How to configure the AT-AR450S Firewall using the Graphical User Interface (GUI)

Introduction

This document describes the firewall configuration facility available on the AT-AR450S HTTP-based Graphical User Interface (GUI). The GUI is a web-based device management tool, designed to make it easier to configure and monitor the router, and provides an alternative to the Command Line Interface (CLI). Its purpose is to make complicated tasks simpler and regularly performed tasks quicker.

The AT-AR450S is referred to as the AR450S throughout this document.

Hardware and software used

The description in this document is based on an AR450S router running software release 2.5.2.

Allied Telesyn
Simply connecting the IP world

While every effort has been made to ensure that the information contained within this document is accurate, Allied Telesyn International can not accept any liability for errors in, or omissions arising from the use of this information.

Accessing the GUI

You gain web access to the AR450S by typing into a web browser the IP address of the router, then inserting a username and password into the resulting login dialog. Table 1 shows supported operating system and browser combinations. A copy of Internet Explorer can be found on the router's Documentation and Tools CD-ROM.

Table 1: Supported browsers and operating systems

	IE 5.0	IE 5.5	IE 6.0	NS 6.2.2	NS 6.2.3
Windows 95	✓				
Windows 98	✓	✓	✓		
Windows ME	✓	✓	✓	✓	✓
Windows 2000	✓	✓	✓	✓	✓
Windows XP	✓	✓	✓	✓	✓

JavaScript must be enabled. To enable JavaScript in Internet Explorer:

1. From the Tools menu, select Internet Options
2. Select the Security tab
3. Click on the Custom Level button
4. Under the Scripting section, ensure that "Active scripting" is enabled.

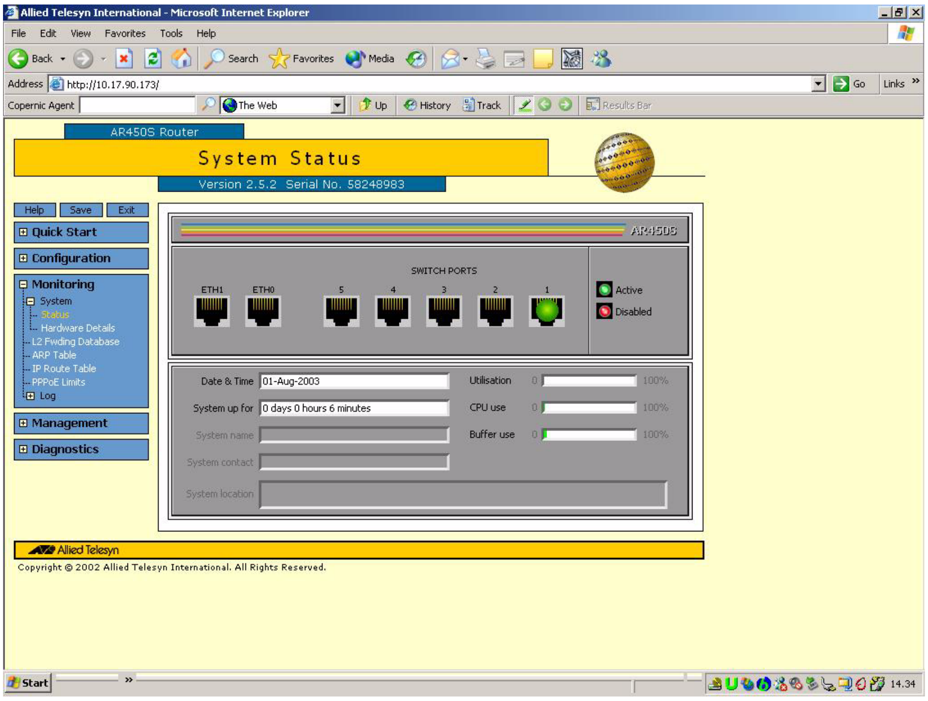
To enable JavaScript in Netscape 6.2.*x*:

1. From the Edit menu, select Preference
2. Select the Advanced menu option.
3. Ensure that the "Enable JavaScript for Navigator" checkbox is checked.

The minimum screen resolution on the PC is 800x600.

When you have typed in your router's IP address and entered your username and password, the web GUI opening screen as shown in Figure 1 is displayed. This screen shows the system status on the AR450S router, and system hardware details for AR410 Series routers.

Figure 1: An example of the System Status page of the AR450S



Date & Time: 01-Aug-2003

System up for: 0 days 0 hours 6 minutes

System name:

System contact:

System location:

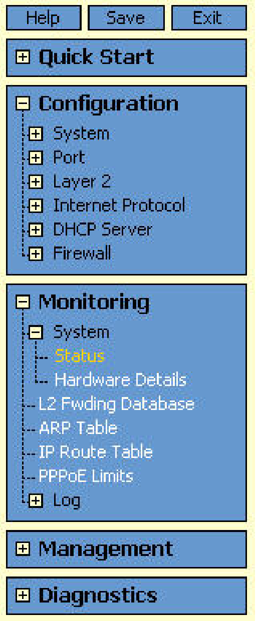
Utilisation: 0 100%

CPU use: 0 100%

Buffer use: 0 100%

Copyright © 2002 Allied Telesyn International. All Rights Reserved.

The GUI consists of a large number of pages, which you navigate between using the sidebar menu on the left of the window, as shown below.



GUI Help

The GUI has a comprehensive help system, which is available when configuring the AR450S firewall. The help system supplements the information in this document. If you want help at any time, click the **Help button** on the sidebar menu or on the page for which you require assistance. The GUI's context-sensitive help system is displayed in a pop-up window which covers the title of the GUI page. You can move the banner to any part of your screen and/or resize it. Three types of help are available:

- Click **General Page Info** to see brief background and process flow information. The General Page Info displays when you click the Help button.
- Click **Page Element Info** and roll your mouse over an element, to see information about that element.

  To freeze the banner's display so that the help does not change when you move the mouse, press the [Ctrl] key. To unfreeze, press [Ctrl] again.
  Note that element information is not available for entries in tables. To see descriptions of the columns of tables, click Complete Help Page.
- Click **Complete Help Page** to see all available information, including the element information, in a separate printable window.

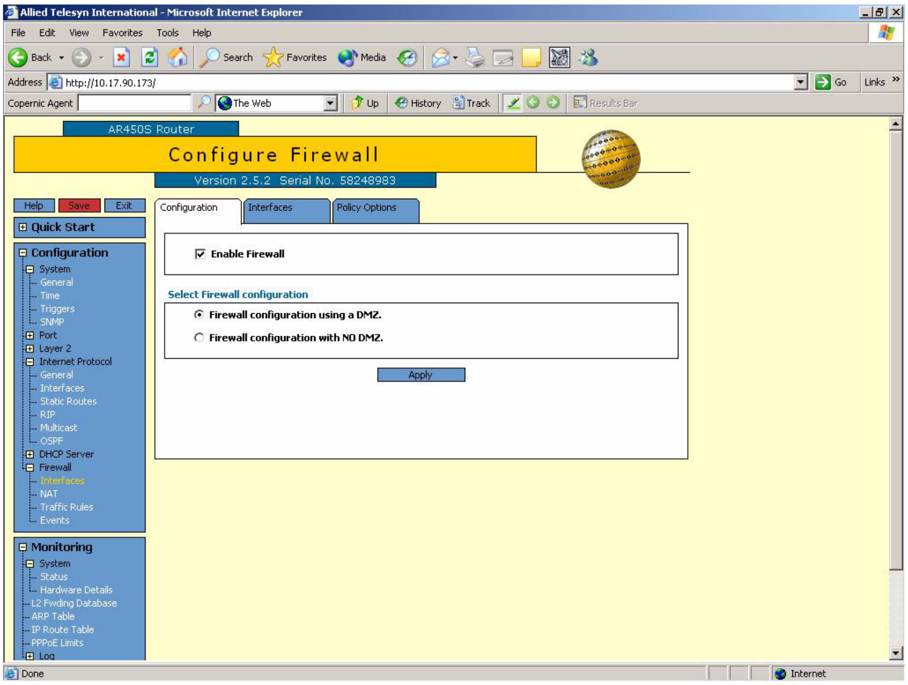
Configuring firewall interfaces

From the Configuration section of the sidebar menu, choose **Firewall**. You may have to click **Configuration** to expand the Configuration menu.

Click **Firewall**, then click **Interfaces**. This displays the Configure Firewall screen as shown in Figure 2. This screen has three tabs, one for configuration, one for interfaces and one for policy options.

You use the configuration tab to select a firewall type, and to enable or disable the firewall.

Figure 2: An example of the Configure Firewall screen



☑ Enable Firewall

Select Firewall configuration

● Firewall configuration using a DMZ.

○ Firewall configuration with NO DMZ.

Configuration tab

The first decision you need to make is whether or not you want to use a DeMilitarised Zone (DMZ). A DMZ keeps your public servers separate from your private LAN. Effectively, this is a choice of whether or not to create a second firewall policy, called DMZ. **Note** that by default no traffic is allowed from the Internet to the DMZ. You must create rules to allow access to your servers.

If you choose not to use a DMZ, the configuration process is simpler as there is only one Firewall policy presented in the configuration windows.

If you choose to have a DMZ, you do not have to configure the DMZ policy immediately. The presence of this other policy does not affect the functionality of the primary policy at all. This means that you can choose "**Firewall configuration using a DMZ**" even if you are not using it initially, but you simply want to have the option to use the DMZ policy in the future.

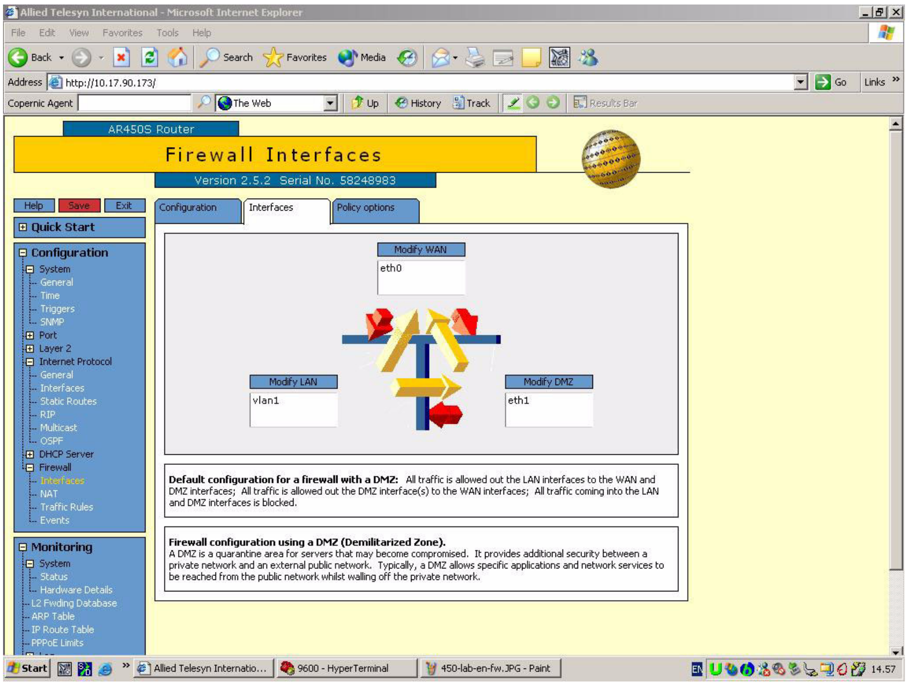
Click **Apply** to accept your configuration changes.

Interfaces tab

The next tab on this screen is the Interfaces tab.

Click the **Interfaces tab** to display the Firewall Interfaces screen, as shown in Figure 3.

Figure 3: An example of the Firewall interfaces screen



Default configuration for a firewall with a DMZ: All traffic is allowed out the LAN interfaces to the WAN and DMZ interfaces; All traffic is allowed out the DMZ interface(s) to the WAN interfaces; All traffic coming into the LAN and DMZ interfaces is blocked.

Firewall configuration using a DMZ (Demilitarized Zone).
A DMZ is a quarantine area for servers that may become compromised. It provides additional security between a private network and an external public network. Typically, a DMZ allows specific applications and network services to be reached from the public network whilst walling off the private network.

This screen shows all the interface groups managed by the firewall:

- Local Area Network (LAN)
- Wide Area Network (WAN), and
- DeMilitarised Zone.

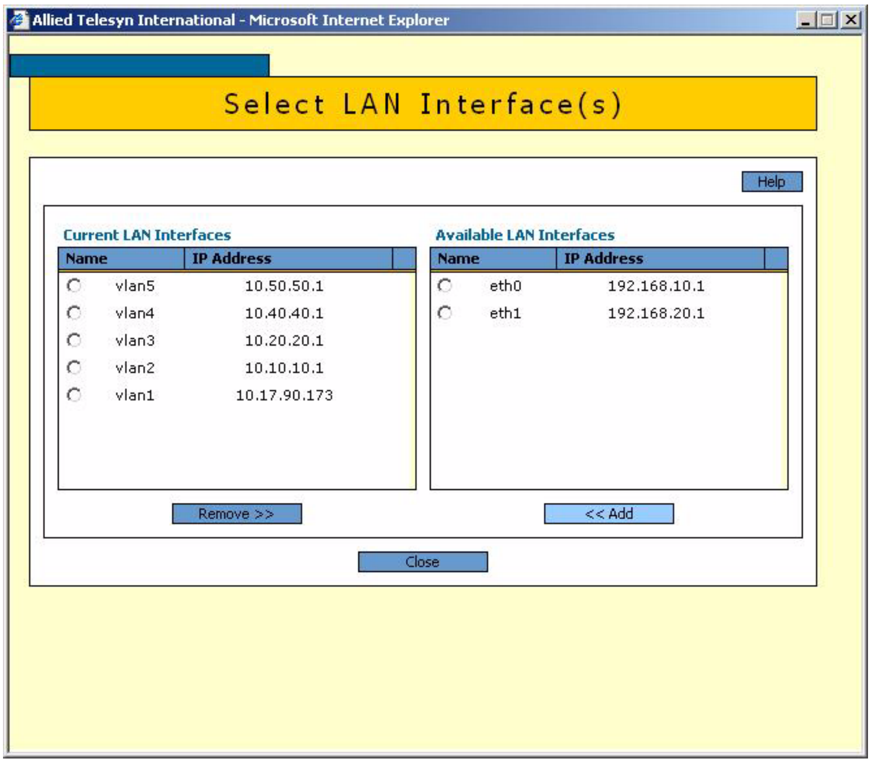
This screen provides you with the opportunity to add existing IP interfaces into one of these interface groups. You do this by clicking **Modify LAN**, **Modify WAN** or **Modify DMZ**. This presents windows that enable the IP interfaces to be moved into or out of the chosen group, as shown in Figure 4 on page 7, Figure 5 on page 7, and Figure 6 on page 8.

You must have already created the IP interfaces. The firewall configuration process does not create any IP interfaces by default.

The interface lists shown in the following three figures are examples only.

! *Every IP interface must be attached to the firewall. Otherwise you will have no protection from attack over that interface. If you add an IP interface after initially configuring the firewall, you must return to the page shown in Figure 3 and manually add it to the firewall.*

Figure 4: An example of the Select LAN Interface window



Allied Telesyn International - Microsoft Internet Explorer

Select LAN Interface(s)

Help

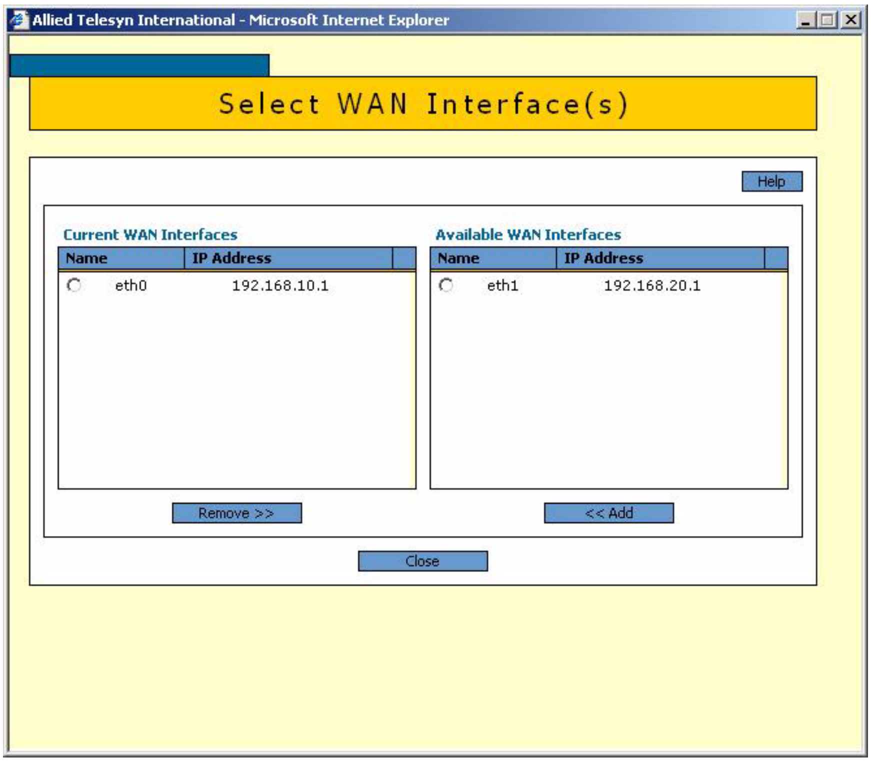
Current LAN Interfaces

Name	IP Address
○ vlan5	10.50.50.1
○ vlan4	10.40.40.1
○ vlan3	10.20.20.1
○ vlan2	10.10.10.1
○ vlan1	10.17.90.173

Available LAN Interfaces

Name	IP Address
○ eth0	192.168.10.1
○ eth1	192.168.20.1

Figure 5: An example of the Select WAN Interface window



Allied Telesyn International - Microsoft Internet Explorer

Select WAN Interface(s)

Help

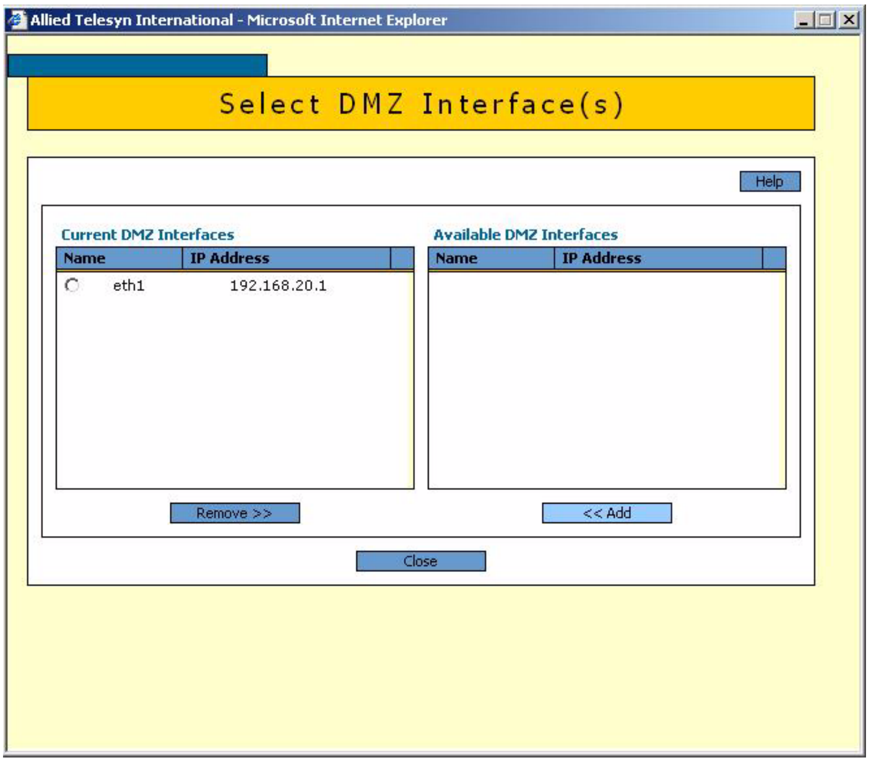
Current WAN Interfaces

Name	IP Address
○ eth0	192.168.10.1

Available WAN Interfaces

Name	IP Address
○ eth1	192.168.20.1

Figure 6: An example of the Select DMZ Interface window



Select DMZ Interface(s)

Current DMZ Interfaces

Name	IP Address
○ eth1	192.168.20.1

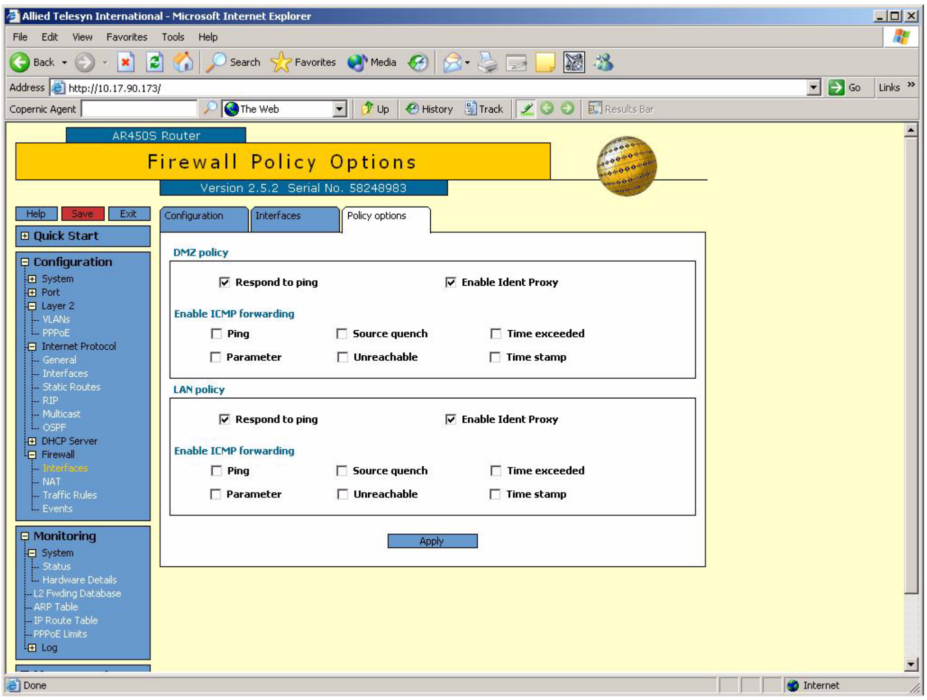
Available DMZ Interfaces

Name	IP Address

Policy options tab

The final tab in the screen is Policy Options. Click the **Policy options tab** to display the firewall policy options screen. The options shown in Figure 7 are the defaults.

Figure 7: An example of the Firewall Policy Options screen



Firewall Policy Options

DMZ policy

☑ Respond to ping ☑ Enable Ident Proxy

Enable ICMP forwarding

□ Ping □ Source quench □ Time exceeded

□ Parameter □ Unreachable □ Time stamp

LAN policy

☑ Respond to ping ☑ Enable Ident Proxy

Enable ICMP forwarding

□ Ping □ Source quench □ Time exceeded

□ Parameter □ Unreachable □ Time stamp

The policy options screen enables you to set the following options on each firewall policy:

- Responding to pings.
- Proxying ident requests.
- Forwarding ICMP packets.

The **respond to ping** checkbox allows users on the Internet and on the private side of the firewall to ping the router. The private interface will always respond to pings.

The **enable ICMP forwarding** checkboxes specifies which ICMP messages the router will forward and respond to over the policy's interfaces in both directions; Public-to-Private AND Private-to-Public.

The ident proxy is a very specific feature that is required to enable successful sessions to some external FTP and SMTP servers - those which send back an ident request to the client before accepting the connection. The **ident proxy** checkbox enables the firewall to respond to these requests on behalf of the client device on the Private side of the firewall.

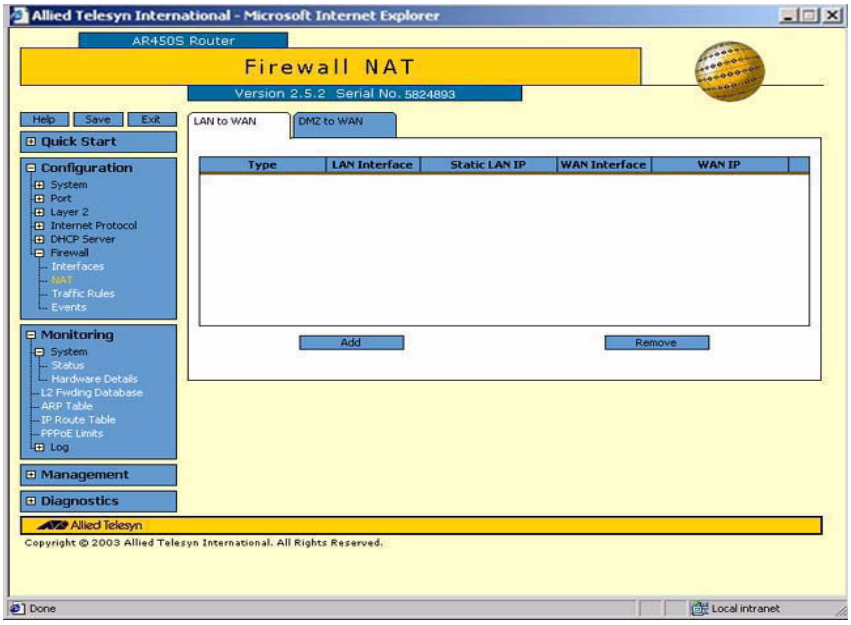
Refer to the GUI help for more information.

Configuring firewall Network Address Translation (NAT)

The next item in the Firewall submenu is NAT, or Network Address Translation.

Clicking **NAT** displays the screen shown in Figure 8, which allows you to view, add and remove the configured Network Address Translations for your LAN.

Figure 8: An example of the Firewall NAT LAN screen

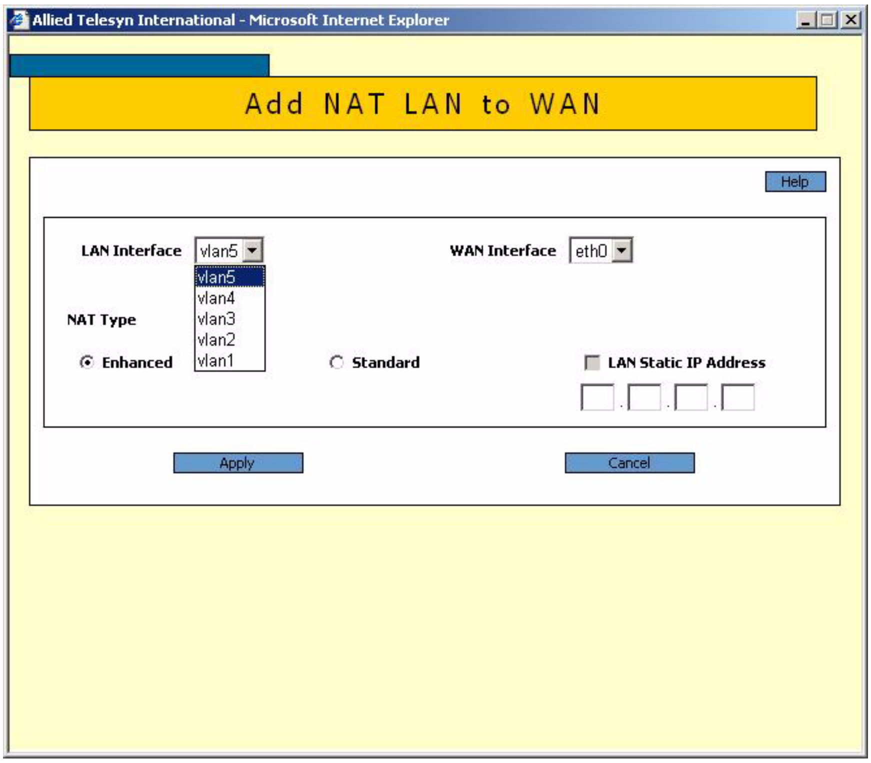


Type	LAN Interface	Static LAN IP	WAN Interface	WAN IP

Each firewall policy appears as a separate tab in this window. You can apply NAT to individual interfaces within both the LAN and DMZ interface groups.

Clicking on the **Add** button for any policy takes you to the relevant Add NAT windows shown in Figure 9 and Figure 10.

Figure 9: An example of the Add NAT LAN to WAN window


Allied Telesyn International - Microsoft Internet Explorer

Add NAT LAN to WAN

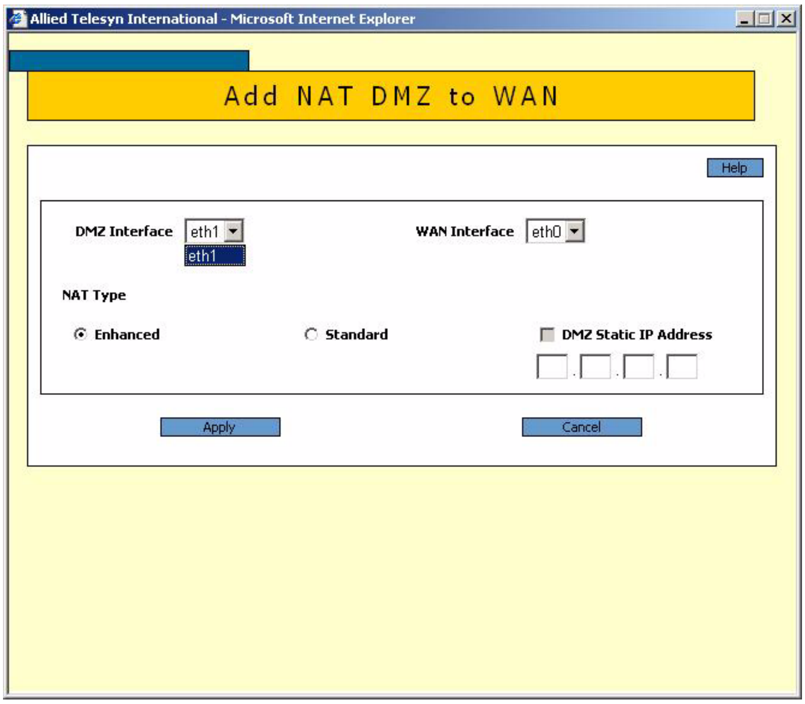
LAN Interface: vlan5

WAN Interface: eth0

NAT Type

● Enhanced ○ Standard ☐ LAN Static IP Address

Figure 10: An example of the Add NAT DMZ to WAN window


Allied Telesyn International - Microsoft Internet Explorer

Add NAT DMZ to WAN

DMZ Interface: eth1

WAN Interface: eth0

NAT Type

● Enhanced ○ Standard ☐ DMZ Static IP Address

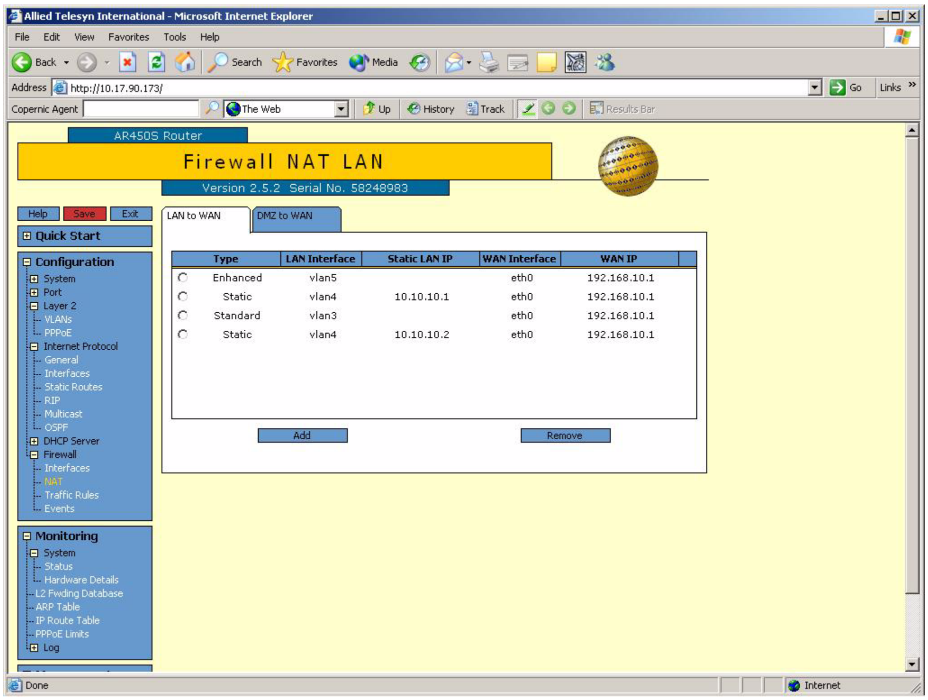
Note that you can specify different NAT features for each of the IP interfaces within an interface group. For example, the VLAN5 interface, within the LAN group, can have enhanced NAT applied to it, and the VLAN2 interface, also within the LAN group, could have static NAT applied to it.

Types of NAT you can configure

You are able to configure the following NAT types using the GUI:

- Enhanced NAT, which maps all the hosts connected to a particular IP interface to the the global address on a WAN interface.
- Static Standard NAT, which maps the IP address of a single device in your LAN to the global address on a WAN interface. For this option, select **Standard** and enter into the LAN static IP address field the IP address of a device on the private LAN.
- Dynamic Standard NAT, which allows all the devices on a particular LAN to use the global address on a WAN interface. For this option, select **Standard** and leave the LAN Static IP Address blank.
  Note that only one LAN device can use the globally-unique IP address at a time.

Figure 11: An example of a NAT configuration using all of the available options described above



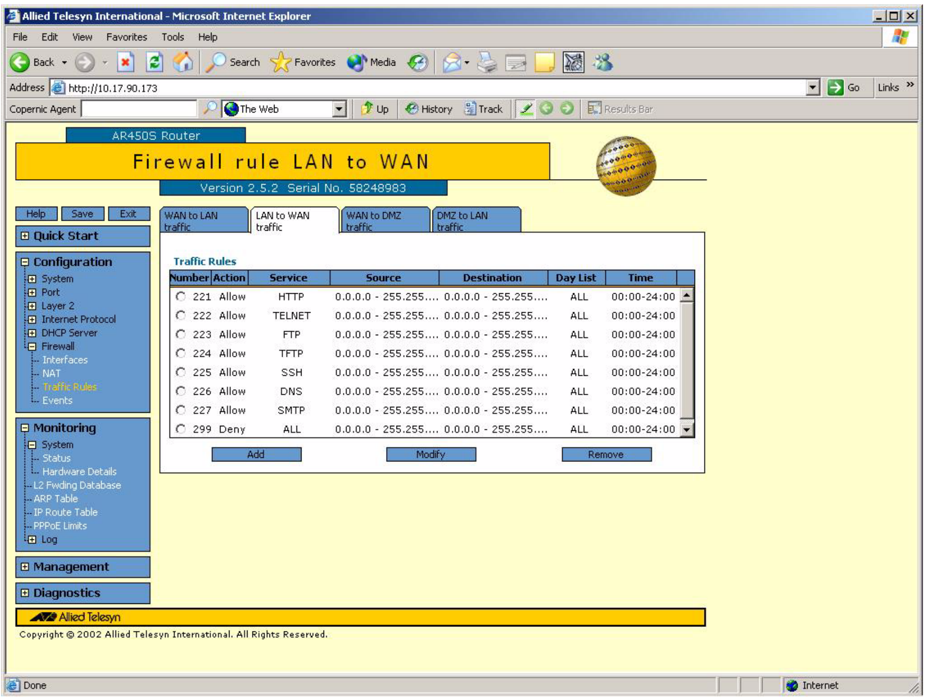
	Type	LAN Interface	Static LAN IP	WAN Interface	WAN IP
○	Enhanced	vlan5		eth0	192.168.10.1
○	Static	vlan4	10.10.10.1	eth0	192.168.10.1
○	Standard	vlan3		eth0	192.168.10.1
○	Static	vlan4	10.10.10.2	eth0	192.168.10.1

Configuring firewall traffic rules

The next item in the Firewall submenu is Traffic Rules.

Clicking **Traffic Rules** displays the Firewall Rules screen, as shown in Figure 12. This screen shows four tabs, one for each traffic direction on each policy e.g. LAN to WAN traffic. All currently defined rules for each policy/direction combination are shown. You are able to add, modify and delete rules.

Figure 12: An example of the LAN to WAN traffic rules screen



Traffic Rules

Number	Action	Service	Source	Destination	Day List	Time
○ 221	Allow	HTTP	0.0.0.0 - 255.255....	0.0.0.0 - 255.255....	ALL	00:00-24:00
○ 222	Allow	TELNET	0.0.0.0 - 255.255....	0.0.0.0 - 255.255....	ALL	00:00-24:00
○ 223	Allow	FTP	0.0.0.0 - 255.255....	0.0.0.0 - 255.255....	ALL	00:00-24:00
○ 224	Allow	TFTP	0.0.0.0 - 255.255....	0.0.0.0 - 255.255....	ALL	00:00-24:00
○ 225	Allow	SSH	0.0.0.0 - 255.255....	0.0.0.0 - 255.255....	ALL	00:00-24:00
○ 226	Allow	DNS	0.0.0.0 - 255.255....	0.0.0.0 - 255.255....	ALL	00:00-24:00
○ 227	Allow	SMTP	0.0.0.0 - 255.255....	0.0.0.0 - 255.255....	ALL	00:00-24:00
○ 299	Deny	ALL	0.0.0.0 - 255.255....	0.0.0.0 - 255.255....	ALL	00:00-24:00

The default behaviour of the initial firewall configuration created by the GUI is shown in Table 2.

Table 2: Default configuration policies

	To	To	To
From	LAN	DMZ	WAN
LAN	Not applicable	Allow	Allow
DMZ	Disallow	Not applicable	Disallow
WAN	Disallow	Disallow	Not applicable

You can create rules to allow and deny particular traffic flows, based on the:

- Source IP address range.
- Destination IP address range.
- Destination TCP/UDP port.
- Protocol type.
- Day of week.
- Time of day.
- NAT requirements.

As noted earlier, there are four tabs on the firewall rule window, one for each traffic direction on each policy. The method for configuring the rules is identical for each tab. The main difference between the tabs is the range of rule numbers available for each case. The list of available ranges for each tab is:

- Rule Range Number for WAN to LAN is 1 to 150
- Rule Range Number for DMZ to LAN is 151 to 220
- Rule Range Number for LAN to WAN is 221 to 299
- Rule Range Number for WAN to DMZ is 51 to 299

The possible operations are add, modify, and delete a firewall rule. **It is not possible to change the ID number of a rule once it has been created.** This is because the rule number governs the order in which rules are executed. It is important to plan your rule numbering in advance, before beginning the process of creating the rules. For example, it is better to have more specific rules at the top of the list, and more generic rules at the end of the list.

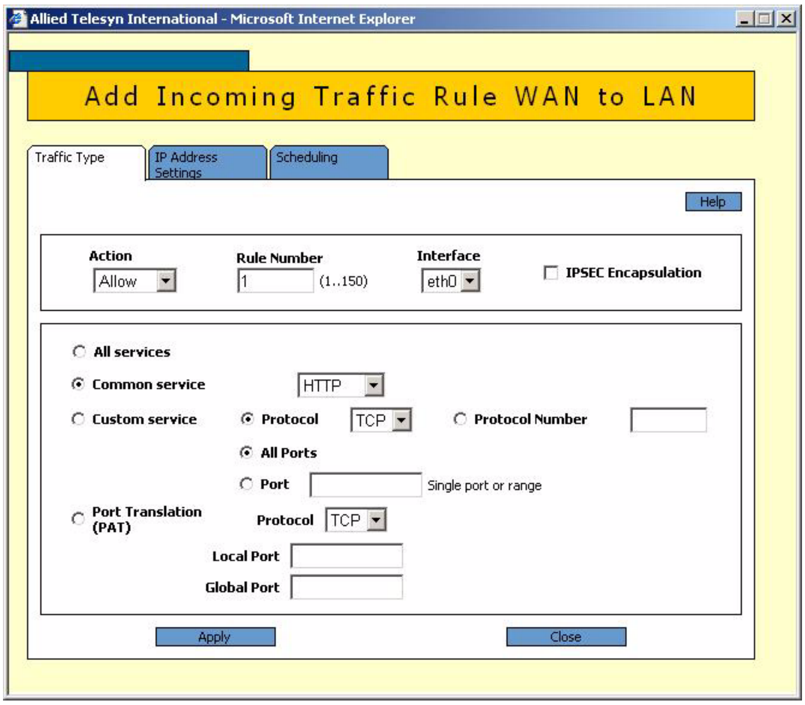
Adding a firewall rule

Clicking on the **Add** button displays a window, similar to Figure 13 on page 14, in which you can create new rule definitions. This window is similar for each of the policy/direction combinations as follows:

- WAN to LAN
- LAN to WAN
- WAN to DMZ, and
- DMZ to LAN.

Note that the LAN to WAN and DMZ to LAN combinations don't have port translation options.

Figure 13: An example of the Add Traffic Rule window


Allied Telesyn International - Microsoft Internet Explorer
Add Incoming Traffic Rule WAN to LAN
Traffic Type
IP Address Settings
Scheduling
Help
Apply
Close

Action: Allow

Rule Number: 1 (1..150)

Interface: eth0

☐ IPSEC Encapsulation

○ All services

● Common service: HTTP

○ Custom service: ● Protocol: TCP ○ Protocol Number

● All Ports

○ Port: Single port or range

○ Port Translation (PAT): Protocol: TCP

Local Port

Global Port

There are three tabs on this window:

- Traffic type.
- IP address settings.
- Scheduling.

To read about the default behaviour of the firewall and firewall policies in detail, refer to "*Understanding the firewall's behaviour*" on page 19.

Traffic Type tab

The traffic type tab enables you to set the general properties of a particular firewall rule as shown in Figure 13. The properties and their meanings are described in Table 3.

Table 3: Traffic type properties and their meanings

Property	Meaning
Action	There are three types: ◆ Deny - block matching traffic ◆ Allow - allow matching traffic to pass through the firewall, and allow the creation of new TCP/UDP sessions that match the rule ◆ NoNAT - the same effect as Allow, but has the added feature that NAT will not be applied to the packets, even if NAT is defined on the policy to which the rule is applied.
Rule Number	This is not just an ID number for the rule but also specifies the order in which rules will be used, i.e. an incoming packet is compared against the firewall rules in the order defined by their Rule Numbers. The action applied to the packet will be the action defined by the FIRST rule that matches the packet. If no rules match the packet, the applied action will be the default action for the particular direction of the packet, Public-to-Private or Private-to-Public.

Table 3: Traffic type properties and their meanings

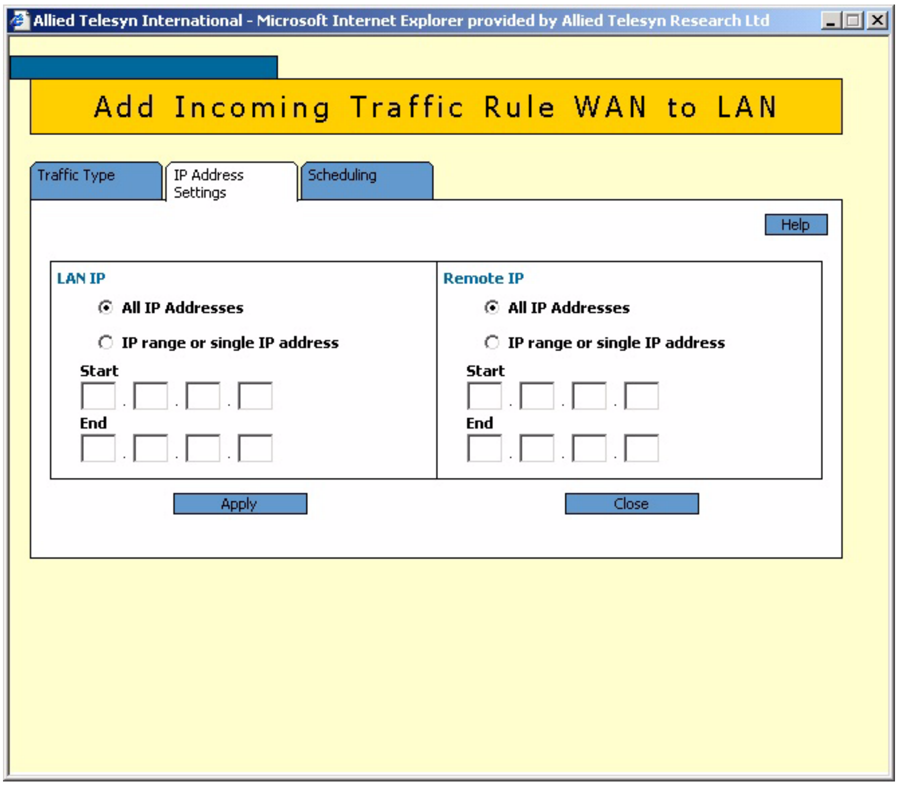
Property	Meaning
Interface	This is the interface to which the rule will be applied. The rule will apply to packets entering the router via this interface and leaving via another interface of the relevant policy.
IPSEC Encapsulation	Specifies whether or not the rule only applies to packets that arrived into the router IPSEC encapsulated and were decapsulated by the IPSEC engine on the router, **Note** that this checkbox is NOT relevant to the case of IPSEC encapsulated packets that are simply being forwarded through the router in encapsulated form. It is only relevant to packets that have been decapsulated, or that will be encapsulated, by the router itself. This checkbox is most often used in combination with the NoNAT action as the IPSEC encapsulated packets are frequently being tunnelled from one private LAN to another, so NAT is not relevant to them.
Protocol/Port Number	There are four mutually exclusive radio buttons. ◆ All services - No restriction. All protocol types and all TCP/UDP port numbers match this rule. ◆ Common service - This allows you to choose from a dropdown list of common TCP and UDP services such as HTTP, DNS, FTP, TFTP. ◆ Custom service - This allows you to specify a protocol and/or port number in the most general fashion. You can either choose the protocol from a dropdown list of well-known protocols such as TCP, UDP, GRE, IPSEC, or specify the protocol number. If you specify UDP or TCP, then it you can also specify the particular port numbers to which the rule applies - either 'all ports' or a specified range of ports. ◆ Port Translation - This option is significantly different to the three above. If you choose this option, packets will not only be forwarded, they will also have static NAT applied to them. You can specify the protocol to match, either UDP or TCP, and the port translation to carry out - from **Global Port** to **Local Port**. Port translation can only be specified for rules being applied to a public interface.

IP Address Settings tab

The IP address settings tab enables you to specify the source and destination IP address to which the rule applies, as shown in Figure 14 on page 16.

Note the titles of the left-hand and right-hand group boxes in this window. The titles may change depending on the policy and direction making it clear which devices the IP addresses belong to. In the example window shown in Figure 14 on page 16, LAN IP refers to the IP address of the device on the private LAN, and Remote IP refers to the IP address of the device out on the Internet.

Figure 14: An example of the IP Address Settings window



Allied Telesyn International - Microsoft Internet Explorer provided by Allied Telesyn Research Ltd

Add Incoming Traffic Rule WAN to LAN

Traffic Type | IP Address Settings | Scheduling

Help

LAN IP

● All IP Addresses

○ IP range or single IP address

Start

End

Remote IP

● All IP Addresses

○ IP range or single IP address

Start

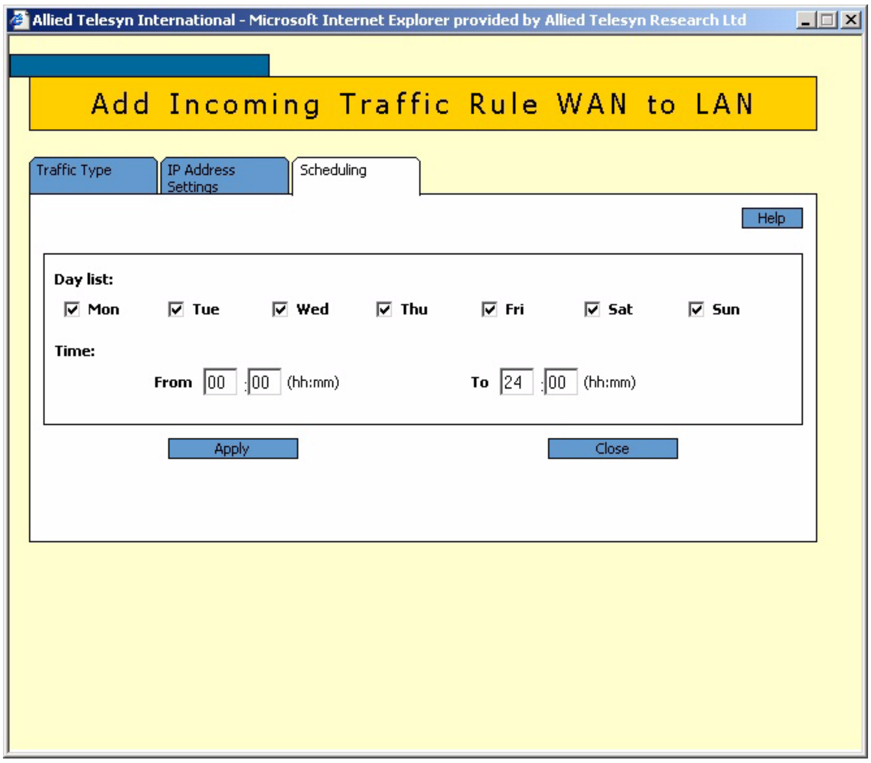
End

Apply Close

Scheduling Tab

The scheduling tab enables you to specify the days of the week, and hours of the day in which the firewall rule is active, as shown in Figure 15.

Figure 15: An example of the scheduling tab window



Allied Telesyn International - Microsoft Internet Explorer provided by Allied Telesyn Research Ltd

Add Incoming Traffic Rule WAN to LAN

Traffic Type | IP Address Settings | Scheduling

Help

Day list:

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

Time:

From 00 : 00 (hh:mm) To 24 : 00 (hh:mm)

Apply Close

Setting the time

The time you specify for **From** must be earlier than the time you specify for **To**, e.g. if you enter "08:00" in From and "17:31" in To, the rule will apply from 8:00am until 5:31pm.

Time periods begin and end at midnight. Therefore, to apply the rule to a time period between a given time and midnight, enter the time in From, and leave To blank, e.g. if you enter "17:31" in From, the rule will apply from 5:31pm until midnight. To apply the rule to a time between midnight and a given time, enter the time in To, and leave From blank, e.g. if you enter "08:00" in To, the rule will apply from midnight until 8:00am. To apply the rule overnight, e.g. from 17:31 to 08:00, you need two rules.

Configuring firewall events and alarms

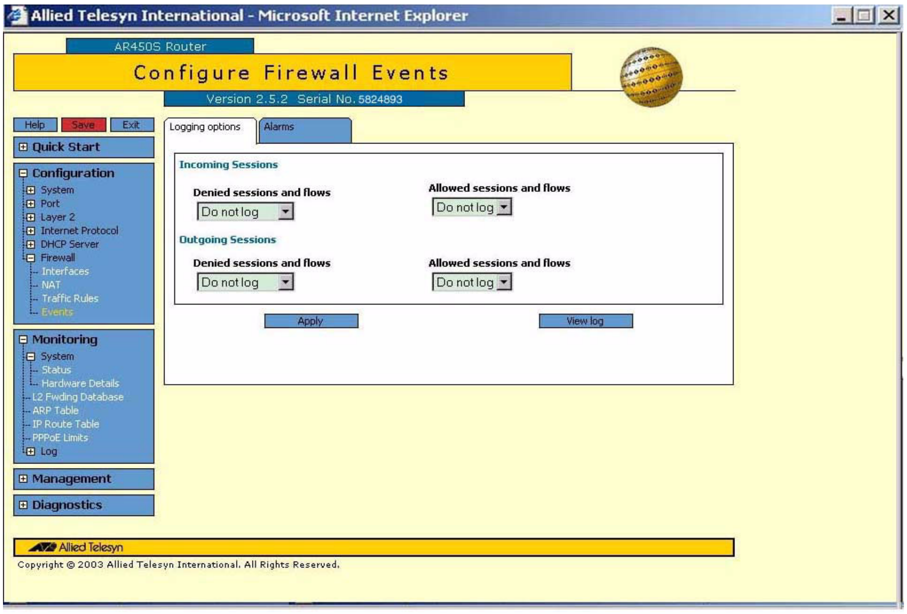
The last item in the Firewall submenu is Events. The Events menu item enables you to set some parameters that are general to the Firewall module as a whole. These are not policy-specific parameters.

Clicking **Events** displays the Configure Firewall Events screen, as shown in Figure 12. This screen shows two tabs, logging options and alarms.

Logging options tab

The Logging options tab allows you to determine which types of events will be recorded into the router log. You can log the start time and beginning of flow of allowed inbound and/or outbound flows. You can also log deny events on inbound and/or outbound packets.

Figure 16: An example of the firewall events logging options window



Incoming Sessions

Denied sessions and flows: Do not log

Allowed sessions and flows: Do not log

Outgoing Sessions

Denied sessions and flows: Do not log

Allowed sessions and flows: Do not log

Copyright © 2003 Allied Telesyn International. All Rights Reserved.

For each type of event that you decide to log, you have the option of a simple log entry, or a more comprehensive, 'extended' log entry.

Alarms tab

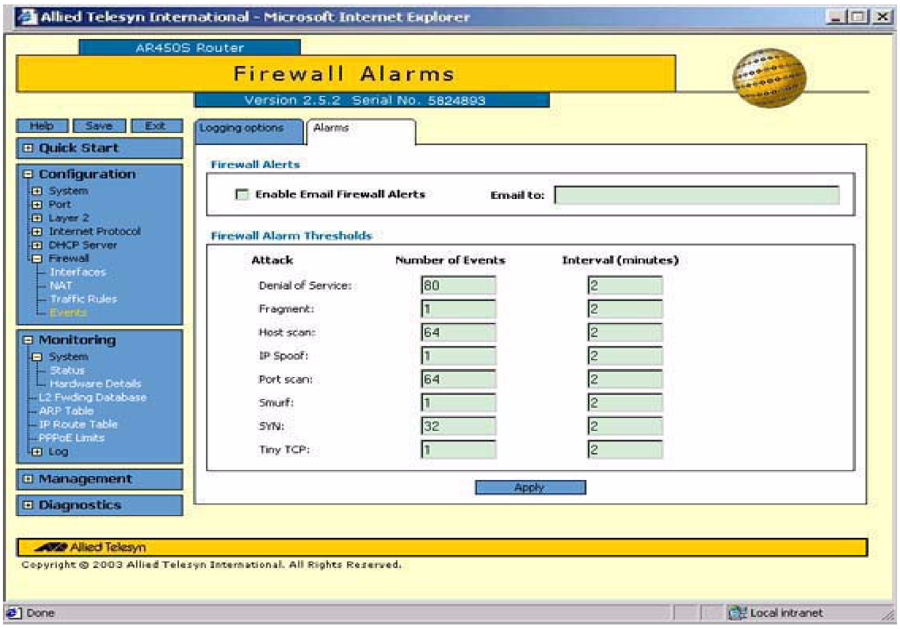
The Alarms tab allows you to set the thresholds at which the firewall module will decide that certain types of attack are underway. You are also able to provide an email address to which the firewall will send alarm messages every time any attack is detected. Most attacks consist of a stream of packets that follow a certain pattern.

> ***You can find descriptions and default settings for each type of attack in the GUI help.***

The threshold is set by specifying how many packets consistent with a certain attack type need to be received within a certain period before the firewall module will decide that an attack is occurring.

> ***You should not change the Alarm Thresholds unless the current thresholds are not working for your network. Contact your nearest authorised Allied Telesyn reseller or distributor for more information and help regarding these thresholds.***

Figure 17: An example of the firewall alarms window



Firewall Alerts

□ Enable Email Firewall Alerts Email to:

Firewall Alarm Thresholds

Attack	Number of Events	Interval (minutes)
Denial of Service:	80	2
Fragment:	1	2
Host scan:	64	2
IP Spoof:	1	2
Port scan:	64	2
Smurf:	1	2
SYN:	32	2
Tiny TCP:	1	2

Understanding the firewall’s behaviour

This section gives extra information to support the GUI configuration description, because to understand which rules you need to create, you need to understand the default behaviour of the firewall and firewall policies. The default behaviour of the firewall policies is as follows:

- Traffic from the public side (WAN) to the private side (LAN) is always denied unless specifically allowed.
- Traffic from the private side (LAN) to the public side (WAN) is always allowed unless specifically denied.
- If a policy has multiple public interfaces, then the default behaviour is to allow traffic that arrives at one public interface destined for an address beyond the other public interface.

The initial configuration created by the GUI has two policies:

- A LAN policy.
  Private interface LAN and public interfaces WAN and DMZ.
- A DMZ policy.
  Private interface DMZ and public interfaces LAN and WAN.

These policies correspond to the following firewall commands.

```
enable firewall
create firewall policy="guidmz"
create firewall policy="guilan"
add firewall policy="guidmz" int=eth1 type=private
add firewall policy="guidmz" int=vlan1 type=public
add firewall policy="guidmz" int=eth0 type=public
add firewall policy="guilan" int=vlan1 type=private
add firewall policy="guilan" int=eth1 type=public
add firewall policy="guilan" int=eth0 type=public
```

Given the default behaviour of the firewall, the default behaviour of traffic going to and from the LAN and DMZ policies can be summarised as shown in Table 4 on page 19, and Table 5 on page 20.

Table 4: LAN Policy

	To	**To**	**To**
From	**LAN - Private**	**DMZ - Public**	**WAN - Public**
LAN - Private	Not applicable	Allow	Allow
DMZ - Public	Disallow	Not applicable	Allow
WAN - Public	Disallow	Allow	Not applicable

Table 5: DMZ Policy

	To	To	To
From	**LAN - Public**	**DMZ - Private**	**WAN - Public**
LAN - Public	Not applicable	Disallow	Allow
DMZ - Private	Allow	Not applicable	Allow
WAN - Public	Allow	Disallow	Not applicable

You can see these two policies conflict in their opinion as to whether traffic should be allowed between the LAN and DMZ interfaces. The “law” in such cases of conflict is:

'If ANY of the policies state that packets between a particular pair of interfaces should be disallowed, then they will be disallowed".

The effect of these policies is that traffic may only pass from LAN to WAN and from DMZ to WAN. All other traffic will be disallowed.

Adding the rule shown below has the effect that the DMZ policy will allow *all* traffic from LAN to DMZ.

```
add firewall poli="guidmz" rule=50 access=allow int=vlan1 protocol=ALL
```

Given that the LAN policy also allows *all* traffic from LAN to DMZ, and *all* traffic from LAN to WAN, the two policies thereby unanimously agree that those traffic flows should be allowed.

Hence, the default behaviour of the initial firewall configuration created by the GUI is shown in Table 6.

Table 6: Default configuration policies

	To	To	To
From	**LAN**	**DMZ**	**WAN**
LAN	Not applicable	Allow	Allow
DMZ	Disallow	Not applicable	Allow
WAN	Disallow	Disallow	Not applicable

Therefore, it is only necessary to create further firewall rules if the desire is to change the behaviour of the firewall from that shown in Table 6.

For more information about the GUI, and about the Firewall, see the GUI Help, your AR450S User Guide and Software Reference, or contact your nearest authorised Allied Telesyn reseller or distributor.