT
LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY
OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF
SUCH DAMAGE.

The licence and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution licence
[including the GNU Public Licence.]

SNMP Library

Copyright 199 by Carnegie Mellon University
All Rights Reserved
Permission to use, copy, modify, and distribute this software and its documentation for any purpose and without fee is hereby granted, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation, and that the name of CMU not be used in advertising or publicity pertaining to distribution of the software without specific, written prior permission.

CMU DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE, INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS, IN NO EVENT SHALL CMU BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTUOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

FreeBSD source codes

Copyright (c) 1982, 1986, 1993
The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:
1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS``AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

MD5 Algorithm

Copyright (C) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

These notices must be retained in any copies of any part of this documentation and/or software.

SNMP Agent

Copyright (c) 1996,1997 Wes Hardaker and the University of California at Davis

COPYRIGHT

Many portions of the code in this package were distributed by Carnegie Mellon University. All other code and changes to the original code written by Wes Hardaker at the University of California at Davis is copyrighted under the following copyright:

Permission is granted to use, copy, modify and distribute this software and documentation. This software is distributed freely and usage of it is not subject to fees of any kind. It may be included in a software compact disk set provided that the author is contacted and made aware of its distribution.

LInteger math library

LInteger Version 0.2 Source Code and Documentation

Copyright (C) 1996 by Leonard Janke

This source code and documentation may be used without charge for both commercial and non-commercial use. Modification of the source code or documentation is allowed provided any derivate work is clearly indentified as such and all copyright notices are retained unmodified. Redistribution of the source code or documentation is unlimited, except by the limits already mentioned, provided that the redistribution is not for profit. Those wishing to redistribute this source code or documentation or any work derived from either for profit must contact Leonard Janke (janke@unixg.ubc.ca) to work out an acceptable arrangement.

Anyone who wishes to distribute a program statically linked against the functions provided may do so providing that he or she includes a copy of this note with the program.

Distribution of libraries compiled from this source code is unlimited if the distribution is not for profit and this copyright notice is included. Those wishing to distribute libraries compiled from this source code or any work derived from it for profit must contact Leonard Janke (janke@unixg.ubc.ca) to work out an acceptable arrangement.

Anyone using this source code or documentation or any work derived from it, including, but not limited to, libraries and statically linked executables, must do so at his or her own risk, and with understanding that Leonard Janke will not be held responsible for any damages or losses that may result.

Appendix D - What's new in version 5.0

In this appendix are listed all modifications and new features of version 5.0, when compared to version 4.5. They are:

- New multiplatform GUI, written from scratch;
- Possibility of administration of several firewalls simultaneously through the same interface;
- Cooperative cluster, with the possibility of using up to 64 firewalls in parallel, splitting the traffic among them. In this king of cluster, there is no connection loss, even when one or more of the participating firewalls goes down;
- Link balancing, allowing the simultaneous use of several links from different or not ISPs;
- SMTP proxy with added features;
- Virus scanning and removal in HTTP and FTP downloads;
- Enhanced anti-spoofing control;
- Support to 802.1q protocol;
- Support to RADIUS and LDAP protocols to perform user authentication;
- Grouping of filtering rules in policies;
- Hierarchy of access profiles;
- Anti-suicidal protection mechanism;
- Visualizations of CPU and memory use statistics of the host the firewalls is running through the GUI, on real- time;
- Anti-flood control, limiting the maximum number of simultaneous connections from a given host to a specific service/server