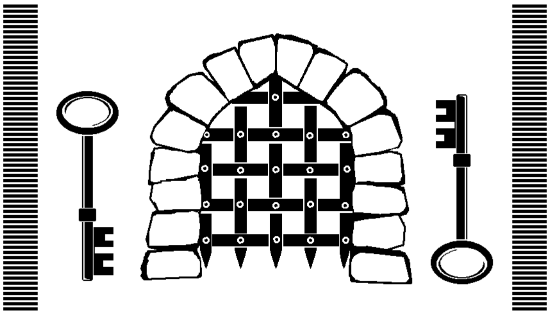
LuciGate
User Guide



Lucidata House
Selwyn Close
Great Shelford
CAMBRIDGE CB2 5HA
England

tel: +44(0)1223 846100
fax: +44(0)1223 846100
email docs@lucidata.co.uk

Publication Details

Publication Details

All possible care has been taken in the preparation of this publication, but Lucidata accepts no liability for any inaccuracies that may be found.

Lucidata reserves the right to make changes without notice to both this publication and to the product which it describes.

If you find any errors in this publication or would like to make suggestions for improvement, please write/fax or email the Company at the address below.

Lucidata House
Selwyn Close
Great Shelford
CAMBRIDGE
CB2 5HA
England

tel: +44(0)1223 846100
fax: +44(0)1223 846100
email: docs@lucidata.com

Publication number LuciGate Issue number 3 (First Issue 7/96)

Revision Details

Issue	First Published	Revised	Pages
4	06/00	11/01	2,3,8,10,12-15,17-19 Appendix (pp 23-33)
		04/06	2,13,25,26,34

FM 13348 BS EN ISO 9001:1994

All Lucidata products are designed, developed and tested under the control of its ISO9000 compliant Quality Management System. The high quality of our products is thus assured. Should any issues on the quality of our products arise please address them to the Quality Manager via any of the addresses given on page 2. This User Guide contains all the necessary information for the proper installation and configuration of the product to ensure the highest level of performance.

Warranty

Lucidata warrants that the products described in this User Guide are free from defects in manufacture and that they meet the specifications and functionality described in this User Guide. Lucidata will replace parts and repair defects in manufacture, on a return to factory basis, for a period of 12 months from the date of our original invoice provided that the product has only been used in the manner and for the purpose described in this User Guide. Lucidata does not warrant that the products described in this User Guide are suitable for any specific application and the purchaser must be satisfied of the suitability of the product for the intended application as best known to the purchaser. Lucidata does not accept any contingent liability for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages arising from the use of its equipment. Lucidata assumes that if its equipment is used in a business critical or any other essential application, then the system design should incorporate sufficient resilience to ensure that a single failure would not have disproportionate consequences.

Service and Support

If a unit fails, and you have bought it from a Lucidata appointed dealer, you should contact that dealer. If bought from the manufacturer, return the unit in its original packing to the address on page ii.

You should telephone or fax Lucidata prior to returning the unit to ascertain whether an apparent fault is due to mis-operation rather than to a technical fault within the unit and to obtain a returns number.

Lucidata reserves the right to charge for any investigation of an apparent fault that is found to be due to incorrect operation, or for the repair of a fault that is due to the unit not being used in accordance with the instructions in this User Guide.

Maintenance

Faults that occur outside the warranty period and are not covered by a separate maintenance contract, will be repaired on a time-and-materials basis. Please telephone Lucidata prior to returning your unit. You will be given an estimate of the repair costs.

Service and Support

Should a Lucidata product appear to fail you should, in the first instance, contact your supplier who will be able to advise you and possibly solve your problem. If you contact Lucidata you should have the product description, serial number, date and place of purchase at hand so that we can efficiently identify your unit. If after assistance from our technical staff it appears that there is a failure you will be given a Returns Number to mark the package returned to the Lucidata factory. Units will be repaired free of charge if they are within warranty. Outside the warranty period repairs will be charged at Lucidata's normal rates. You will be given an estimate of the repair cost prior to work commencement.

Lucidata reserves the right to charge for any investigation it undertakes if the apparent fault is due to improper operation of the unit, or if the unit has been damaged by usage outside the scope of this User Guide.

Additional In-Warranty services may be available in some countries. Contact your local dealer who will be able to advise you.

Post Warranty

The arrangements for Post Warranty servicing vary from country to country. Your local dealer will be able to advise you as to whether you can take out a Post Warranty Maintenance Contract.

Safety

WARNING

This product is for indoor use only.
This equipment must be earthed.
This equipment must NOT be operated with the lid removed as dangerous voltages exist inside.

Contents

Introduction

For those readers wishing to get started straight away and who are not interested in a philosophical discussion you may proceed to the *Installation Section* directly.

IT Security (ITSEC) is a complex and wide ranging subject which allows plenty of scope for misunderstanding. The functional richness of the Internet, World Wide Web and popular Application Software has opened up an increasing number of holes in the security integrity of these systems. These weaknesses can be and are exploited by individuals to compromise organisations that have become ever increasingly reliant upon their IT systems. There is not and never will be a single simple solution in a box to neutralise all the possible malicious attacks that can be designed to subvert the legitimate use of IT technology. The purpose of this brief introduction is to clearly define what Firewalls are and what they can reasonably be expected to do.

Firewalls in General

The word firewall is used increasingly to define a function which is quite often added to some other device or system which in itself is not a firewall. Routers and some operating systems offer firewall features. A firewall can be a simple device, directly analogous to the physical barrier designed to delay the spread of a fire from one building area to another, or it can be a complex structure of cooperating devices which together provide the required degree of logical and physical separation between a trusted network segment and an untrusted network segment.

Different terminologies are used to describe these networks by different authors. We use the term Inner World Network to describe the trusted network segment. Other descriptions include: Local Network, Protected Network, Private Network. Entities on the Inner World Network are called Inner World Hosts. Similarly the untrusted network segment, from where we think an attack on our trusted network segment might originate, is called the Outer World Network. Other descriptions include: External Network, Alien Network, Hostile Network, Public Network. Traffic going from the Inner World to the Outer World is called Outbound Traffic and traffic going from the Outer World to the Inner World is called Inbound Traffic.

The primary purpose of a firewall is to apply rules to the traffic flowing in both directions and either allow it to pass or not. Secondary functions may include Network Address Translation (NAT) and detecting and reporting Alarm conditions. When a firewall is not functioning it should behave as an Air Gap and not allow any traffic to pass in either direction. Commercial firewalls frequently place limits on the number of simultaneous users by imposing a license agreement.

The Lucigate Firewall

The Lucigate Firewall is a simple box that is a pure firewall appliance. It can be used with other devices to create more complicated firewall structures if so desired and it does not prevent the use of other end-to-end security technologies such as Virtual Private Network (VPN). The Lucigate Firewall does not impose any restriction on the number of simultaneous users. It forms the very first barrier between the Outer World and the Inner World and as such takes the full force of any attack.

The Lucigate Firewall will not fall over if attacked but will stop passing potentially damaging traffic into the Inner World until normality is restored. If it needs to restart it will do so in less than two seconds which is virtually instantaneous when compared to the boot time of a General Purpose Computer (GPC) It can perform Network Address Translation (NAT) both at the subnet level and on an individual host basis.

One of the big differences between firewalls for computer networks and firewalls that really are walls built to resist fires, is that the users want computer firewalls to do many different things, sometimes, all at the same time. This leads to problems of mutually exclusive actions in which either no traffic gets through the firewall or unintended traffic leaks through. The first version of the LuciGate Firewall was designed to be very symmetric and operated with very simple blanket rules that were relatively unambiguous. The penalty for such apparent simplicity was the tortuous design of rules to allow for ever increasing user requirements and the need to add custom one shot rules such as let DNS use UDP but nobody else. Analysis of user requirements led us to the conclusion that the functionality required was to enable the firewall to protect both a network of Clients from outside attack and to allow Servers on the same network to service requests from outside. Control of Peer to Peer custom access was also required.

A unique feature of the Lucigate Firewall is that it is controlled by a smartcard that we call the Key. Like a padlock the Lucigate will not be open to any traffic if there is no Key present. The rules are written on the Key using a program running on a standard PC. There is no way of controlling the Lucigate from the network so there is no way to compromise it from the network. For this reason the bulk of this manual is devoted to the programming of the Key as the Lucigate Firewall itself has very few characteristics.

Installation

The installation of the Lucigate Firewall is very straightforward as there are no hardware options to select.

The switched mode power supply is of the universal input type and accepts mains power of 110VAC 60Hz or 230VAC 50Hz.

The input circuitry autosenses whether connection has been made to the 10Base2 or 10BaseT network sockets.

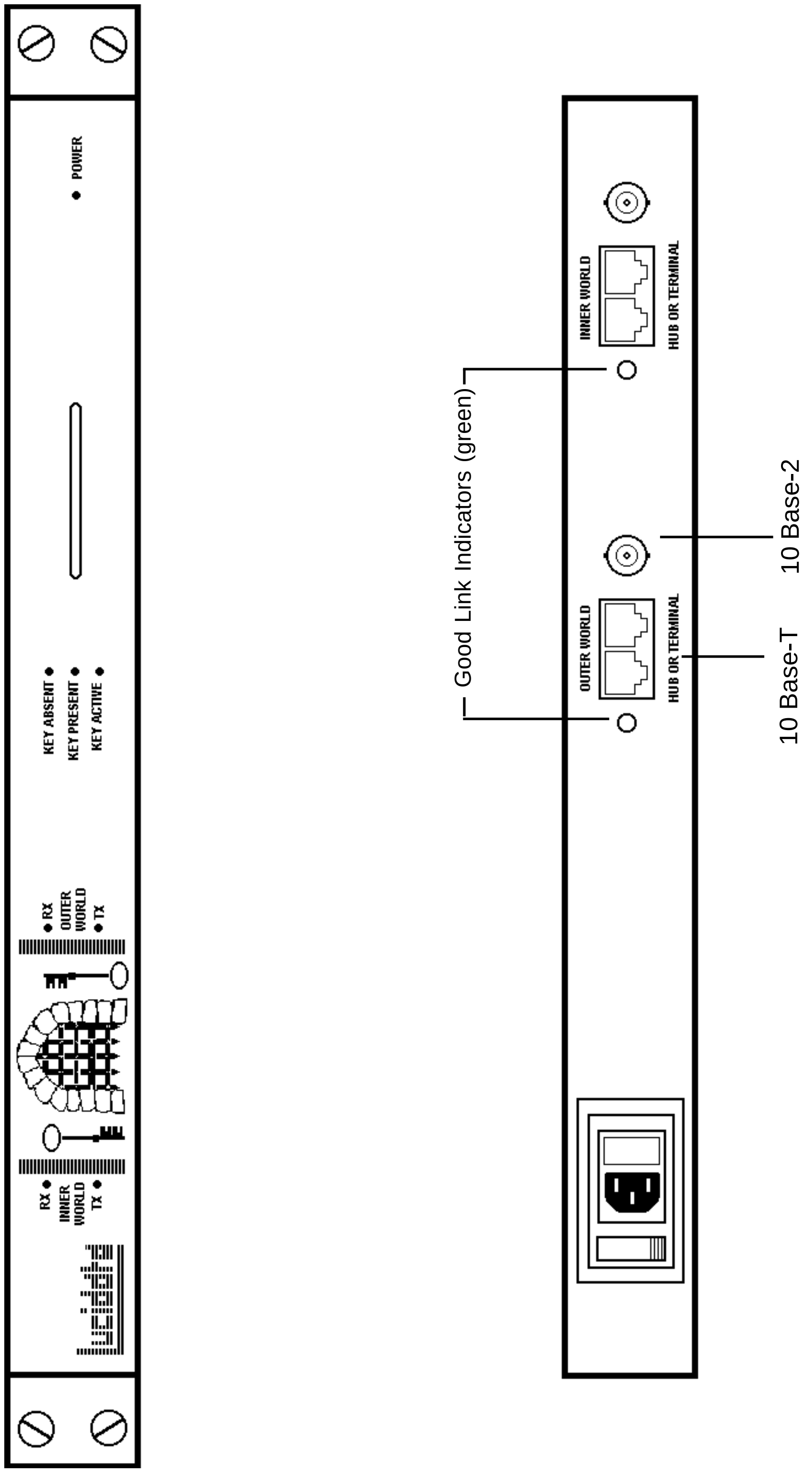
The user has to decide whether to operate the Lucigate free standing on a horizontal surface using the default rubber feet or fix the rack mounting ears provided with the eight M5 screws and secure it to a 19” rack.

For convenience and to avoid the need to have cross-over cables, there are two 10BaseT RJ45 jacks for the Inner World and two for the Outer World. Each pair has one jack wired to connect directly to a hub and the other wired to connect directly to a network card on a terminal or router. Which is which is shown in the diagram on the product identification label at the rear of the unit. Connection must only be made to one jack of each pair or the 10Base2 plug on each side. If the 10BaseT cables have been correctly installed the green LEDs adjacent to the RJ45 jacks will be illuminated. The location of the various connections are shown in Fig. 1.

A common configuration is where the Lucigate Firewall is connected between the Access Router to the Internet or other external network and a Hub on the internal network. In this case the Hub is connected to the RJ45 connector nearest the Green LED on the Inner World set of connectors at the back of the Lucigate. The Router is connected to the RJ45 connector nearest to the BNC plug on the Outer World set of connectors.

Care should be taken when connecting the LuciGate to the network via a switch and subsequently removing the direct connection to the Access Router. The switch may insist on passing traffic to the Access Router on the port it was previously connected to rather than through the port that the LuciGate is connected to. This problem can usually be overcome by re-setting the switch so that it has to re-discover where things are.

Also ensure that any devices that are connected to the LuciGate operate at 10Mbps half duplex.


POWER
KEY ABSENT
KEY PRESENT
KEY ACTIVE
RX
OUTER WORLD
TX
RX
INNER WORLD
TX
INNER WORLD
HUB OR TERMINAL
OUTER WORLD
HUB OR TERMINAL
Good Link Indicators (green)
10 Base-2
10 Base-T

Case	Welded Mild Steel
Dimensions	400mm x 230mm x 45mm
Weight	3Kg
Power Connector	IEC Switched, 3 pin connector fused with 20mm 2A (T) HBC fuse.
Power Input	85-264V AC, 47-440Hz, 10 Watts
Safety Approvals	PSU Approved to UL 1950, CSA 22.2 No 234 and EN 60950.
Network Connections	10Base-2 coaxial Plug and two 10Base-T RJ45 jacks per side. One RJ45 wired for direct Hub connection and one wired for direct Terminal connection each side. 10 Mbps half duplex only.
Throughput	Sustained agregate 2Mbps
Indicators	One green LED at rear for each side showing a good 10Base-T link. Two Yellow LEDs on front panel for each side showing Transmitted and Received packets. One Red, one Yellow and one Green LED to show status of unit. One Red power on indicator.
Internal controls	One bank of DIL switches to select low level options at factory only
Smart Card Reader	Supports cards conforming to ISO7816-1/2/3
Mountings	Free standing unit with rubber feet supplied with two mounting brackets and screws for standard 19" rack. Optional extended brackets and Anti-Tamper front panel and screws for standard 19" rack.
Key Management	Filters constructed and programmed onto smartcard key using off-line KeyCutter program running on a PC.
Monitoring	LuciGuard program running on a networked PC.
Design, Manufacture and Test	LuciGate was designed, manufactured and tested in the UK by Lucidata under the control of our ISO9000 accredited Quality Assurance System and was designed to meet the assessment criteria of ITSEC level E3 for a security product.
Smart Mouse	General Information Systems Model SM1
Power Adaptor for Smart Mouse	Supplies 8-12 Volts DC @ 20mA on a female coax plug 1.45mm inner 3.5mm outer diameter with centre negative.

The Smartcard Key

The Lucigate Firewall will not operate without a valid Smartcard key being present. The supplied key has been programmed to allow all ARP transactions for IP to pass and most ICMP traffic. If the supplied Smartcard key is inserted in the slot, you will be able to Ping from the Inner World to the Outer World but not from Outer to Inner.

Note: The correct orientation is with the Gold Contact Area facing upwards and inserted first.

LED Indicators

The Red LED labelled Power indicates when the unit is powered up as might be expected.

There are four Yellow LEDs which show the traffic levels on the Inner and Outer World networks. There are a pair labelled RX and TX for each side. Each time a packet is received (RX) or transmitted (TX) the appropriate LED flashes for 50mS. Under low level traffic conditions it is easy to see those packets that get through and those that do not. Every packet that gets through results in the RX LED on one side and the TX LED on the other side apparently flashing simultaneously.

The Red, Yellow and Green LEDs show the status of the LuciGate and each LED can have three states - On, Off, or Flashing. The following table gives the meaning of the combinations.

Red	Yellow	Green	Meaning of combination
Off	Off	On	Normal Operation
Off	Off	Off	If power on LED is also off, mains fuse or power failure.
Off	Off	Off	Unit not running.
On	Off	Off	Key absent - Traffic detected but all blocked
Off	On	Off	Valid Key but no valid rules defined
Flashing	Flashing	Flashing	Memory Test failure
On	On	On	Unit stopped; unable to initialize clock.
Off	On	On	Unable to initialize card reader
On	Off	On	Unable to initialize Inner World interface.
On	On	Off	Unable to initialize Outer World Interface.
Off	Flashing	Off	Cannot Validate smartcard
On	Flashing	Off	Failure during read of smartcard
On	Off	Flashing	Pre-revision 3 card programmed
Off	On	Flashing	Lists inconsistant, missing set.
Flashing	Off	Off	Bad Card, cannot read it at all

Programming the Key

The Keycutter Program

The LuciGate KeyCutter program will run on any IBM compatible PC running a 32-bit MS Windows OS. The SmartCard Key is accessed via a "Smart Mouse" unit which is plugged into one of the PC's COM ports. Some PC's do not provide sufficient power on this port to enable reading and writing of the smartcard so a power adaptor can be plugged into the back of the "Smart Mouse" to provide this. If a power adaptor was not supplied with your unit, please refer to the Technical Specification before obtaining one locally.

Install the Keycutter program following the instructions on the supplied disks. You do not need to install Luciguard for the Keycutter to work. Connect the SmartMouse to a spare COM port. Execute the file LUCIG***.EXE. The first time you run the KeyCutter program select **Key/COM Port** and make sure the correct COM port is selected. This value will be saved in the LUCIGATE.INI file.

Select **File/Open Key File** and you should see EXAMPLE.KEY in the directory file list. Double click on EXAMPLE.KEY and you will notice the **Rules** and **Security ID** menu items are now enabled. Select **Rules** and you will see three rules displayed in the Ruleset List. Before proceeding you should update the relevant Mnemonic files to reflect the naming conventions of your organisation. This can be done using the **Edit** menu item on the main screen.

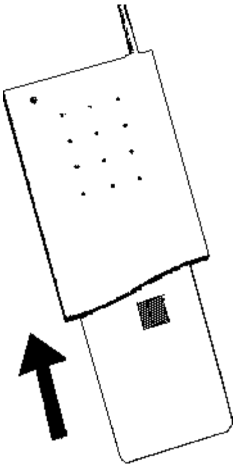


Figure 2

Insert the SmartCard Key into the "Smart Mouse" unit in the orientation shown in *Figure 2*, and proceed to program it for your requirements. The SmartCard Key can be re-programmed at least 10,000 times and will retain the information on it for a minimum of 10 years.

Note: *Avoid touching the contacts with your fingers and do not remove the card from the programming unit during the writing operation.*

***** reflects the revision number of the program e.g. LUCIG313.exe*

About Mnenomic Files

Human beings think best in natural language rather than in numbers so a major change has been to allow the user to name his own services rather than have to use numbers. Several files of mnemonics have been defined to allow the user to add his own definitions or to just include standard values which Lucidata has not included in the default sets. Currently there are seven mnemonic text files all beginning with the letters Mn and following the same simple syntax:

```
Mnemonic,Value in usual base,<Secondary value>,Descriptive text
```

Thus an entry of

```
IP,800,IP suite of protocols
```

in the MnTypes file defines the mnemonic IP to have a value 800 hexadecimal. Similarly

```
Telnet,23,,Telnet Terminal Protocol
```

defines the mnemonic Telnet to have value 23 decimal. If a private service was being offered on a range of port numbers the secondary value is used.

```
MyServices,100,200,MyServices available on ports 100-200
```

In the case of Hosts and Networks the secondary value represents the value that is to be substituted when performing Network Address Translation (NAT)

```
MyHost,1.1.1.1,2.2.2.2,MyHost is known as 2.2.2.2 externally
```

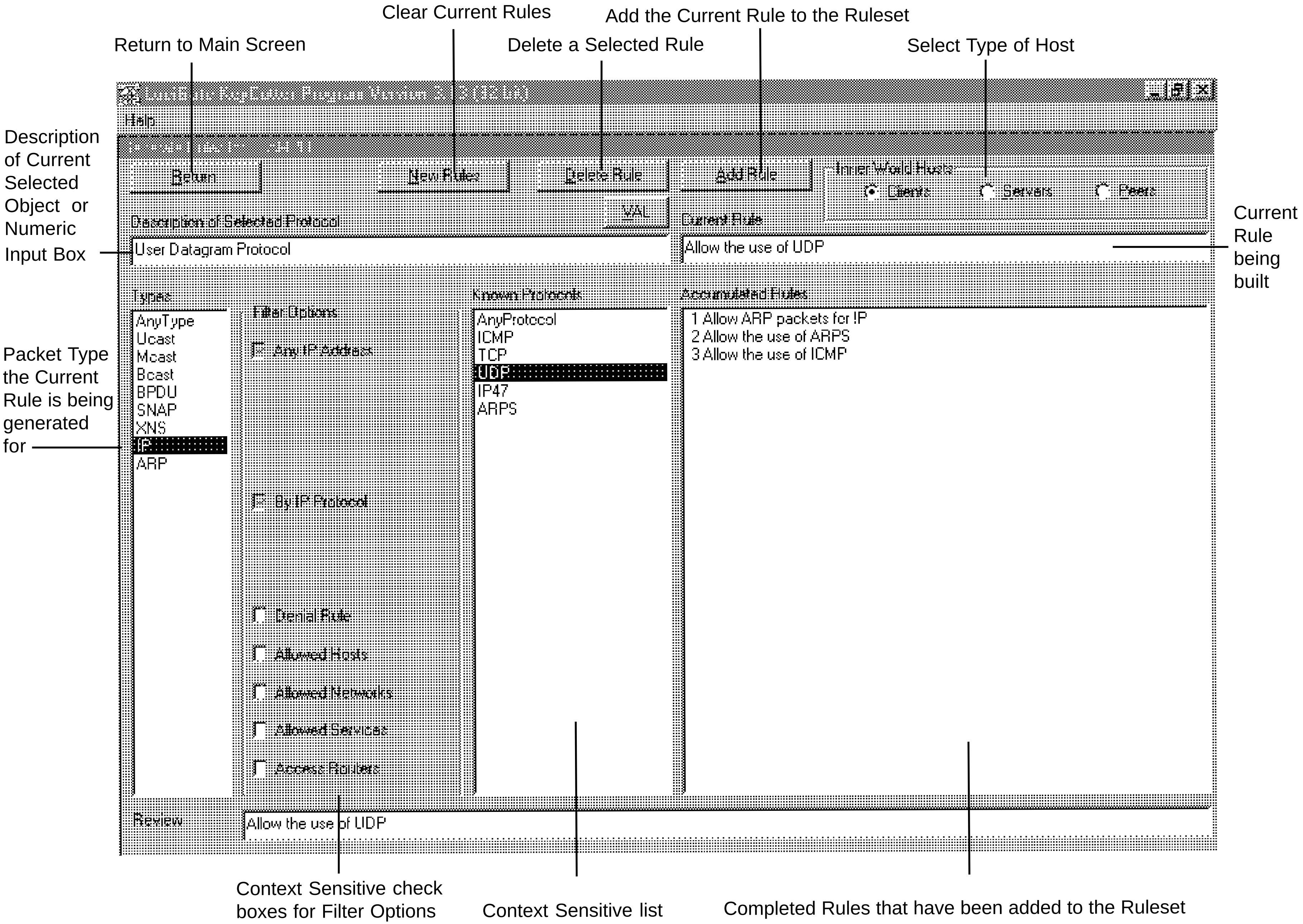
The descriptive text is displayed in a Text Box automatically when the item is selected thus providing a ready reminder and double check as to the identity of the item.

The seven files, which must be in the same directory as the KeyCutter program, are

MnMACS.txt	Define Hardware MAC Source addresses
MnMACD.txt	Define Hardware MAC Destination addresses
MnTypes.txt	Define the Ethernet packet types
MnHosts.txt	Define IP addresses of known hosts
MnNets.txt	Define Network addresses(and their masks)
MnProtocols.txt	Define the IP protocols used
MnPorts.txt	Define TCP/UDP Port numbers

Users must not remove the supplied default values in the MnMACS.txt, MnMACD.txt, MnTypes.txt, MnProtocols.txt and MnPorts.txt files as the KeyCutter program requires certain values to appear. Users own values can be added to them. The MnHosts and MnNets files can be completely changed.

Note: *Any line starting with a single quote mark is treated as a comment. A blank line will terminate a list.*


Return to Main Screen
Clear Current Rules
Delete a Selected Rule
Add the Current Rule to the Ruleset
Select Type of Host
Description of Current Selected Object or Numeric Input Box
Current Rule being built
Packet Type the Current Rule is being generated for
Context Sensitive check boxes for Filter Options
Context Sensitive list
Completed Rules that have been added to the Ruleset
Help
Return
New Rules
Delete Rule
Add Rule
VAL

Inner World Hosts: ● Clients ○ Servers ○ Peers

Description of Selected Protocol: User Datagram Protocol

Current Rule: Allow the use of UDP

Types:
- AnyType
- Ucast
- Mcast
- Bcast
- BPDU
- SNAP
- XNS
- IP
- ARP

Filter Options:
- ☑ Any IP Address
- ☑ By IP Protocol
- □ Denial Rule
- □ Allowed Hosts
- □ Allowed Networks
- □ Allowed Services
- □ Access Routers

Known Protocols:
- AnyProtocol
- ICMP
- TCP
- UDP
- IP47
- ARPS

Accumulated Rules:
1 Allow ARP packets for IP
2 Allow the use of ARPS
3 Allow the use of ICMP

Review: Allow the use of UDP

Generating Rules

To define a new Ruleset, select **File/New Key File** from the main menu and enter a meaningful Ruleset Name when prompted.

Selecting **Rules** from the main menu will bring up the Rules Generation Screen as shown in *Figure 3*. By default, nothing at all is allowed to pass through the Lucigate Firewall. Every traffic type has to be explicitly defined and associated with some network entity. These definitions can be extremely wide and let virtually everything through or they can be extremely narrow. The objective is flexibility. It should also be pointed out that the configuration of the LuciGate Firewall is now completely Inner World oriented as that is the entity being protected.

As discussed in the *Introduction*, three modes of potentially simultaneous operation are identified. We call them **Client Protection**, **Server Support** and **Peer to Peer**. Any given firewall configuration may operate in one or more of these modes at the same time but the programming is done one mode at a time.

Client, Server and Peer rules may be input in any order because the program sorts them before compiling them into the format used by the Lucigate Firewall.

Rules are executed with the following precedence within the Lucigate Firewall -

Peer Rules before **Server** Rules before **Client** Rules.
All overrides **Hosts** overrides **Networks**.

The human interface has been designed with the intention of letting the user make a choice, and then presenting him with the options available in that context. At all times the rule being built is displayed in the *Current Rule* text box. It is also copied to the full screen width *Review* text box. Some selections will result in an apparent truncation of options because the rule needs no more input.

When a dynamic list of items is presented, i.e. Hosts, selecting an item with a **single click** of the mouse is sufficient to enter the name into the current rule. If a **double click** is performed additional options may become visible in the Filter Options frame.

We have erred on the side of producing more simple rules than fewer complex ones. The decision to let the user drive the process is because of the ability of the human mind to come up with new and unexpected applications which could not, in our view, be properly supported by a Wizard asking dumb questions. It also allows full access to the inherent flexibility of the LuciGate Firewall. However, logical consistency checking is minimal so it is possible to make 'silly sets' that stop everything. Be particularly careful in mixing *Allowing* type rules and *Denying* type rules on a single Host. If you explicitly allow one thing everything else is automatically denied. Irrespective of which boxes or items you have selected, the *Current Rule* should say exactly what will happen in English. Rules already added to the Ruleset list may be reviewed at any time by selecting them with a single mouse click.

As a guide we suggest that for IP networks you start by allowing the ARP packet type and selecting ARP for IP. Then implement your security policy. As each new rule is built up you can add it to the list of rules making up the Ruleset you are creating at virtually any time. You do not have to go down to the finest detailed level if you do not want to. For example, you can stop at allowing the TCP protocol without specifying ports but it is more secure to do so.

Make sure everyone can use ARP and have access to the Router, provided you want to of course.

Some Points to Consider

Allowing ICMP packets by default does not allow Echo requests from the Outer World or any request for information on Routing or attempts to define routes. These defaults may be overwritten, if desired, by double clicking on ICMP when it is displayed in the protocol list and clicking the appropriate Filter Option. Enabling ICMP routing options also enables IP routing options.

If all the rules specify explicit Outer World Hosts or Networks then all local traffic between otherwise authorised hosts will automatically be prevented from "leaking out" into the Outer World. If the rules are more open, i.e. only limit remote access by protocol or service, then a rule like

```
    Deny LocalNet using Any IP Protocol to access Localnet
```

must be added to prevent inadvertantly qualifying some internal traffic. This rule is also important in protecting against the following attacks:

IP Masquerade attacks - where the attacker pretends to be a local host by using an IP address local to the Inner World.

Land Attack - where the source and destination IP addresses are the same and can cause confusion on less robust IP stacks.

Various other "popular" attack methods that the Lucigate automatically protects against are :

Ping of Death - where an ICMP Echo request is carried in an illegally large packet. Any illegal packet, by size or checksum, is automatically discarded.

Corruption of sub-net Masks - is prevented by default ICMP rules blocking relevent control packets.

Eavesdropping - by rerouting traffic via hostile site is prevented by default ICMP rules blocking relevent control messages.

SYN Floods - are moderated by an adaptive algorithm reducing their impact while not blocking any server.

The Client Mode

Most applications, like connecting a private network to the Internet, will only use this mode so the majority of the functionality of the KeyCutter program will be found here. Automatically such features as allowing TCP connections to be initiated from the Outer World are denied and there is no way to allow them, in this mode.

Note: If an Inner World Host wants to allow such connections it must define the details when Server Mode or Peer Mode is selected in the Rule Generator.

The main purpose of this mode is to define the properties of individual hosts or sub-nets and say what protocols and services you will allow them to access in the Outer World.

The Server Mode

Typically some private networks also host their own Web Sites or e-mail servers and want to allow the whole world access to these servers. This requires making holes in the barrier that was erected to protect the client population of the network from the dangers of the Outer World. In this mode each server can be precisely defined and the services it will offer to the Outer World carefully limited. Local users still have direct access unless a multi-firewall configuration is used with the creation of a Demilitarized Zone (DMZ). Server address translation can also be used to ‘remove’ the server from the local network as far as the Outer World is concerned.

The Peer Mode

This mode is used where there are specific external hosts that have special privileges to access certain resources on the local network. The hosts and the resources are literally identified on a one to one basis forming a ‘private’ communications channel. This mode is really just a highly restrictive combination of the other two modes but keeps the association separate from the more sweeping rules.

Routers

When connecting a private network to the Internet it is usual to have the access router on the Outer World side of the firewall. If the router lays in the same subnet as the clients of the local network there is no problem but if it is owned by an ISP for example it will have a registered address and IP translation will be necessary as the local clients will expect to find their default gateway on their own network. There are various options to get round these problems at various levels of the program.

Keyboard Shortcuts

Shortcuts other than those visible on captions are **Alt/T** to return to the **T**ypes list, **Alt/L** to return to the Pop-Up **L**ist if it is visible and **Alt/U** to move to the Accumulated R**U**les list. The twelve *Filter Option* checkboxes can be reached by **Alt/1,2,3,4,5,6,7,8,9,0,-** or **=**. The *Enter* key acts as a mouse double click when positioned in a Pop-Up list.

Security ID

The **Security ID** menu allows the user to assign an IP address, Security Port and Security String to the LuciGate itself. If IP type packets and the ICMP protocol are enabled, then ECHO requests (Pings) bearing the LuciGate IP address will get a standard echo response. This allows simple checking for the presence of the LuciGate, but only from the Inner World.

If the monitoring function (LuciGuard) is required, then a Security Port needs to be defined. An optional Security String can also be defined and act as a password for additional security or to differentiate between several LuciGate firewalls.

Saving the Ruleset

It is recommended to save the Ruleset to disk before writing to the smartcard.

Select **File** on the main screen and choose **Save Key File**. The default filename suggested will be the Ruleset name with a .KEY extension. If the suggested filename is changed the file is saved under that name and then the Ruleset name is reset to the root part of the filename.

Saving a Report

A copy of the text of the Ruleset can be saved to disk for subsequent printing or archival purposes. Select **File** on the main screen and choose **Save Report File as Text**. The default filename suggested will be the Ruleset name with a .TXT extension. If the suggested filename is changed the file is saved under that name but the Ruleset name is left unchanged.

Writing the Key

Select **Key** from the main screen and **Write Key** will invoke some prompts to ensure that the Smartcard Key is properly located in the Smart Mouse ready for programming. If errors are reported often it is probable that your PC does not have enough current drive capability on the COM port and you should use the auxiliary power adaptor supplied. When the Key has been successfully written the program automatically does a Save Key File with no prompts. This is because there is no textual information stored on the Key so that if a Key is Read into the KeyCutter the Key contents are interpreted with reference to the saved key file. It is therefore not a good idea to rename .KEY files once a Key has been programmed.

The LuciGuard Monitor Program

The LuciGuard program will run on any 32-bit MS Windows system that support Windows Sockets. All the files on the distribution disk can simply be copied to a convenient directory. It is a Windows Sockets Application and can be started by double clicking the LuciGuard icon. However before attempting to start the application the file LUCIGMAN.INI should be updated to reflect the values programmed under Security ID in the KeyCutter.

The format of the file is simply a list of assignments of values to keywords. If the program does not recognise the string to the left of the '=' or there is no '=' the whole line is treated as a comment.

The most important values which ***must*** be assigned are: NAME which is a string, used to identify a particular LuciGate when reporting events in the log; SECIP which is the IP address programmed on the Smartcard Key for the LuciGate; SECPO which is the UDP port number to be used for the security dialogue between LuciGuard and LuciGate;

Optional keywords are SECID which can be used to identify a particular configuration of the Key and must match the value on the Key and RETRY which controls how many times the LuciGate is prepared to not get a response before triggering the alarm.

The remaining optional keywords enable the user to pre-select the various items in the menus. They are ALARM, NORESPONSE, BYPASSED, BAD_ID, STATUS, ATTACKS and AUDIT. Assigning a value ENABLED has the effect of selecting the item from a menu. Assigning any other value not containing the string ENABLED will de-select the item.

The LUCIGMAN.INI file distributed with the LuciGuard program LUCIGMAN.EXE shows all the keywords.

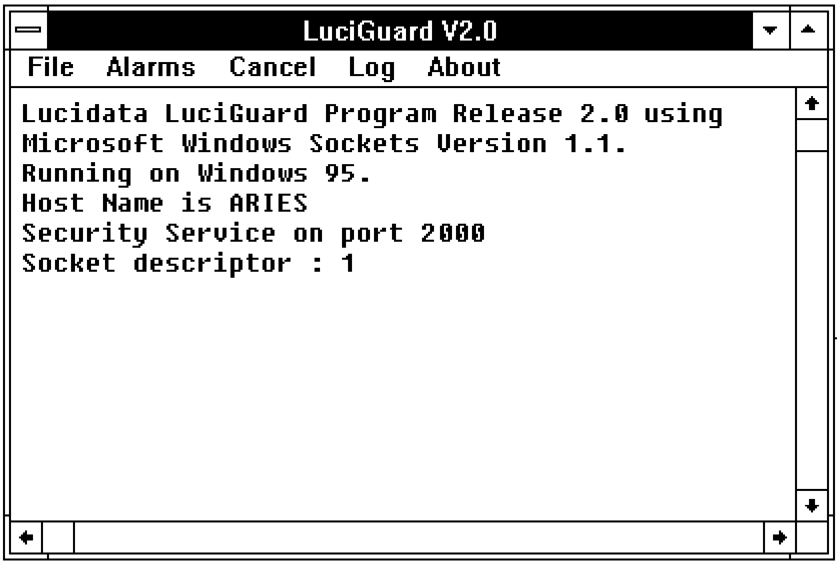
The program may be terminated by clicking **Exit** under the **File** Menu.

The **Alarms** Menu initially shows all Alarms enabled with check marks. Selections can be unchecked (disabled) by clicking with the mouse.

If an alarm event has triggered the audible warning, clicking **Cancel** stops the sound until the next alarm event.

Audit Log

The file LUCIGMAN.LOG will always record the starting and stopping of the program but will only keep a log of activities if the option **Audit Log** under the **Log** Menu is enabled. All events are time stamped and added to any existing log file so the log can get quite long. It should be reviewed frequently and if 'clean' deleted or archived under another name before next activating the LuciGuard program.



```
Lucidata LuciGuard Program Release 2.0 using
Microsoft Windows Sockets Version 1.1.
Running on Windows 95.
Host Name is ARIES
Security Service on port 2000
Socket descriptor : 1
```

The files LUCIGMAN.INI and LUCIGMAN.LOG should both reside in the same directory as LUCIGMAN.EXE. Multiple LuciGuard programs can be run concurrently, provided they are run from different directories.

Figure 4. is a sample from the log file showing typical entries.

```
LuciGuard Started at 08:27:23 on the 05/02/1997
Audit Log Not Enabled
08:27:27  Logging Enabled
08:27:27  Firewall No.1 Not Responding
08:27:30  Alarm Acknowledged
08:27:31  Firewall No.1 Not Responding
08:27:34  Firewall No.1 Not Responding
08:27:36  Firewall No.1 Restarted
08:27:36  Firewall No.1 Key Changed
08:27:40  Alarm Acknowledged
08:44:21  Firewall No.1 Not Responding
08:44:23  Firewall No.1 Key Removed
08:44:28  Alarm Acknowledged
08:45:19  Firewall No.1 Possibly Bypassed
08:45:21  Firewall No.1 Possibly Bypassed
08:45:22  Alarm Acknowledged
08:45:23  Firewall No.1 Possibly Bypassed
08:45:25  Firewall No.1 Possibly Bypassed
08:45:28  Firewall No.1 Possibly Bypassed
08:45:29  Firewall No.1 Possibly Bypassed
08:45:32  Firewall No.1 Possibly Bypassed
08:45:34  Firewall No.1 Possibly Bypassed
08:45:34  Alarm Acknowledged
08:45:36  Firewall No.1 Possibly Bypassed
08:45:38  Alarm Acknowledged
08:46:16  Firewall No.1 Not Responding
08:46:18  Firewall No.1 Key Changed
08:46:22  Alarm Acknowledged
08:48:12  Firewall No.1 Bad Sec.ID
08:48:14  Firewall No.1 Bad Sec.ID
08:48:16  Firewall No.1 Not Responding
08:48:18  Firewall No.1 Key Changed
08:48:22  Alarm Acknowledged
08:57:57  Audible Alarm Disabled
08:58:04  No Response Alarm Disarmed
08:58:08  Bypass Alarm Disarmed
08:58:10  Bad ID Alarm Disarmed
08:58:13  Status Change Alarm Disarmed
08:58:15  Audible Alarm Enabled
08:58:24  Bypass Alarm Armed
08:58:37  Bad ID Alarm Armed
08:58:40  Status Change Alarm Armed
08:58:45  Logging Disabled
08:58:48  LuciGuard Stopped
```

Sample LuciGuard LOG File

Alarm Conditions

The LuciGuard program will send a probe message to the firewall about every two seconds. It will allow about two seconds for a response before trying twice more in quick succession.

No Response Alarm

If it fails to get a response and the **No Response** Alarm is checked, then the alarm is triggered. The alarm event can be generated by a powered down firewall, a disconnection or network fault between the monitor and the firewall, removal of the key or its replacement by an invalid key.

In a very busy network it is possible that the security poll or its reply may be lost as it uses the UDP protocol. Under these conditions it may be advisable to set the RETRY count in the .INI file to a value greater than the default of one to avoid frequent erroneous alarms.

Bypassed Alarm

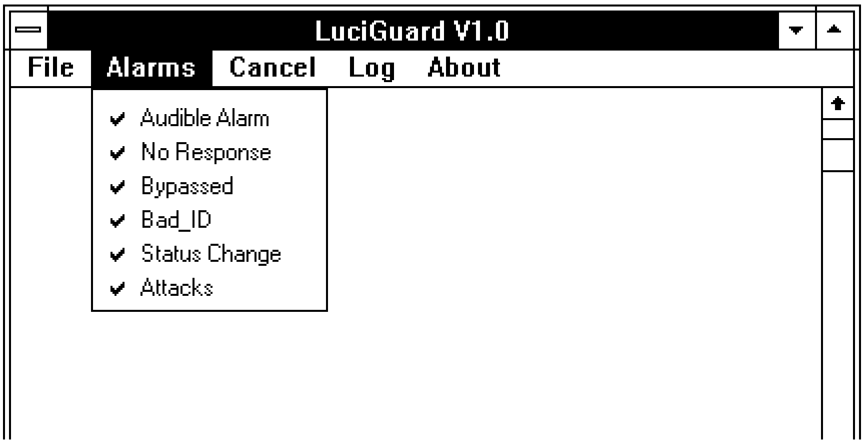
If the LuciGate Firewall has been passing packets through to the Outer World but has not been getting any back it may have been bypassed. That is to say that it has been left connected to the Inner World so that it can be 'seen' but the Outer World has been directly connected to the Inner World. This alarm can be triggered in very low traffic level conditions because some legitimate infrequent packets may be sent to the Outer World and get no response for quite valid reasons. It only takes one successful reply within ten seconds to reset the dead man timer and so not trigger the alarm. In high traffic situations it is unlikely to generate false alarms. This alarm can be disabled by unchecking the option **Bypassed?** in the **Alarms** Menu.

Status Change Alarm

If the Status Change option is checked in the Alarms Menu any apparent change in configuration of the firewall like switch settings or key removal and replacement will trigger an alarm. It could be an indication that the firewall is being tampered with.

Bad ID Alarm

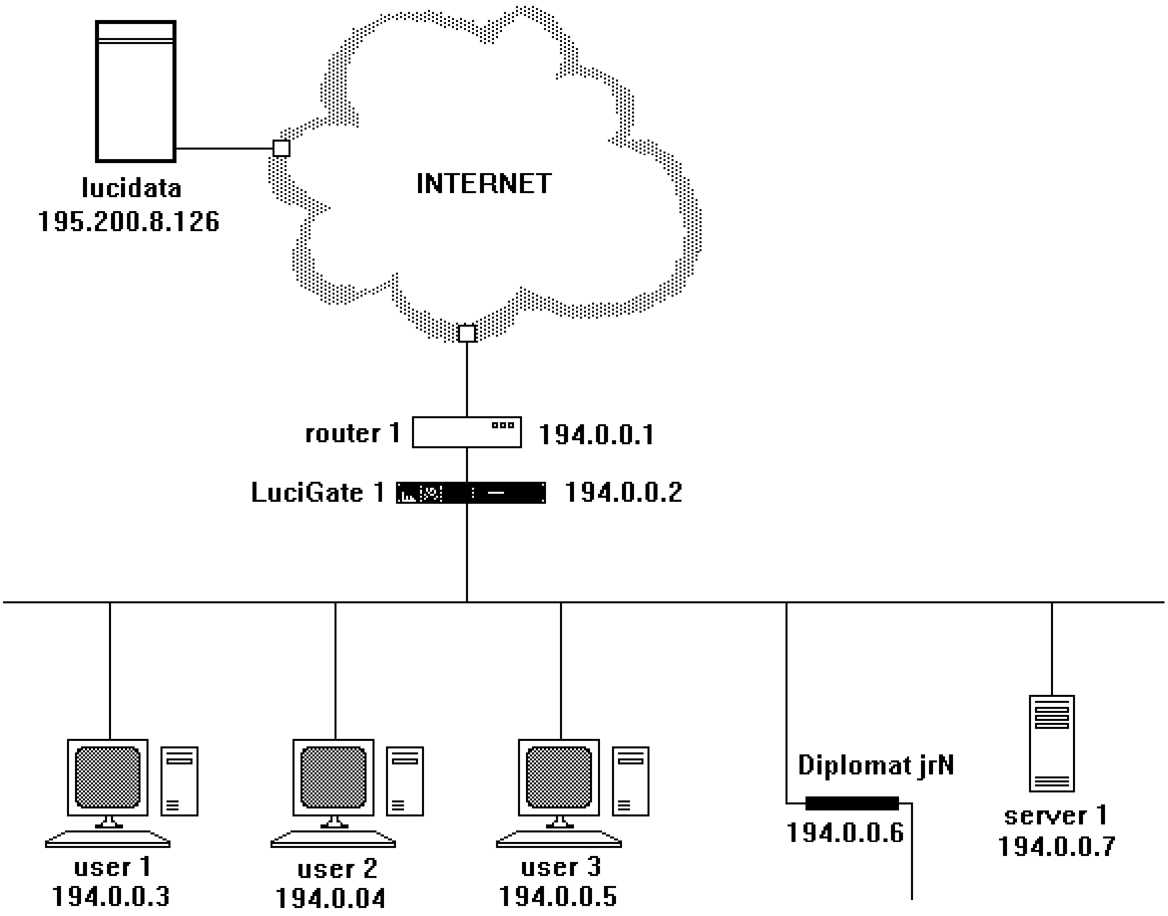
The response packet from the LuciGate Firewall contains a copy of the Security String if one has been programmed on the key. If the Bad_ID option is checked in the Alarms Menu the Security String is checked against the value held in the .INI file and if they do not agree the alarm is triggered. Use of this feature can form part of a configuration control procedure.



✓ Audible Alarm
✓ No Response
✓ Bypassed
✓ Bad_ID
✓ Status Change
✓ Attacks

The following pages give a short tutorial with examples of how to use the LuciGate Firewall. You are strongly advised to follow the tutorial before attempting to set up your own system.

It will also be helpful to have the KeyCutter program installed and running on a nearby screen as you follow the tutorial.



As an illustration of how the LuciGate Firewall might be used in practice a hypothetical scenario is shown in figure A1.

It depicts an organisation that has a local network which includes a registered subnet 194.0.0.0 to 194.0.0.7 named *LocalNet*.

It has an access router *(router 1)*, to the Internet and the LuciGate Firewall(*LuciGate 1*) has been placed in the usual position to protect the network. There is no significance in the way the IP addresses have been allocated in the example and there is no need for the LuciGate itself to have an IP address. One "specially" privileged remote host has been identified as *lucidata* for the purposes of this example.

Within the subnet the users have different requirements to access the Internet and therefore their access is tailored to their requirements, not so much to limit their capability, but to minimise their visibility in the global IP/Protocol/Port address space.

The users are pure Clients but the network also hosts its own Web Server called *server1*. *Server1* also acts as a proxy mail server.

Diplomat jrN is a special piece of hardware performing some esoteric control and monitor function on local equipment and is monitored and configured from *lucidata* remotely.

We will use this same scenario to illustrate several common type of configuration. Before we start however we must make sure all the things we are going to talk about have been given mnemonic names in the appropriate mnemonic files. The five mnemonic files relevant to this tutorial are listed below for ease of reference.

MnTypes.txt

```
'Mnemonic,Packet Type Value in hex,Comment
Ucast,1,All Ethernet Packets with Unicast Addresses
Mcast,2,All Ethernet Packets with Multicast Addresses
Bcast,3,All Ethernet Packets with Broadcast Addresses
IP,800,The IP family of protocols
ARP,806,Address Resolution Protocol
BPDU,42,Bridge Protocol Data Units
XNS,E0,All Xerox derived protocols
SNAP,AA,SNAP Frames like Appletalk
```

MnHosts.txt

```
'Mnemonic,IP,Optional Translation,Comment
router1,194.0.0.1,,Access router to the Internet
LuciGate1,194.0.0.2,,Lucigate Firewall
user1,194.0.0.3,,First local client user
user2,194.0.0.4,,Second local client user
user3,194.0.0.5,,Third local client user
jrN,194.0.0.6,,Diplomat jrN Async/TCP convertor
server1,194.0.0.7,,Our local web server
lucidata,195.200.8.126,,Remote friendly site
```

MnNets.txt

```
'Mnemonic,Net Address/Mask,Optional Translation,Comment
localnet,194.0.0.0/255.255.255.248,,Local subnet of 8 addresses
```

MnProtocols.txt

```
'Mnemonic,Protocol Value in decimal,Comment.
ICMP,1,Internet Control Management Protocol
TCP,6,Transport Control Protocol
UDP,17,User Datagram Protocol
ARPS,255,Pseudo IP Protocol for ARP
GRE,47,General Routing Encapsulation used by PPTP
ESP,50,Encapsulation Security Payload used by IPSec
AH,51,Athentication Header used by IPSec
L2TP,115,Level 2 Tunneling Protocol
```

MnPorts.txt

```
'Mnemonic,Lower or only value in decimal,Upper bound if it
exists,Comment. Updated 02/03/06
FTP1,20,,File Transfer Protocol Interactive
FTP2,21,,File Transfer Protocol Data
SSH,22,,Secure Shell
Telnet,23,,Terminal Service Port
SMTP,25,,Simple Mail Transport Protocol
ESMTP,587,,Mail Submission Protocol
DNS,53,,Domain Name Service
BOOTPS,67,,BootP Server
BOOTPC,68,,BootP Client
HTTP,80,,Hyper text Transfer Protocol
HTTPS,443,,Secure HTTP
POP3,110,,Post Office Protocol Service
IMAP4,143,,IMAP4 Mail Protocol
SUNRPC,111,,Sun Remote Procedure Call
PPTP,1723,,PPTP Port
IPSECESP,50,,TCP port used by IPSec for ESP
IPSECAH,51,,TCP port used by IPSec for AH
IPSECIKE,500,,UDP port used by IPSec for IKE
jrNServer,1058,,A JRN Service
jrNRemote,12345,,Remote JRN configuration
Pondside,1012,,Remote pondside monitor
```

Note: There are two ranges of Ports predefined within the Keycutter called LoPorts and HiPorts. These are put in for user convenience and represent the usual ranges of port numbers that are used for Well Known Services, 1 to 1023, and ordinary Clients, 1024 to 65368. Application developers have not stuck to this convention however and some services are offered on ports in the HiPort range. Some systems also limit the range of ports used by client processes to 1024 to 5000 or other values. When the user is familiar with the conventions used in his/her own environment different ranges should be defined and used instead of the defaults to further tighten the effect of the rules.

We will also use a shorthand way of describing which buttons and lists you need to use to generate the rules we will be talking about. The *Rules* screen has three major columns of items that you can choose from starting with the packet *Types* list on the left of the screen. There is then a variable set of *Filter Options* that change dynamically as you interact with the program. Finally there may or may not be a list of things appearing from time to time which you can either ignore, single click or double click on. To help you navigate around these objects when building up a rule we adopt the following conventions:

Items from the packet *Types* column are surrounded by angle brackets i.e. **<**IP**>**

Items from the *Filter Options* are surrounded by square brackets i.e. **[**By Host IP**]**

Items from a list of things are surrounded by round brackets i.e. **(**ICMP**)** and a double click is shown with double brackets as **((**ICMP**))**

Before we proceed however we need to start a *New Ruleset* for this demonstration. We do this by selecting *New Key File* from the *File* menu and supplying a name. This tutorial uses the name EXAMPLE1. We then select the *Rules* menu and click *New Rules* to initialise some internal tables.

Example 1 - Simple Access to the Internet

This is the most common requirement – to let all machines on the network have access to the Internet but to protect the local network from penetration from outside. There are three rules that are almost always needed so it is worth explaining them here.

For any workstation to communicate with a host computer that is not on the same physical network as itself requires the help of a router or gateway. In our example network *router1* would be defined as the default gateway in each of the workstations. This means that whenever a workstation had a packet of data to send to a remote host it would send it via *router1*. In order to do this the workstation needs to find out the physical or Ethernet address of the network adapter of *router1*. It does this by issuing an ARP (Address Resolution Protocol) request. Now there are many types of ARP requests flying about any network that is Microsoft based and we do not need to pass them to the router if they are not IP ARPs. So our first rule is obtained by clicking on ARP in the Types list and ARP for IP in the Filter Options or using our shorthand

<ARP**> [**ARP for IP**]**

This produces the text "**Allow ARP packets for IP**" in the *Current Rule* window which can now be added to our new Ruleset by clicking the *Add Rule* button.

There will be many IP ARP packets going between different workstations on the network that are of no interest to *router 1.* It will only respond to ARP packets addressed to it so there is no point in getting *Lucigate 1* to pass on any other ARPs as it is unecessary extra work. So our second most common rule is generated by

<IP**> [**Any IP Address**] [**By IP Protocol**] (**ARPS**) [**Access Routers**] (**router1**)**

This produces the text "**Allow the use of ARPS to access router1**" in the Current Rule window. Add it to the Ruleset.

Any access to the Internet will need to be able to resolve names of things to IP addresses. This service is provided by DNS (Domain Name System) servers using the UDP (User Datagram Protocol) protocol. Now the UDP protocol is potentially dangerous as it is symmetrical - there is no difference between Client and Server. So we make a restricted rule that gives us access to the DNS service at minimum risk i.e. only the Client's HiPorts are open for access to the DNS service.

<IP**> [**Any IP Address**] [**By IP Protocol**] ((**UDP**)) [**From Port**] (**Hiports**) [**Allowed Services**] (**DNS**)**

This produces the text "**Allow the use of UDP Hiports for DNS service**" in the *Current Rule* window. Notice how the extra *Filter Option* appeared when UDP was double clicked.

But our users want to surf the web so we need a fourth rule.

<IP**> [**Any IP Address**] [**By IP Protocol**] ((**TCP**)) [**From Port**] (**Hiports**) [**Allowed Services**] (**HTTP**)**

This produces the text “**Allow the use of TCP Hiports for HTTP service**” in the *Current Rule* window. Once this last rule has been added you can return to the main screen by clicking the *Return* control.

Select the *Key* menu item, place a Smartcard key in the Smart Mouse programming unit and click on *Write Key*. When the process is finished select the *Key* menu item again and click on *Read Key*. The *Summary* window should show the current date and time recorded. Plug the Key into a powered up and connected Lucigate firewall and all the users will have access to the Internet. A Key File is automatically saved with the Ruleset name and extension .KEY when a Key is cut.

It is good practice to keep a human readable record of what has been configured, so before leaving the Keycutter program, select the *File* menu item and choose *Save Report File as Text*. Using the default name will create a file called example1.txt a print out of which is reproduced below for ease of reference.

```
LUCIGATE KEYCUTTER REPORT GENERATED ON 08/11/01 AT  08:34:21

Keycutter Version 3.13 05/11/01

THE FOLLOWING RULES ARE IN RULESET EXAMPLE1

 1 Allow ARP packets for IP
 2 Allow the use of ARPS to access router1
 3 Allow the use of UDP HiPorts for DNS service
 4 Allow the use of TCP HiPorts for HTTP service
```

Example 2 – Some Users have extra privileges

In this example we build on Example 1 to allow some users to do more. Typically the IT Manager (*user 1*) wants to be able to download files from anywhere in the world but for security reasons does not want this facility available to anyone else except his deputy (*user 2*). The IT Manager also needs to be able to Ping anywhere in the world and Telnet onto the access router for routine monitoring. Downloading files uses the File Transfer Protocol or FTP and Ping uses the Internet Control Message Protocol or ICMP. *User 3* has been given special permission to access an on-line Banking site from work and needs to be able to use the secure Hypertext Transfer Protocol (HTTPS).

Start by loading the EXAMPLE1 Ruleset by clicking the *File* menu item and selecting *Open Key File*. Find the file EXAMPLE1.KEY and load it. Click the *Rules* menu item and notice that the rules appear in the *Ruleset* display. DO NOT click New Rules as this would clear the existing rules and we want to add to them. First add the IT Managers choices.

<IP> [By Host IP] ((user1)) [By IP Protocol] (ICMP)

This produces the text “**Allow user1 to use ICMP**” in the Current Rule window. *Add Rule*.

<IP>[By Host IP] ((user1)) [By IP Protocol] ((TCP)) [From Port] (HiPorts)[Allowed Services](FTP1)

This produces the text “**Allow user1 to use TCP HiPorts for FTP1 service**” in the *Current Rule* window. *Add Rule*.

<IP> [By Host IP] ((user1)) [By IP Protocol] ((TCP)) [From Port] (HiPorts)[Allowed Services] (Telnet)[Access Routers](router1)

This produces the text “**Allow user1 to use TCP HiPorts to access Telnet service on router1**” in the *Current Rule* window. *Add Rule.*

Now the deputy’s FTP access.

<IP> [By Host IP] ((user2)) [By IP Protocol] ((TCP)) [From Port] (HiPorts) [Allowed Services] (FTP1)

This produces the text “**Allow user2 to use TCP HiPorts for FTP1 service**” in the *Current Rule* window. *Add Rule*.

Now user 3’s on-line Banking.

<IP> [By Host IP] ((user3)) [By IP Protocol] ((TCP)) [From Port] (HiPorts) [Allowed Services] (HTTPS)

This produces the text “**Allow user3 to use TCP HiPorts for HTTPS service**” in the *Current Rule* window. *Add Rule*.

Return to the main screen but DO NOT Write Key straight away because the original EXAMPLE1.KEY file will be overwritten. First click *File* and select *Save Key File*. Then edit the filename to EXAMPLE2.KEY before saving. Also *Save Report File as Text.* The report file example2.txt is printed below.

```
LUCIGATE KEYCUTTER REPORT GENERATED ON 08/11/01 AT  10:11:32

Keycutter Version 3.13 05/11/01

THE FOLLOWING RULES ARE IN RULESET EXAMPLE2

 1 Allow ARP packets for IP
 2 Allow the use of ARPS to access router1
 3 Allow the use of UDP HiPorts for DNS service
 4 Allow the use of TCP HiPorts for HTTP service
 5 Allow user1 to use ICMP
 6 Allow user1 to use TCP HiPorts for FTP1 service
 7 Allow user1 to use TCP HiPorts to access Telnet service on router1
 8 Allow user2 to use TCP HiPorts for FTP1 service
 9 Allow user3 to use TCP HiPorts for HTTPS service
```

Example 3 - We have a Server

Carrying on from where we left off in the previous example enter the Rules screen again. Whenever the Rules screen is entered the programming is automatically approached from the point of view of an Inner World Client. This is because Clients have the least privileges. We now want to allow our Web Server to be visible to the outside world and to let it accept connections. We also want it to be able to exchange mail with other mail servers which use the Simple Mail Transport Protocol or SMTP. So *Server1* must be given Client rights to access external SMTP servers.

<IP**>[**By Host IP**]((**server1**)) [**By IP Protocol**]((**TCP**))[**From Port**](**HiPorts**)[**Allowed Services**](**SMTP**)**

This produces the text “**Allow server1 to use TCP HiPorts for SMTP service**” in the *Current Rule* window. *Add Rule*.

We now change the programming mode by clicking the option button labelled *Servers* in the panel labelled *Inner World Hosts* near the top right hand corner of the screen. You will see that we now get different words and grammar appearing in the *Current Rule* window. To make our server visible as an SMTP server to the outside world we need –

<IP**> [**By Server IP**] ((**server1**)) [**By IP Protocol**] ((**TCP**)) [**On TCP/UDP Port**] (**SMTP**)**

The rule “**server1 offers TCP SMTP service on port 25**” appears in the *Current Rule* window. *Add Rule*. We do not have to go back to the beginning to enable the Web Server rule we just click on HTTP in the services list. The *Current Rule* window now contains “**server1 offers TCP HTTP service on port 80**”. *Add Rule*.

Return to the main screen and save the Key File as EXAMPLE3.KEY and its Report as example3.txt. Example3 looks like this –

```
LUCIGATE KEYCUTTER REPORT GENERATED ON 08/11/01 AT  13:54:51

Keycutter Version 3.13 05/11/01

THE FOLLOWING RULES ARE IN RULESET EXAMPLE3

 1 Allow ARP packets for IP
 2 Allow the use of ARPS to access router1
 3 Allow the use of UDP HiPorts for DNS service
 4 Allow the use of TCP HiPorts for HTTP service
 5 Allow user1 to use ICMP
 6 Allow user1 to use TCP HiPorts for FTP1 service
 7 Allow user1 to use TCP HiPorts to access Telnet service on router1
 8 Allow user2 to use TCP HiPorts for FTP1 service
 9 Allow user3 to use TCP HiPorts for HTTPS service
 10 Allow server1 to use TCP HiPorts for SMTP service
 11 server1 Offers TCP SMTP service on port 25
 12 server1 Offers TCP HTTP service on port 80
```

Example 4 – A Trusted Relationship

It is possible to make very tight bindings between local and remote hosts. In this example we are prepared to let an application program running on a remote site that we trust, *lucidata*, to take control of a device on our network, the *Diplomat jrN*. We know that the application always uses UDP port jrNServer to control the Diplomat jrN and that the *Diplomat jrN* will only respond on port jrNRemote so we can make it happen. First we select the final programming mode by clicking on the button labelled *Peers* in the *Inner World Hosts* panel on the *Rules* screen, then –

<IP>[By Host IP]((jrN))[By IP Protocol]((UDP))[On TCP/UDP Port]((jrNRemote))[Peer Hosts]((lucidata))[Allowed Ports](jrNServer)

This produces the rule "**jrN Only Allows UDP on port 12345 to bind to lucidata port 1058**" in the Current Rule window. Save it as EXAMPLE4.KEY and its Report file as example4.txt. The full set of rules now look like -

```
LUCIGATE KEYCUTTER REPORT GENERATED ON 08/11/01 AT  14:25:13

Keycutter Version 3.13 05/11/01

THE FOLLOWING RULES ARE IN RULESET EXAMPLE4

 1 Allow ARP packets for IP
 2 Allow the use of ARPS to access router1
 3 Allow the use of UDP HiPorts for DNS service
 4 Allow the use of TCP HiPorts for HTTP service
 5 Allow user1 to use ICMP
 6 Allow user1 to use TCP HiPorts for FTP1 service
 7 Allow user1 to use TCP HiPorts to access Telnet service on router1
 8 Allow user2 to use TCP HiPorts for FTP1 service
 9 Allow user3 to use TCP HiPorts for HTTPS service
 10 Allow server1 to use TCP HiPorts for SMTP service
 11 server1 Offers TCP SMTP service on port 25
 12 server1 Offers TCP HTTP service on port 80
 13 jrN Only Allows UDP on port 12345 to bind to lucidata port 1058
```

Example 5 - Monitoring the LuciGate

So far the Lucigate has been totally invisible to both the Inner and Outer Worlds. It always will be invisible to the Outer World but it is usually helpful to at least be able to Ping it from the inside as a way of checking it is still alive. You may also wish to use the LuciGuard monitor program which was described earlier. To give the Lucigate an IP address click on the *Security ID* menu item and assign an IP address if you simply want to Ping it. If you want to use LuciGuard, you need to assign a Port and (optionally) an ID string. This information is displayed as follows in the Report File.

```
LUCIGATE KEYCUTTER REPORT GENERATED ON 08/11/01 AT  15:08:25

Keycutter Version 3.13 05/11/01

THE FOLLOWING RULES ARE IN RULESET EXAMPLE5

 1 Allow ARP packets for IP
 2 Allow the use of ARPS to access router1
 3 Allow the use of UDP HiPorts for DNS service
 4 Allow the use of TCP HiPorts for HTTP service
 5 Allow user1 to use ICMP
 6 Allow user1 to use TCP HiPorts for FTP1 service
 7 Allow user1 to use TCP HiPorts to access Telnet service on router1
 8 Allow user2 to use TCP HiPorts for FTP1 service
 9 Allow user3 to use TCP HiPorts for HTTPS service
 10 Allow server1 to use TCP HiPorts for SMTP service
 11 server1 Offers TCP SMTP service on port 25
 12 server1 Offers TCP HTTP service on port 80
 13 jrN Only Allows UDP on port 12345 to bind to lucidata port 1058


Lucigate IP Address is  -    194. 0. 0. 2
Lucigate Security Port is    2000
Lucigate ID string is   -   LUCIGATE1
```

Example 6 - Using MAC address Filtering

With the increased use of WiFi connectivity and the more likely use of DHCP it has become more difficult to rely on IP addresses alone as an identifying method for a device. Since Rev 3.13 of the Lucigate Firmware and Rev. 3.21 of the Keycutter program it has been possible to utilize MAC address lists. A MAC address is usually permanently assigned to a network adaptor and is propogated through WiFi access points. It is necessary however to maintain two separate lists, one for adaptors on the Inner World, called Source addresses, and one for network adaptors on the Outer World called Destination addresses. These lists are kept in files MnMACS.txt and MnMACD.txt respectively.

There is one special case that must be bourne in mind. If a single MAC Destination address is selected in a Ruleset the actual network adaptor of the Lucigate Inner World interface is programmed with that address to take advantage of the hardware's efficiency in recognizing it. This avoids the Lucigate having to deal with the majority of the packets seen on the LAN segment that are local to the segment. Qualifying packets will be passed through untouched unless they contain the IP address of the Lucigate itself (if defined) when they will be further processed. Similarly if a single MAC Source address is selected the actual network adaptor of the Lucigate Outer World interface is programmed with that address.

In all other cases the MAC addresses contianed in the Ruleset will be consolidated into source and destination lists that will be used to qualify packets travelling through the Lucigate. The MAC rules are very simple and if defined are tested before any other rule.

Where there are large numbers of network adaptors that need access there is a psuedo entry in the MAC lists presented which has the effect of selecting all the entries in the corresponding MnMAC list.

```
LUCIGATE KEYCUTTER REPORT GENERATED ON 26/04/06 AT  16:24:27

Keycutter Version 3.21 02/03/06 VB5

THE FOLLOWING RULES ARE IN RULESET EXAMPLE6

 1 Allow ARP packets for IP
 2 Allow the use of ARPS to access router1
 3 Allow the use of UDP HiPorts for DNS service
 4 Allow the use of TCP HiPorts
 5 Allow the use of ICMP
 6 Allow All Adaptors to be a Source Adaptor
 7 Allow Lucidata to be a Source Adaptor


Lucigate IP Address is  -    194. 0. 0. 2
Lucigate Security Port is    2000
Lucigate ID string is   -   LUCIGATE1
```

Rule 7 is not necessary as Lucidata is in the list of All Adaptors but was included to show the two rule types that can be generated.