



Allied Telesyn

240E ADSL Router

IPSEC passthrough howto on the 240E

Document version 1.2

Important

This guide is written to help get you up and running as quickly as possible with a standard IPSEC connection running through the 240E. To allow a UDP IPSEC connection the standard ports are protocol UDP port 2746.

This guide complements the NZ 240E Quickstart Guide available with the 240E router or on the <http://www.at-nz.co.nz> website.

The full product manual can be downloaded from:

<http://www.at-nz.co.nz/products/adsl.html>

Latest New Zealand Quick Start documentation and SW updates can be downloaded from:

<http://www.at-nz.co.nz/products/adsl.html>

Contents Page

240E ADSL Router	1
IPSEC passthrough howto on the 240E	1
Important	2
Contents Page	3
Default IP and management settings for New Zealand	4
Preparation.....	4
IP Settings for Clients.....	4
For windows 95/98/ME.....	4
For Windows 2000/XP (see Figure 1).....	4
Information on IPSEC/VPN/ADSL	5
Connecting to the 240E	5
Opening a web connection	5
Example use of a 240E in a IPSEC VPN	5
.....	5
Finding the 240E's Public IP.....	6
NAT Setup.....	6
Enabling and Setting up NAT	6
Define NAT interfaces	7
ISAKMP pinhole (reserve mapping).....	9
IPSEC pinhole (reserve mapping)	9
Saving Settings	9
Adding Firewall Functionality (for advanced users).....	11
ISAKMP Firewall Filter	12
IPSEC (protocol 50) Firewall Filter	13
UDP IPSEC Firewall Filter – Only use if necessary	13
Saving Settings	14

Default IP and management settings for New Zealand

Router IP address 192.168.1.1
 Router Subnet Mask 255.255.255.0

Management and
 configuration access

User name manager
 Password friend
 For web and telnet access

Preparation

- Network card (NIC) installed on your PC
- TCP/IP protocol is installed for the network card
- Details from your ISP
 - Login name and password
 - DNS server(s) ip address(s)

IP Settings for Clients

For windows 95/98/ME

- From your windows desktop right click on the “**Network Neighbourhood**” icon. Select **Properties**.
- From the **Configuration** tab select TCP/IP -> xxx where xxx refers to the network card (NIC) in the PC.
- Click **properties**.
- Select the **IP address tab**.
- Click the option to **Specify an IP address**.
- Enter **IP address** = 192.168.1.2
Subnet Mask = 255.255.255.0
- Click on the **Gateway** tab.
- Set the **New Gateway** = 192.168.1.1 Click the **Add button**.
- Click on the **DNS** tab, click **enable DNS**
- Enter your ISP’s DNS server IP address. Click the **Add button**.
- If you don’t know the ISPS DNS server use 203.96.91.1
- Click **OK** then **OK** to save the settings.
- You may be asked to **restart** the PC. Click **Yes**

For Windows 2000/XP (see Figure 1)

- **Settings - Control panel – Network Connections**
- **Click Properties**
- Open **Local Area Network Connections**. **Double Click** Internet protocol (TCP/IP)
- Select Use the following IP address
- **IP address** = 192.168.1.2
Subnet mask = 255.255.255.0
Default Gateway = 192.168.1.1
- Select Use the following DNS
Preferred DNS = 192.168.1.1
Alternate DNS = 203.96.91.1

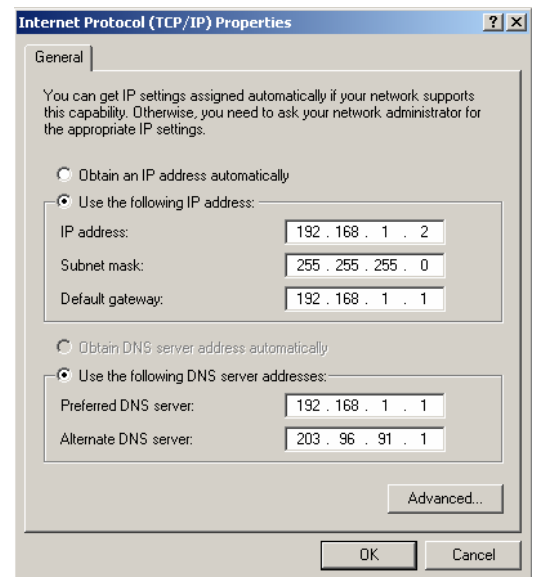


Figure 1

Information on IPSEC/VPN/ADSL

IPSEC on a 300,400,700,rapier series switch/router

<http://www.alliedtelesyn.co.nz/documentation/arrouter/241/pdf/ipsec.pdf>

IPSEC RFC/ITF

<http://www.ietf.org/html.charters/ipsec-charter.html>

Howstuffworks.com VPN

<http://www.howstuffworks.com/vpn.htm>

Howstuffworks.com ADSL

<http://www.howstuffworks.com/dsl.htm>

Connecting to the 240E

Opening a web connection

To run the AT-AR240E web interface, ensure that your Web Browser is Microsoft® Internet Explorer 5.0 (or later) and disable any proxy settings on your Web Browser. Enter the IP address (*with the http:*) <http://192.168.1.1:8080> in the browser's Open Location windows and press **Enter**. You will be required to login as follows:

Username = manager

Password = friend

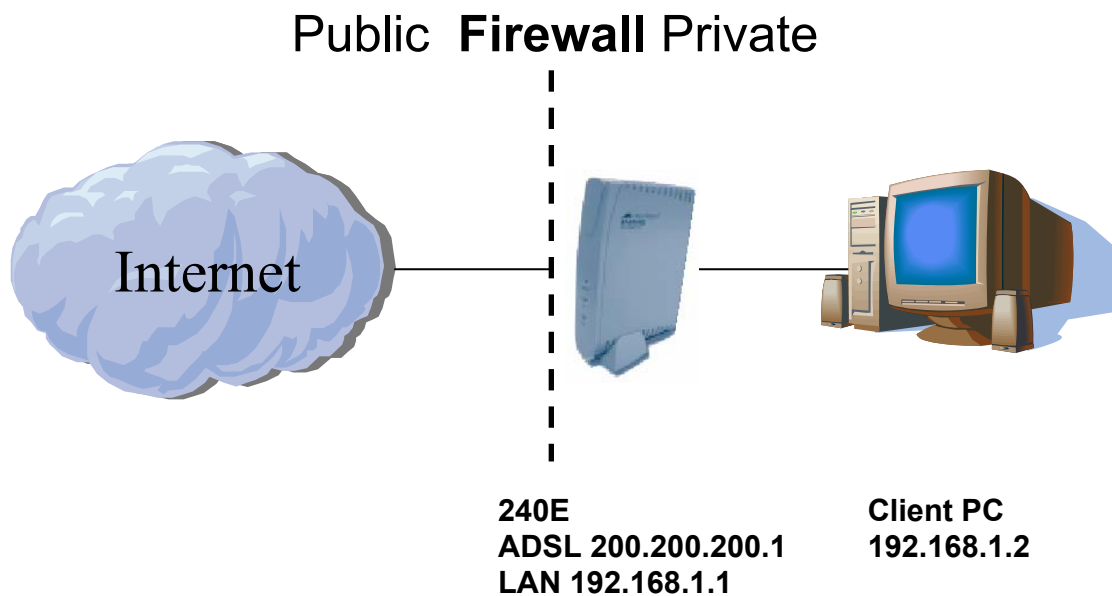
Assuming that the 240 has the following completed

1.1. **ADSL** connection has been setup

If not then please see **NZ 240E quick start guide**

<http://www.at-nz.co.nz/products/adsl.html>

Example use of a 240E in a IPSEC VPN



The PC is running a VPN client and connects to a corporate VPN via the internet. The 240E can pinhole to a VPN concentrator like the AR-320S using a similar setup. Please contact a Allied Telesyn Reseller for more info.

Finding the 240E's Public IP

1. To find the public ip address on the 240E press the **blue "Status"** Button
2. Click on the **yellow "internet"** button to display your **internet IP address** and **DSL Connection rate**. Write you're your **public ip address** below for later when you need to set up pinholes in the NAT. **Public ip = _____**

AT-AR240E - Microsoft Internet Explorer

Welcome to your

Allied Telesyn AR 240

Software Release 1-0-0

Status

ADSL

LAN - USB

IP Routing

DHCP

DNS

Security

Users Management

Error Log

Save Configuration

Software Update

Restart

Interface name: internet

IP interface

IP address (via DHCP)	210.54.144.24
-----------------------	---------------

Public IP address

DSL interface

Port Name	atm
Connected	true
Tx Bit Rate	800000
Rx Bit Rate	5568000
Tx Cell Rate	1886
Rx Cell Rate	13132
Modem State	Showtime (LO)
Modem Operational Mode	G.DMT
Modem Configured Mode	multi

DSL connection speed

Connection mode
G.DMT / G.Lite in NZ

ATM connection:

Port name	atm	Active	TRUE
Rx VPI	0	Tx VPI	0
Rx VCI	100	Tx VCI	100
Rx packets	14	Tx packets	16
Rx bad packets	0	Tx bad packets	0
QOS Class	ubr	Peak Cell Rate	2000
Sustainable Cell Rate	0	Maximum Burst Size	0

PPPoA parameters:

Status	open for IP, sent 16, received 14
LLC headers	false
HDLC headers	false
Authentication	pap
Username	user@jetstreamgames.co.nz

Allied Telesyn

Copyright © 2002 Allied Telesyn. All rights reserved.

NAT Setup

Enabling and Setting up NAT

Step 1 Press the blue **"Security"** button on the left.

NAT has to be enabled between the internal and the external interfaces.

Step 2 Click the **enabled** radio button at the top and press yellow **apply** button. The screen should change from the screen below (figure 2) to the one below that (figure 3).

Security	
Enabled <input checked="" type="radio"/>	Disabled <input type="radio"/>
Firewall	Configure
Dynamic Port Opening	Configure
Attack Detection and Blocking	Configure
NAT	Configure
Apply	

Figure 2

Security	
Enabled <input checked="" type="radio"/>	Disabled <input type="radio"/>
Firewall	Configure
Dynamic Port Opening	Configure
Attack Detection and Blocking	Configure
NAT	Configure
Apply	

Interfaces List		
Name	Type	Action
<input type="text" value="internet"/>	<input type="text" value="external"/>	ADD

Figure 3

Define NAT interfaces

Step 3 You can now define security interfaces from the drop down boxes. Define the security interfaces as follows: (see Figure 4)

Interfaces List		
Name	Type	Action
lan	internal	Delete
usb	internal	Delete
internet	external	Delete
<input type="text" value="internet"/>	<input type="text" value="external"/>	ADD

Figure 4

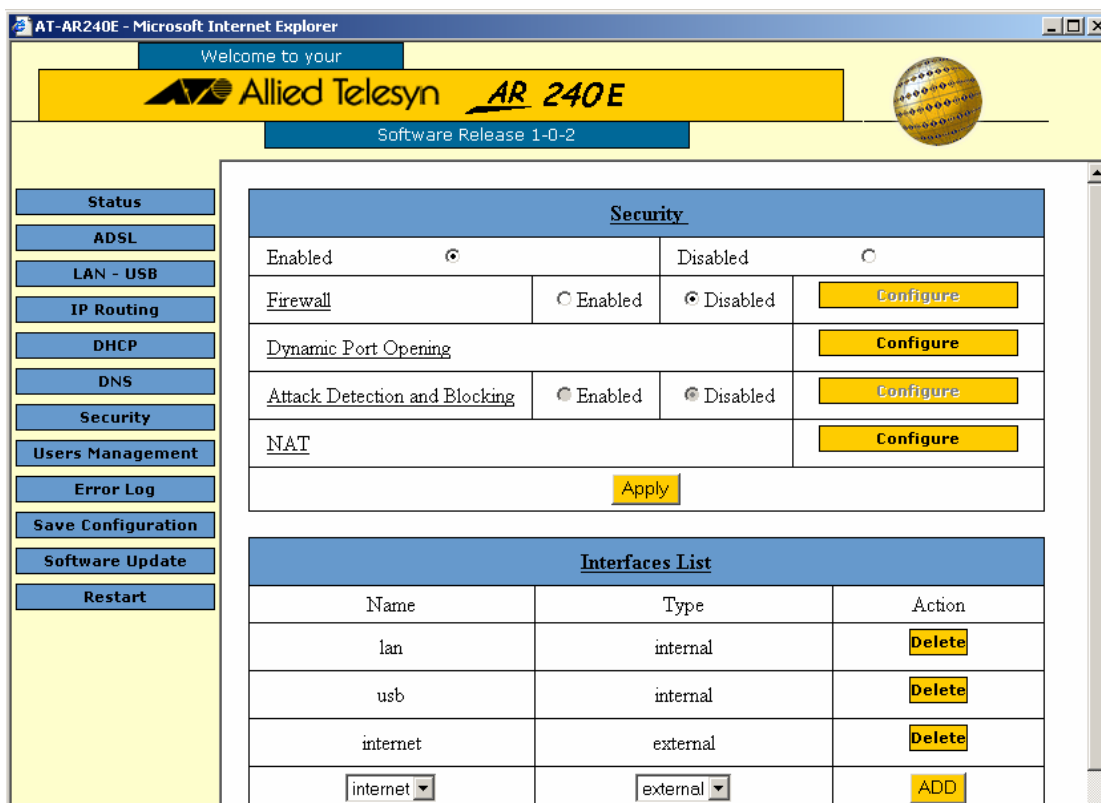


Figure 5

1. Now click on the yellow **configure** button for NAT and within the NAT window click **configure** for the "internet" row. Then click, "**enable NAT to internal interfaces**". The screen below appears and internet browsing should now be possible.

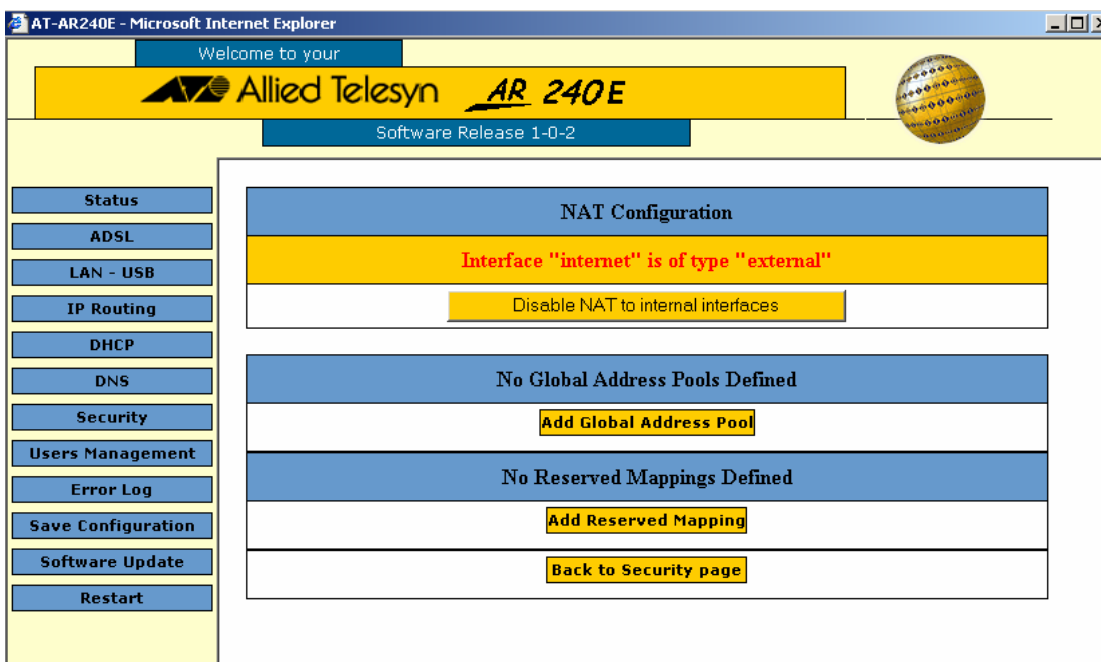


Figure 6

2. Now you need to add pinholes for the IPSEC connection. Click on the "**Add Reserve Mapping**". See figure 6
3. Press the yellow "**Configure**" button.

ISAKMP pinhole (reserve mapping)

Used for “shared secret” key exchange.

4. First pinhole is for the ISAKMP traffic. Input the **Global IP** the **Internal IP**, Protocol **UDP** and **port number** is **500** and press **apply**.

Reserved Mapping Configuration			
Add Reserved Mapping on interface:internet			
Global IP Address	Internal IP Address	Protocol	Port Number
200 . 200 . 200 . 1	192 . 168 . 1 . 2	udp	500
Apply			
Return to NAT Configuration page			

Figure 7

IPSEC pinhole (reserve mapping)

5. Second pinhole is for the IPSEC encrypted traffic. Input the **Global IP** the **Internal IP**, Protocol **IPSEC** and **port number** is **0** and press **apply**.

Reserved Mapping Configuration			
Add Reserved Mapping on interface:internet			
Global IP Address	Internal IP Address	Protocol	Port Number
200 . 200 . 200 . 1	192 . 168 . 1 . 2	ipsec	0
Apply			
Return to NAT Configuration page			

Figure 8

NOTE: Only if you have setup your unit to use UDP IPSEC

UDP IPSEC pinhole – Use only if necessary

9. The ISAKMP “pinhole” is needed as well as IPSEC UDP “Pinhole” for IPSEC over UDP. Input the **Global IP** the **Internal IP**, Protocol **UDP** and **port number** is **2746** and press **apply**. The ports for UDP IPSEC differ between different vendors but the standard port is 2746.

Note: your global ip address can be obtained from the status (home) page and then click on the internet adsl definition. See page 6

Saving Settings

1. Click on the blue “**Save Configuration**” button. The screen will show Figure 9. Press the yellow “**Save**” button. The window will remain for up to a minute as the configuration is saved. Once the configuration is saved the screen will show Figure 10 and the 240E setup has finished.

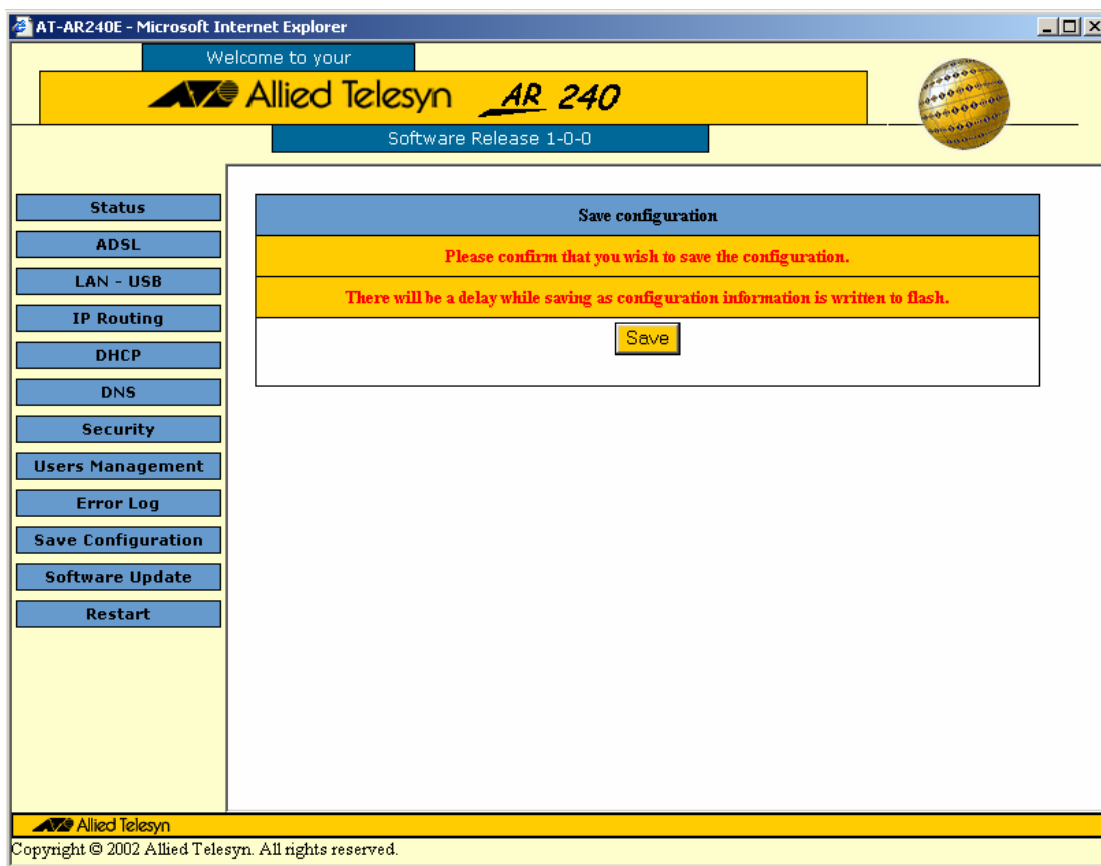


Figure 9

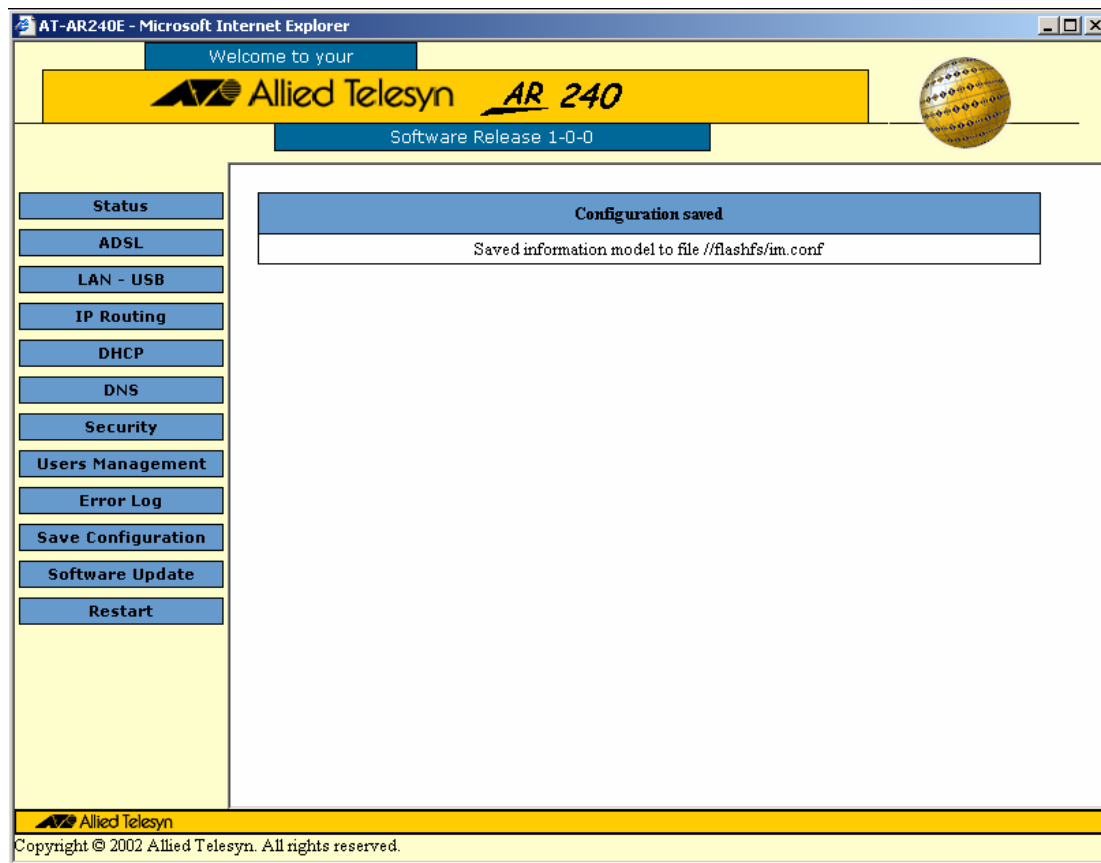


Figure 10 Configuration Saved

Adding Firewall Functionality (for advanced users)

To add firewall functionality the following steps are required.

1. **enable** firewall on the security page and then press **apply**.

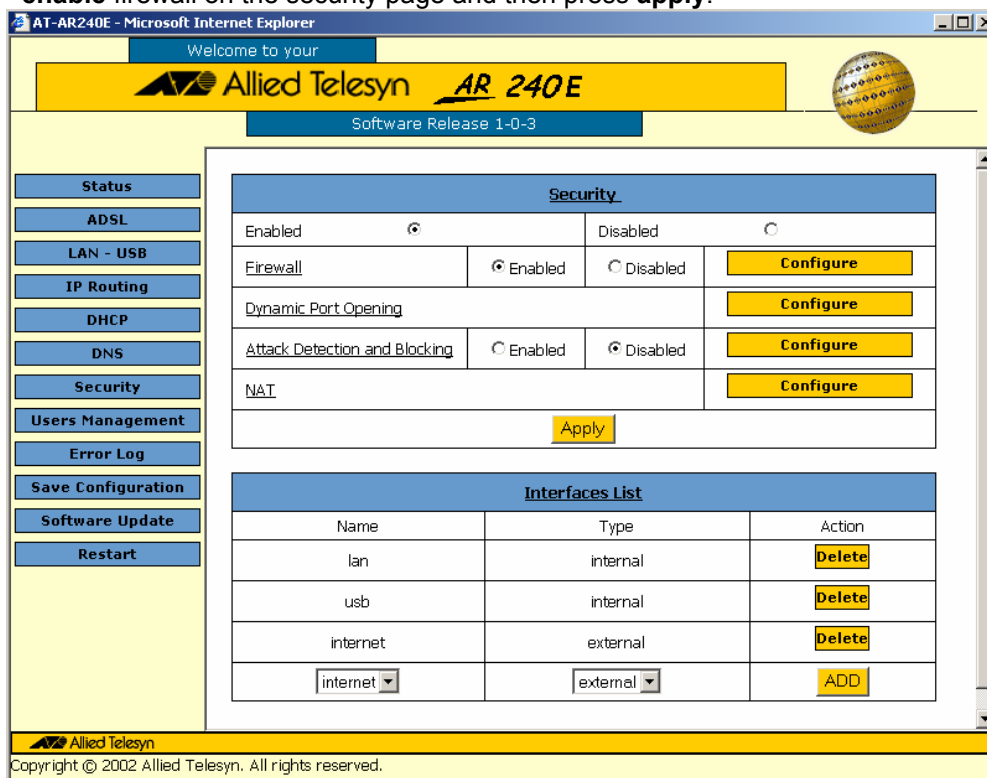
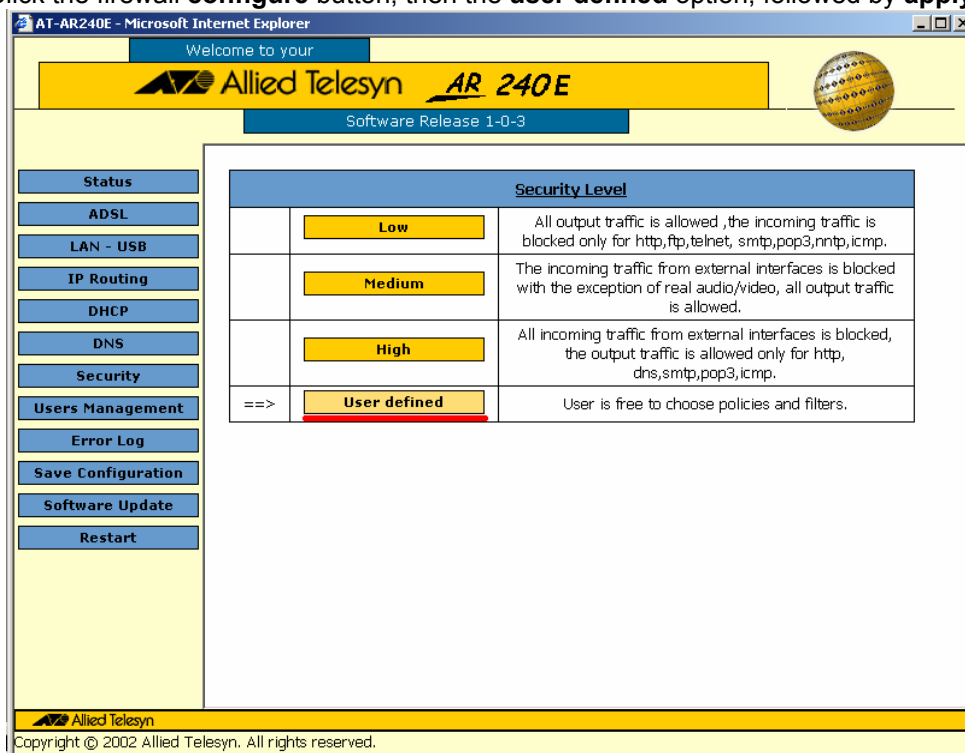


Figure 11

2. Allow all out going connections and incoming pin hole entries
3. Click the firewall **configure** button, then the **user defined** option, followed by **apply**.



- Click on the “Internal – External “ policy **configure** button.

Note: Even though the DMZ policies are not used in the below example they SHOULD NOT be removed.

For a typical network it is recommended that the user defined configuration be made more flexible by deleting all filters(see figure 13) and re-adding them as follows: Add the in-bound filters to match the NAT pin holes. Section 5 and 6.

Note: Filter order is important. If corresponding filter entries are required to match In-coming NAT entries, this must be done before the global entries which allow every thing out and block all remaining incoming connection requests.

Firewall Port Filters	
Firewall Port Filters: external-internal	
No Filters Defined	
Add TCP Filter	
Add UDP Filter	
Add Filter for Other Protocol	
Return to Policy List	
Back to security page	

Figure 13

ISAKMP Firewall Filter

- Click the yellow “Add UDP filter” button.
 Start Port: 500
 End Port: 500
 Inbound: Allow
 Outbound: Allow
 Then press the yellow “Apply” button (see Figure 14)

Firewall Add UDP Port Filter				
Firewall Add UDP Port Filter: external-internal				
Protocol	Port Range		Direction	
Type	Start	End	Inbound	Outbound
UDP	<input type="text" value="500"/>	<input type="text" value="500"/>	<input type="text" value="Allow"/>	<input type="text" value="Allow"/>
Apply				
Return to Filter List				
Return to Policy List				
Back to security page				

Figure 14

IPSEC (protocol 50) Firewall Filter

- Click the yellow “Add filter of other protocol” button.

Protocol: 50
 Inbound: Allow
 Outbound: Allow

Then press the yellow “Apply” button (see Figure 15)

Firewall Add Generic Protocol Filter		
Firewall Add Generic Protocol Filter: external-internal		
Protocol	Direction	
	Inbound	Outbound
50	Allow	Allow
Protocol can be any Protocol Number or a Protocol Name. The following table lists all recognized names:		
	Protocol Number	Protocol Name
	1	ICMP
	2	IGMP
	3	GGP
	4	IP
	8	EGP
	9	IGP
	46	RSVP
	47	GRE
	50	IPSEC
	89	OSPF/IGP
	92	MTP
	94	IPIP
<input type="button" value="Apply"/>		

Figure 15

UDP IPSEC Firewall Filter – Only use if necessary

- Click the yellow “Add UDP filter” button.

Start Port:2746
 End Port: 2746
 Inbound: Allow
 Outbound: Allow
 Then press the yellow “Apply” button

- Click the yellow “Add TCP filter” button.

Start Port:1
 End Port: 65000
 Inbound: Block
 Outbound: Allow
 Then press the yellow “Apply” button

- Click the yellow “Add UDP filter” button.

Start Port:1
 End Port: 65000
 Inbound: Block
 Outbound: Allow
 Then press the yellow “Apply” button

- Click the yellow **“Add filter of other protocol”** button.
 Protocol: 1 (ICMP)
 Inbound: Block
 Outbound: Allow
 Then press the yellow **“Apply”** button .

Saving Settings

- Click on the blue **“Save Configuration”** button. The screen will show Figure 16. Press the yellow **“Save”** button. The window will remain for up to a minute as the configuration is saved. Once the configuration is saved the screen will show Figure 17 and the 240E setup has finished.

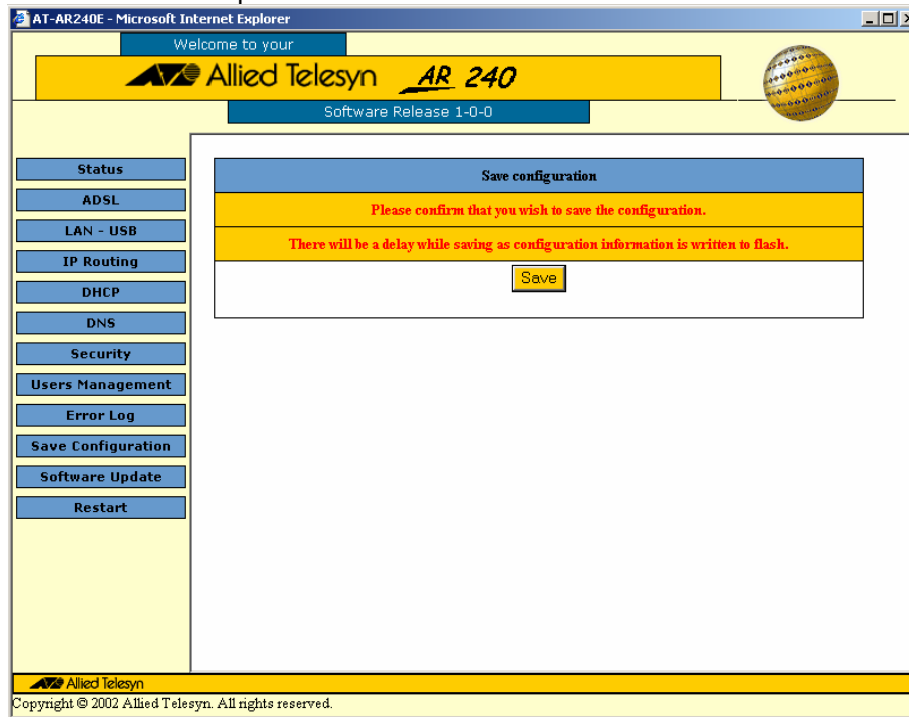


Figure 16

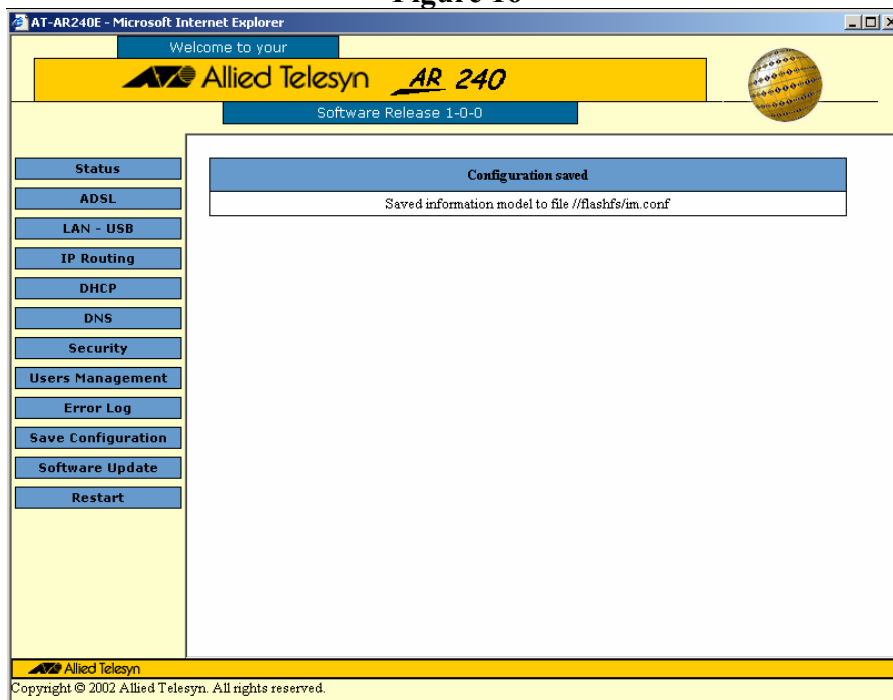


Figure 17 Configuration saved

Help

Always check that the router is installed properly. Check the website for information and how to troubleshoot the router. If you have difficulties contact your reseller or distributor for technical assistance relating to warranties, installation and operation. They will escalate the problem your having through the appropriate channels.

New Zealand Distributors



Connector Systems Ltd
5A Pacific Rse
Mt Wellington Auckland
Free Phone: 0508 Call CSL

WWW: <http://www.connectorsystems.co.nz>
Email: sales@connectorsystems.co.nz



Express Data NZ
Express Data NZ Ltd
Level 12, Microsoft House
3-11 Hunter Street
Wellington
Free Phone: 0800 336 427

WWW: <http://www.expressdata.co.nz>
Email: sales@expressdata.co.nz



Renaissance Ltd
92 Beachcroft Ave
Onehunga Auckland
Free Phone: 0800 800 905

WWW: <http://www.renaissance.co.nz>
Email: info@renaissance.co.nz

Allied Telesyn NZ Sales

Email: at-nz@alliedtelesyn.co.nz

Web: <http://www.at-nz.co.nz>

Phone: 04 566 4438 (Mon-Fri, 9am-4pm)