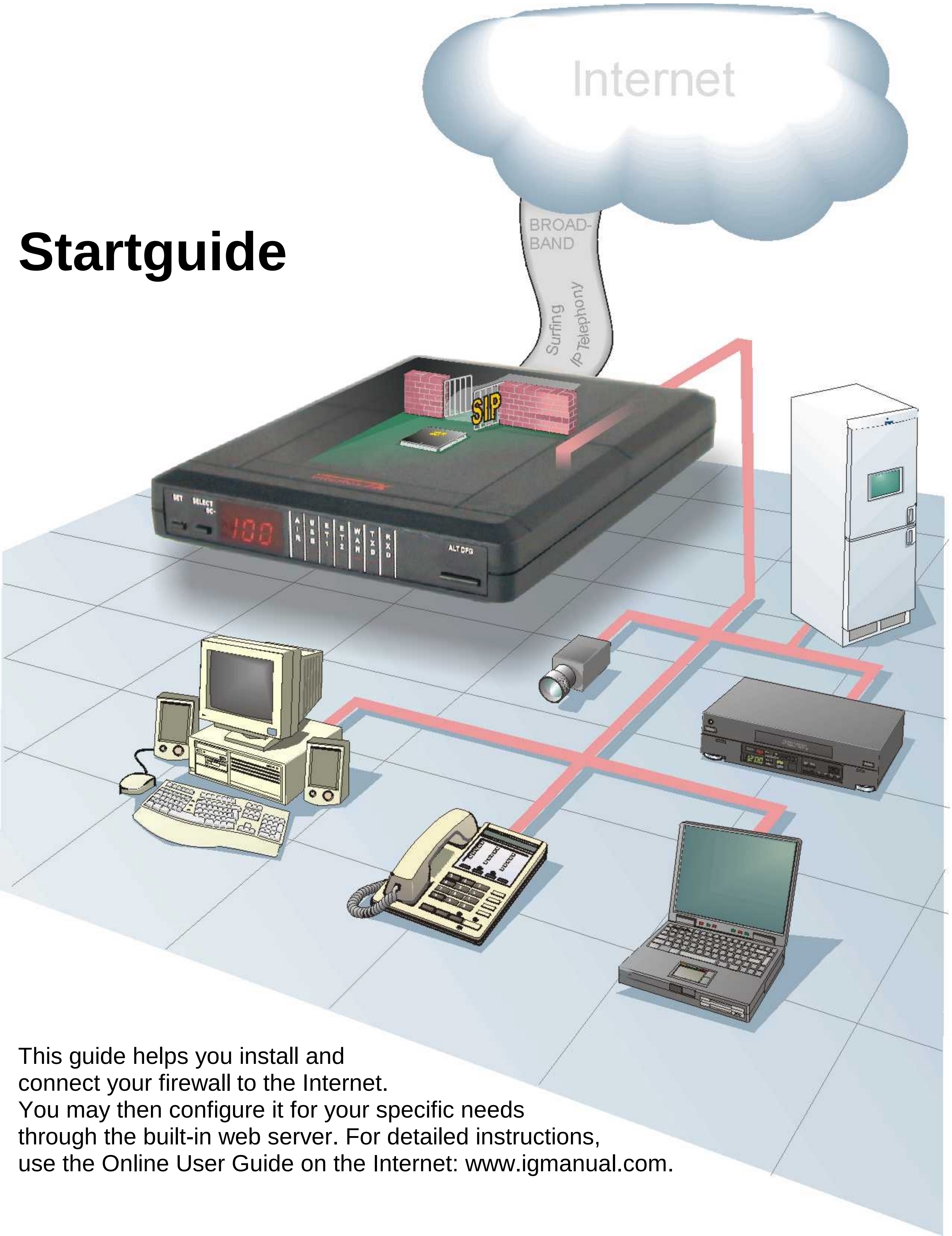
PF-EN-118-Rev.02E2

Startguide



This guide helps you install and
connect your firewall to the Internet.
You may then configure it for your specific needs
through the built-in web server. For detailed instructions,
use the Online User Guide on the Internet: www.igmanual.com.

Quick Start

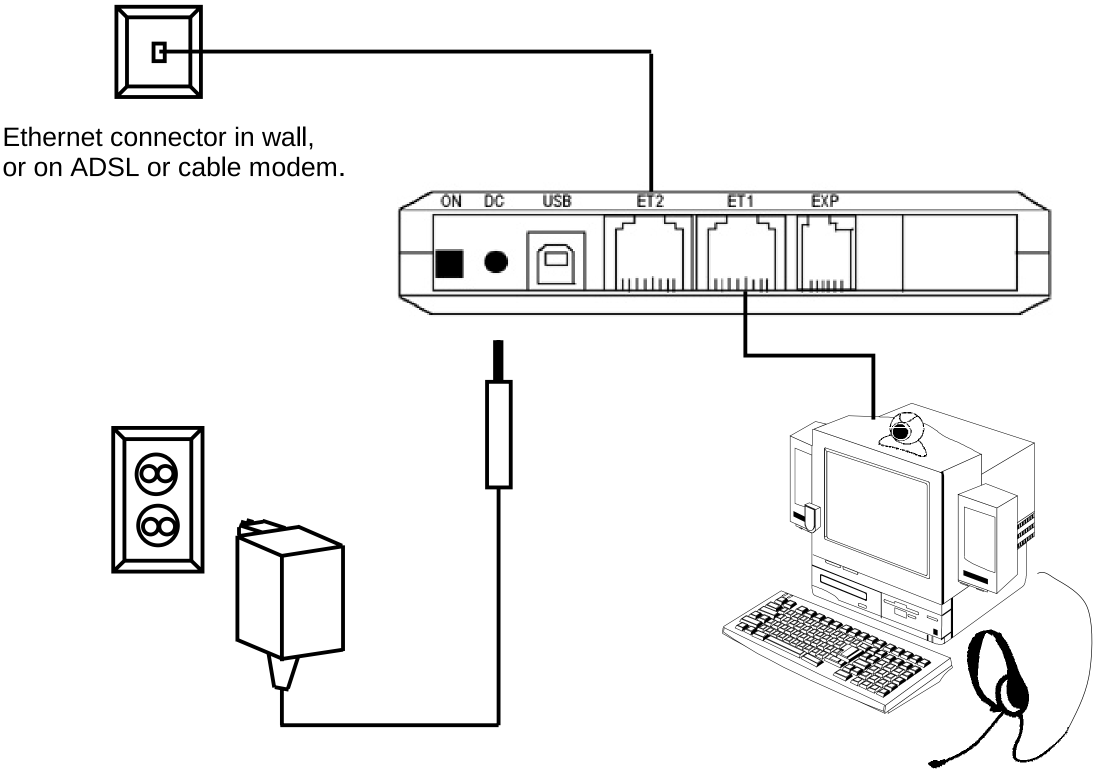
In most cases, the A, B, C steps on this page will get your firewall up and running.
If you run into problems you find the solution to the most common problems in this guide.

A

Hook up the Cables!

Note! Make sure your computer is turned off!

1. Connect the supplied black Ethernet cable between port **ET1** on the back of the firewall and the Ethernet port on your computer.
2. Use the other Ethernet cable to connect port **ET2** of the firewall to your broadband or WAN connection. *(The WAN connection is an RJ45 connector either directly in your wall, or on the back of the equipment (e.g. an ADSL-modem) delivering your broadband connection.)*
3. Connect the power adapter and push the **ON** switch on the rear of the firewall.

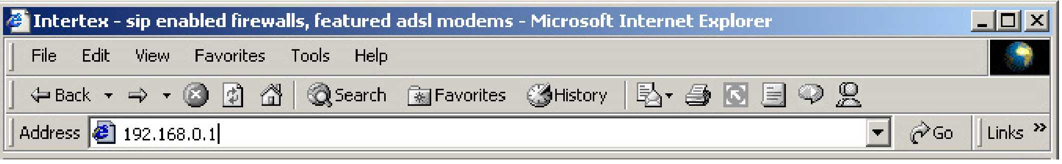


For information about how to connect a LAN, see page 7.

B

Surf into your Firewall!

1. Make sure you have a connection to the Internet (indicated by the WAN LED being lit).
2. Turn your pc on and start your web browser (i.e. Netscape or Internet Explorer).
3. Surf to your firewall by typing its default IP Address: **192.168.0.1** in the address field.



Intertex - sip enabled firewalls, featured adsl modems - Microsoft Internet Explorer

Address 192.168.0.1

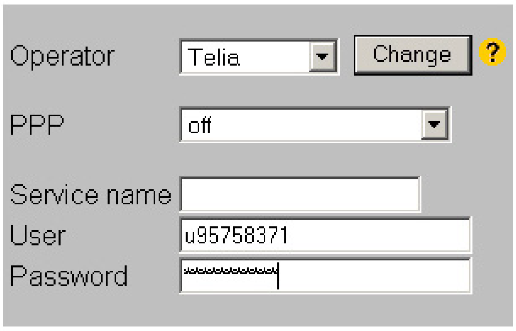
I don’t see the built-in web page! Why?

1. *Do you have an Ethernet card installed in your computer, is it properly configured? Refer to page 8!*
2. *Are the cables correctly connected? Both the **ET1** and **ET2** LEDS should be lit.*
3. *Reboot your PC and try again!*
4. *Is your PC and web browser properly configured? Refer pages 8 and 11!*
5. *Do you run another DHCP Server on your LAN? Refer to page 9!*
6. *Do you use static IP addresses on your LAN? Refer to page 10!*

C

Select operator!

1. Click **Login** on the first page of the web interface.
2. Enter login ”admin”, password ”admin”.
3. Click **Network** on the main menu.
4. Click **Operator, PPP and Keep-alive**.
5. Select national operator of your country from the list, and click **Change**.
6. If you have received any service name, user or password from your operator, enter them.
7. Click **Save**.



Operator Telia

PPP off

Service name

User u95758371

Password ***********

Congratulations! You are now connected to the Internet!

You may start surfing now! You may for instance try surfing to: www.intertex.se.

I don’t see any web pages! Why?

1. *Reboot your PC, allowing it to get fresh configuration data from the firewall, and try again!*
2. *Reboot your firewall and try again!*
3. *Is your firewall properly configured? Press* **ALT CFG** *on your firewall repeatedly until ”Hi” displays.*
4. *Is your web browser properly configured? Refer to page 11!*
5. *Test your Internet connection with the built-in diagnostic test. Refer to page 7!*

We recommend you to read the always up-to-date online user manual. You access it by clicking on **Online User Manual** on the first page on the firewalls web configuration pages. See page 14, for more information.

Overview – Front Panel

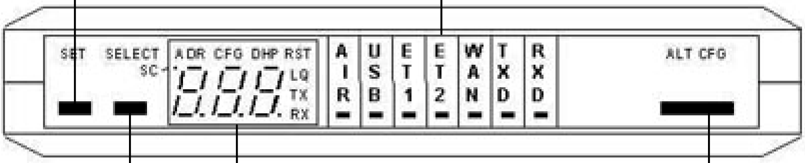
SET
Press once to see firmware version.

Keep pressed for 3 seconds to enter set-up mode: AD, CFG, DHP, RST and LQ.

Interface indicators:

On:	Interface is connected.
Off:	Interface is not used.
Flashing:	Data is sent or received.

AIR –	Wireless (Bluetooth or 802.11) (option)
USB –	Universal Serial Bus
ET1 –	Ethernet 1 (PC or LAN)
ET2 –	Ethernet 2 (WAN / broadband / Internet)
WAN –	Internet connection.
TXD –	Data is sent to the Internet.
RXD –	Data is received from Internet.



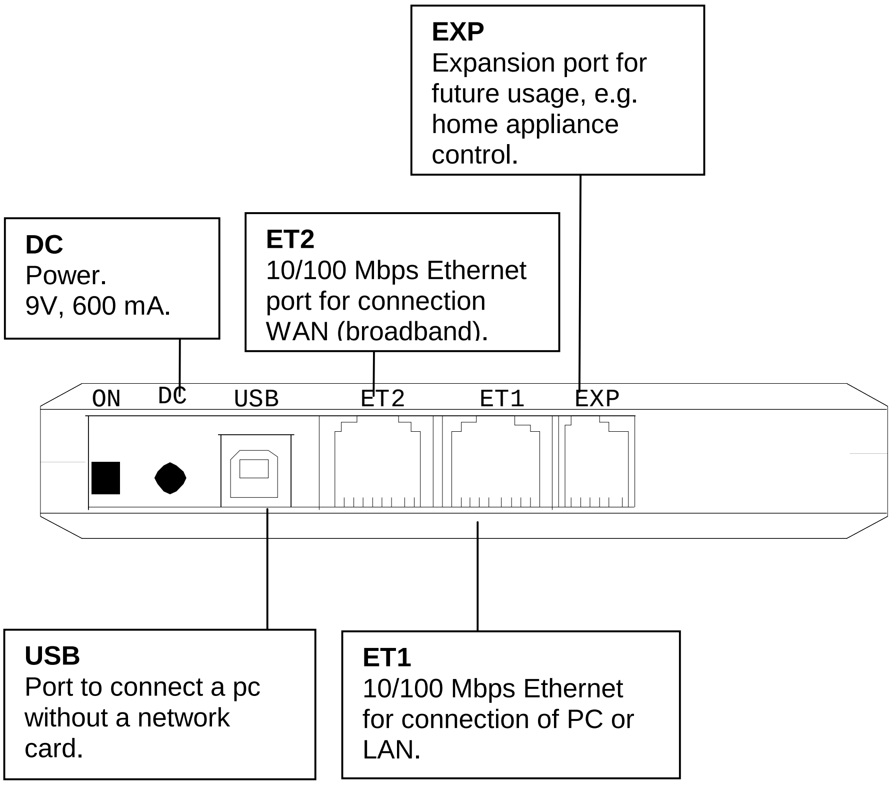
SELECT
Press to see Ethernet speed for ET1 and ET2. Keep pressed for 2 seconds to cancel your settings.

ALT CFG
Press to select firewall security profile.

AD	Show LAN IP addresses of the firewall.
CFG	Configure LAN IP addresses of the firewall.
DHP	Turn LAN DHCP server of the firewall on/off.
RST	Reset all configurations to factory defaults.
LQ	Diagnostic test.
TX,RX	Both lit: full duplex; Toggle: half duplex

Some models of the firewall do not have all the keys and LEDS described above.

Overview – Back Panel



EXP
Expansion port for future usage, e.g. home appliance control.

DC
Power.
9V, 600 mA.

ET2
10/100 Mbps Ethernet port for connection WAN (broadband).

USB
Port to connect a pc without a network card.

ET1
10/100 Mbps Ethernet for connection of PC or LAN.

Some models of the firewall do not have all the connections described above.

Package Details

The following items should be included in your box:

- Getting Started guide (this document).
- The firewall unit.
- Power adapter.
- 2 × Ethernet-cable (RJ45/RJ45, straight through).

If any of the items above are damaged or missing, please contact your retailer.

Note!

If you use your own Ethernet cables, make sure they are wired correctly:

- A straight-through cable must be used to connect the firewall to a PC.
- An Ethernet hub requires a crossover cable to connect the firewall (when the hub does not have a port marked "UPLINK" or similar).

Requirements

In order to set up and use your firewall you need:

- **For connection via Ethernet**: a PC with an Ethernet port or a local network (LAN) using TCP/IP.
- **For connection via USB**: a PC with Windows 98 / 2000 / Me / XP and an USB port.
- A web browser such as the Microsoft Internet Explorer or the Netscape Navigator, version 4 or later, installed on the PC.
- An RJ45 Broadband Internet Connection, from a wall connector, ADSL or Cable modem.

Getting Help

There are several ways to get information about the firewall:

- **Getting Started Guide** – This Getting Started guide helps you to install, configure and start using your firewall.
- **Built in Help** – Every configuration page on the built in web server has help texts that describe the different parameters. Just click the question marks.
- **Online User Manual** – Using the online manual, you will find the latest information tailored for your specific version of the firewall. You can access it via the link on the first configuration page of the firewall or directly at www.igmanual.com.
- **Support** – If you experience problems when installing or using the firewall that cannot be solved by the help indicated above, contact your retailer for assistance.

Detailed instructions

Do you have problems getting your firewall to work?
Read the installation tips and the detailed instructions on the following pages for help!

Connecting a Local Network (LAN)

If you have a Local Area Network (LAN) with several computers connected, you can connect the network hub to your firewall and allow all computers to share the Internet connection.
Usually you need a crossover Ethernet cable to connect the hub to port ET1 of your firewall. But if your hub has a port marked “UPLINK” or similar, you should use a straight Ethernet cable.

If your network uses dynamic IP-addressing (recommended), then the built-in DHCP server of your firewall will provide IP addresses to all PC:s on the LAN. Refer to page 9 for more information.

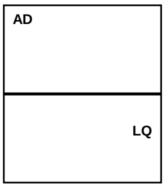
Does your network use static IP addresses? Refer to page 10 for information.

Diagnostic test

If you cannot access the Internet, your firewall can attempt to localise the problem.

Note! The diagnostic test facility is only available in models with keys and a display.

Start the diagnostic test like this:



1. Press and keep **SET** pressed 3 seconds to enter setup-mode.
2. Press **SELECT** 4 times until “LQ” is lit.
3. Press **SET**.

It takes a couple of seconds to perform the test. Any errors discovered are shown in the display. The diagnostic test can find multiple errors, press **SELECT** to flip through all error messages.

”E 1” to ”E 9” indicate errors in your external Internet connection:

E 1 No WAN Ethernet connection. Check the cable connected to ET2. Contact your broadband-supplier if the error remains.

E 2 No WAN DHCP server found. Check configuration according to page 11. Reboot your firewall. Contact your Internet Service Provider (ISP) if the error remains.

E 3 No Gateway found. Check configuration according to page 11. Reboot your firewall. Contact your Internet Service Provider (ISP) if the error remains.

E 4 No DNS server found. Check configuration according to page 11. Reboot your firewall. Contact your Internet Service Provider (ISP) if the error remains.

E 5 No Internet connection. You do have a connection to your ISP, but they have no Internet connection for the moment. Contact your Internet Service Provider (ISP) if the error remains.

”E11” to ”E19” indicate error in your local network:

E11 No Ethernet link. Check the cable connected to port ET1.

E12 No DHCP addresses requested. The DHCP server of the firewall is on, but no PC:s on the LAN have requested addresses. This *may* be OK, but check your settings, see page 9.

E13 No Ethernet packets at all received.
This *may* be OK, but check your settings, see pages 8 and 11.

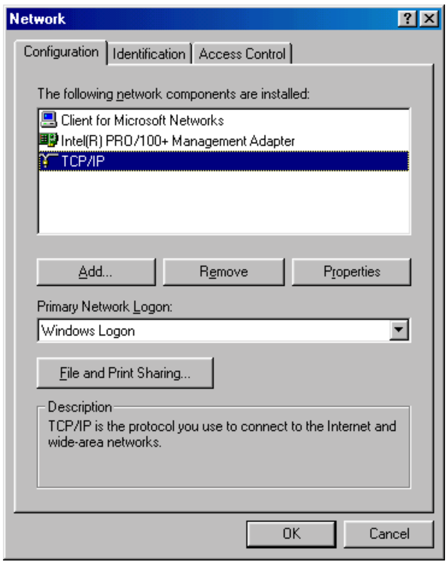
If no error messages are shown, then your Internet connection is OK. Any remaining error is probably due to your PC’s settings. See page 8 for more information!

Check your PC’s settings!

The firewall is delivered with factory defaults that fit most users. If your PC has the default network and web settings, then everything should work at once. If not, please check your PC’s settings:
(The steps described here are for Windows 98. Other operating systems have similar opions, though accessing them may be done differently.)

- Select **Network** in Windows Control Panel or right click on the ”**Network**” icon on your desktop, and select ”**Properties**”.

I have no ”Network” icon on my desktop! Why?
You need a network card installed in your computer. Configure it according to the instructions from the manufacturer.



The following network components are installed:
- Client for Microsoft Networks
- Intel(R) PRO/100+ Management Adapter
- TCP/IP

Primary Network Logon: Windows Logon

Description
TCP/IP is the protocol you use to connect to the Internet and wide-area networks.

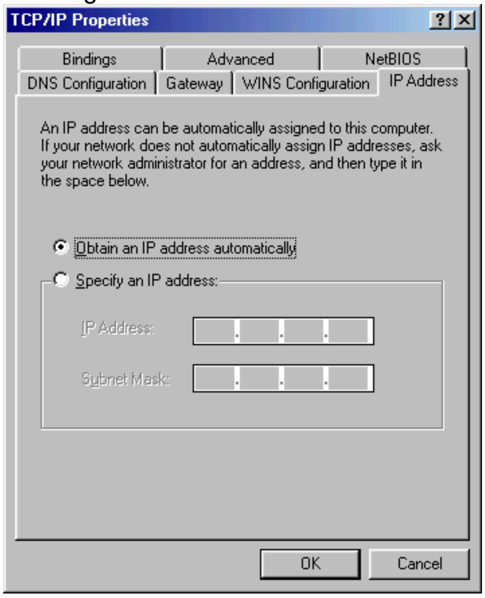
- Double click on ”**TCP/IP**” for your network card on the list that appears.

There is no ”TCP/IP” in the list! Why?
It is not installed. Select ”Add...”, ”Protocol”, ”Microsoft”, ”TCP/IP”.

There are two ways to address computers in a local network (LAN):
Dynamic IP addressing – a DHCP server on the LAN distributes IP addresses to all connected computers.
Static IP addressing – all connected computers use a manually assigned IP address.

Check how your computer is configured to receive an IP address:

a) If it is configured to use dynamic addressing, the settings look like this:

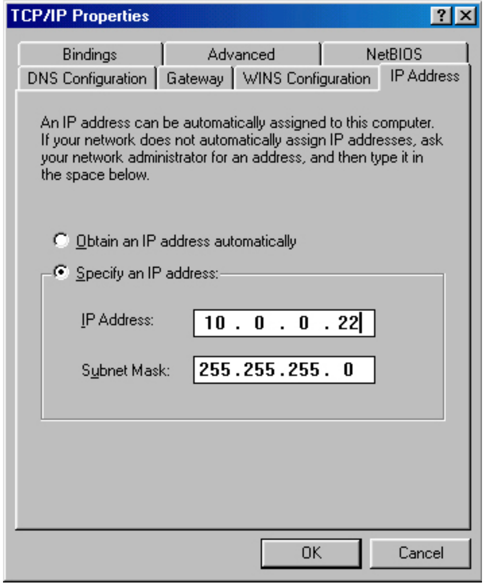


An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically
○ Specify an IP address:
IP Address:
Subnet Mask:

No configuration is needed. The built-in DHCP server in your firewall will distribute correct IP addresses.
Check your setting according to the pages 9, 11, and 12.

b) If it uses static IP addresses the setting look something like this:



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

○ Obtain an IP address automatically
● Specify an IP address:
IP Address: 10 . 0 . 0 . 22
Subnet Mask: 255 . 255 . 255 . 0

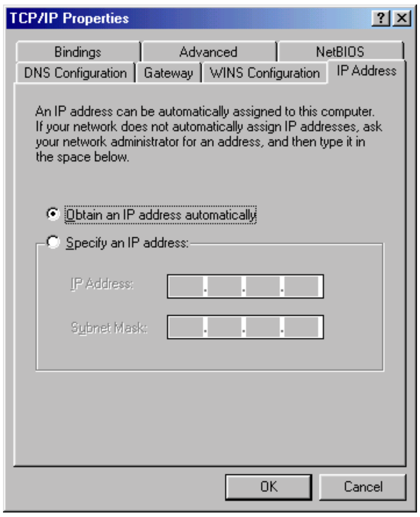
You have two options:
1. **(*recommended*):** Configure all computers on your LAN to use dynamic IP addressing. Refer to page 9 for more information.
2. Configure your firewall and your PC:s so they fit your LAN. Refer to page 10 for more information

Using the firewall with Dynamic IP Addresses on the LAN

The firewall is delivered configured for dynamic IP addressing on the LAN. The firewall acts as a DHCP server and provides IP addresses.

Note! All PC:s on your LAN must be configured like this:

The steps described here are for Windows 98. Other operating systems have similar opions, though accessing them may be done differently.



An IP address can be automatically assigned to this computer. If your network does not automatically assign IP addresses, ask your network administrator for an address, and then type it in the space below.

● Obtain an IP address automatically

○ Specify an IP address:

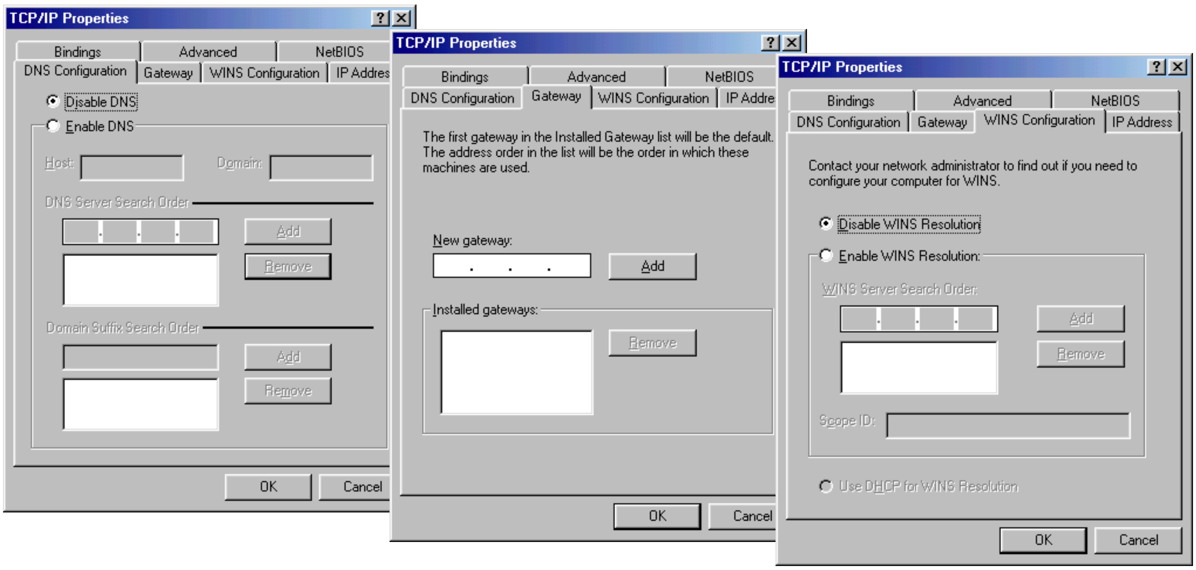
1. Right click on the **Network** icon on your desktop, and select **Properties**.

2. Click on **TCP/IP** for your network card in the list that appears.

3. Click on **Properties** to see TCP/IP configuration:

4. Select **Obtain an IP address automatically**.

5. Check your DNS, Gateway and WINS settings: All fields should be empty and DNS and WINS should be disabled:



● Disable DNS

○ Enable DNS

The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

Contact your network administrator to find out if you need to configure your computer for WINS.

● Disable WINS Resolution

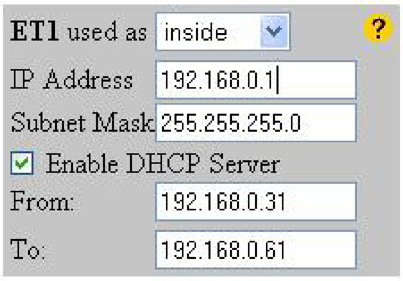
○ Enable WINS Resolution:

○ Use DHCP for WINS Resolution

6. Click **OK** and reboot the PC.

7. You may check that the built-in DHCP server of your firewallis enabled, by viewing the settings of ET2 in the the Network Settings web page (see picture on page 12).

   You can see the most common settings here to the right: These should suit most users.



ET1 used as: inside

IP Address: 192.168.0.1

Subnet Mask: 255.255.255.0

☑ Enable DHCP Server

From: 192.168.0.31

To: 192.168.0.61

If you already run a DHCP server on your LAN you should turn it off or change its settings to distribute the firewall as default gateway.

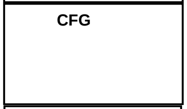
Using the firewall with Static IP Addresses on the LAN

This information is intended for advanced users. If you are not familiar with terms like static IP addressing you do not need to read this chapter. Refer to page 9 instead.

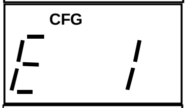
If you want your firewall to be part of an existing LAN that uses static IP addresses, you have to change its LAN (ET1) IP address to an unused IP address that fits the same subnet as your LAN.

You may use the keys on the front panel to change the IP address:

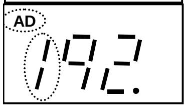
1. Press and hold SET pressed for 3 seconds, to enter setup mode.



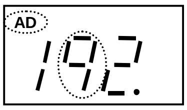
2. Press SELECT once, so CFG is lit.



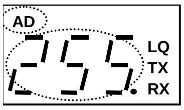
3. Press **SELECT** repeatedly until ”E 1” (ET1) appears in the display.
4. Press **SET**.



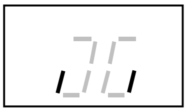
5. Press **SET**. The first 3 digits of the IP address are shown and the first digit flashes.
6. Press **ALT CFG** repeatedly, until the correct digit is displayed.



7. Press SELECT: the next digit flashes, and can be changed using ALT CFG.
8. Use SELECT to step through all digits of the IP address.
   Use SET to step back to the previous digit if you have made any error.
   Use ALT CFG to change the value of the flashing digit.
   You can cancel the IP address set-up, without saving any changes, by pressing the SELECT key and holding it pressed for 2 seconds.



9. After stepping through all digits of the IP address, the subnet mask appears and can be modified. Each subnet mask number can only be set to values 255, 254, 252, 248, 240, 224, 192, 128, or 0.
10. Press ALT CFG repeatedly, until the correct value is displayed.
    Press SELECT to step to the next subnet mask number.



11. When all digits have been displayed the IP address and subnet mask are saved.
12. Complete the installation with the steps on the next page.

Is your firewall not equipped with display and keys?

Do like this:
Connect a PC to the ET1 port on your firewall and configure the PC to use dynamic IP addressing. Refer to page 8.

Change the setting for the ET1 port on your firewall through the built-in web interface. Refer to page 12.

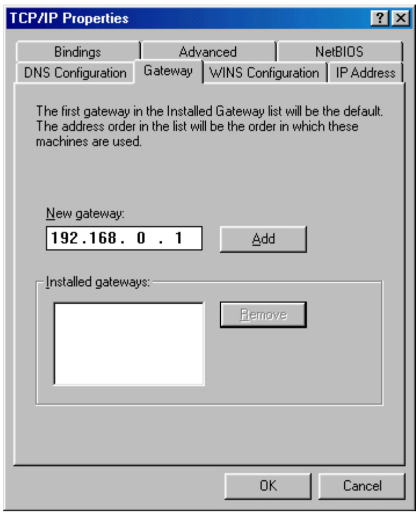
Change PC IP configuration back to its static settings.

Complete the installation with the steps on the next page.

Note! The procedure below has to be performed for all computers connected to your local network (LAN):

(The steps described here are for Windows 98. Other operating systems have similar menues, though accessing them may be done differently.)

1. Right click on the **Network** icon on your desktop, and select **Properties**.
2. Click on ”**TCP/IP**” for your network card on the list that appears.
3. Click **Properties**, select **Gateway**.
4. Enter the IP address of your firewall (the one you entered in step 3-6 on the previous page and click **Add**.
5. Click **DNS Configuration**.
6. Select **Enable DNS**.
7. Copy the DNS settings from the network settings page on the firewall web interface (refer to page 12) to **Search order for DNS servers** and click **Add.**
8. Click **OK**.

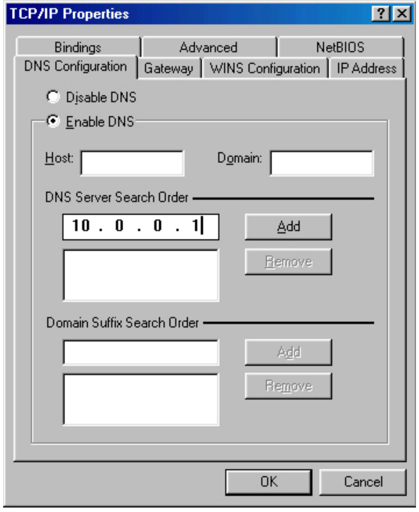


TCP/IP Properties

Bindings | Advanced | NetBIOS | DNS Configuration | Gateway | WINS Configuration | IP Address

The first gateway in the Installed Gateway list will be the default. The address order in the list will be the order in which these machines are used.

New gateway: 192.168. 0 . 1



TCP/IP Properties

Bindings | Advanced | NetBIOS | DNS Configuration | Gateway | WINS Configuration | IP Address

○ Disable DNS

● Enable DNS

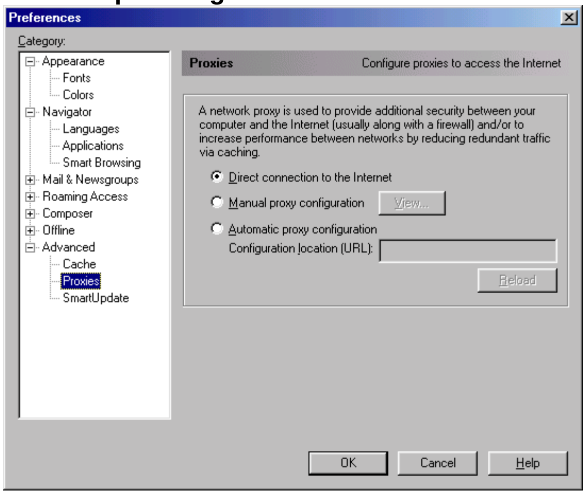
Host: Domain:

DNS Server Search Order: 10 . 0 . 0 . 1

Check the proxy settings of your web browser

If your web browser is configured to use a proxy server, you may have problems reaching the built-in pages of your firewall. In that case, disable the proxy server in your browser:

Netscape Navigator:



Preferences

Category:
- Appearance
  - Fonts
  - Colors
- Navigator
  - Languages
  - Applications
  - Smart Browsing
- Mail & Newsgroups
- Roaming Access
- Composer
- Offline
- Advanced
  - Cache
  - Proxies
  - SmartUpdate

Proxies — Configure proxies to access the Internet

A network proxy is used to provide additional security between your computer and the Internet (usually along with a firewall) and/or to increase performance between networks by reducing redundant traffic via caching.

● Direct connection to the Internet

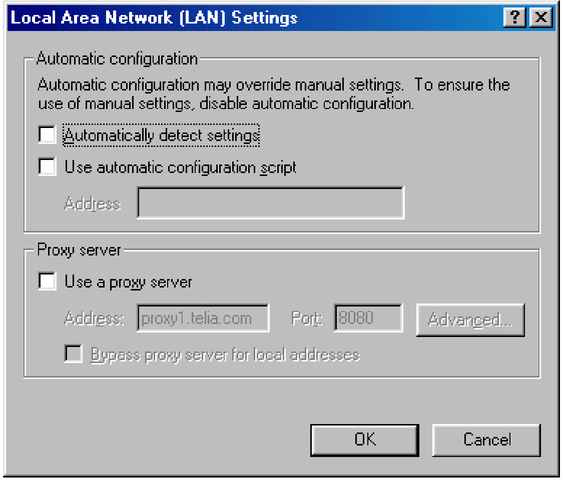
○ Manual proxy configuration

○ Automatic proxy configuration

Configuration location (URL):

Select Edit, Properties, Advanced, Proxies: ”Direct connection to the Internet” shall be selected.

Internet Explorer:



Local Area Network (LAN) Settings

Automatic configuration

Automatic configuration may override manual settings. To ensure the use of manual settings, disable automatic configuration.

□ Automatically detect settings

□ Use automatic configuration script

Address:

Proxy server

□ Use a proxy server

Address: proxy1.telia.com Port: 8080

□ Bypass proxy server for local addresses

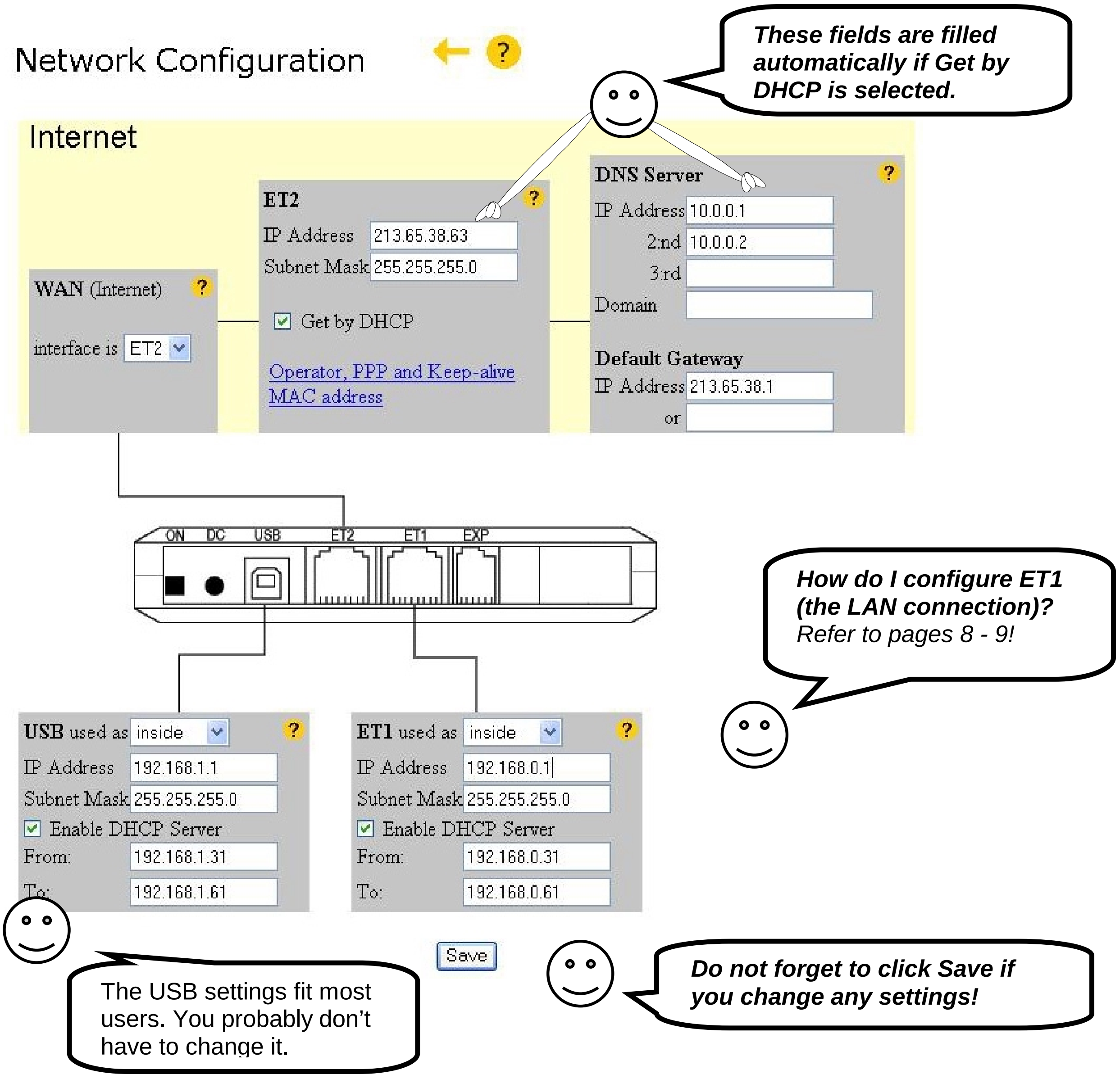
Select Tools, Options, Connection, LAN settings: The checkbox ”Use a proxy-server” must not be selected.

Configure Your Firewall!

Your firewall is delivered with factory settings that fit most users. In some situations however, you may need to change the configuration of your firewall.

To access the built-in pages inside the firewall, do the following:

1. Start a web browser, such as Internet Explorer or Netscape Navigator, on your PC.
2. Write the IP address of your firewall, **192.168.0.1**, in the address field of the browser. The first web configuration page should appear.
3. Click **Log in**.
4. Enter **User name** and **Password**.
   *(At delivery: User name=**admin**, Password=**admin**. You should change them at once!)*
5. Select **Network** in the main menu.
6. If you have received a static IP address, DNS and Gateway addresses from your service provider you should enter these, otherwise select **Get by DHCP**.



Network Configuration

Internet

WAN (Internet)
interface is ET2

ET2
IP Address 213.65.38.63
Subnet Mask 255.255.255.0
☑ Get by DHCP
Operator, PPP and Keep-alive
MAC address

DNS Server
IP Address 10.0.0.1
2:nd 10.0.0.2
3:rd
Domain

Default Gateway
IP Address 213.65.38.1
or

USB used as inside
IP Address 192.168.1.1
Subnet Mask 255.255.255.0
☑ Enable DHCP Server
From: 192.168.1.31
To: 192.168.1.61

ET1 used as inside
IP Address 192.168.0.1
Subnet Mask 255.255.255.0
☑ Enable DHCP Server
From: 192.168.0.31
To: 192.168.0.61

These fields are filled automatically if Get by DHCP is selected.

How do I configure ET1 (the LAN connection)? *Refer to pages 8 - 9!*

The USB settings fit most users. You probably don't have to change it.

Do not forget to click Save if you change any settings!

Note!

Each of the interfaces USB, ET2, ET1 must reside on separate subnets.
Two interfaces cannot have the same IP address – even if one of them is blocked!

Configuring Security Profiles

The active security level is shown on the front panel display. It can be changed using the **ALT CFG** key, or the menu page on the built in web interface.

Hi **Only web and email traffic is allowed -** Highest security, but some applications may have trouble passing.

Lo **All outgoing and legitimate incoming traffic is allowed -** Same security against attacks as the Hi profile, but more applications are allowed to pass out to the Internet.

AC **User editable security profile -** The user may edit the details for this security profile.

bLo **Blocked -** No traffic is allowed to pass. You are disconnected from the Internet.

Does your application have trouble getting out on the Internet?
Do you get an error message?
Change to the ”Lo” security profile!

If you use:

- own servers that you want to make accessible.
- A VPN client to work from home.
- network games (games played together with other users on the net).

you have to configure the firewall to make this traffic pass.

You can edit the firewall settings by choosing **Security** under **Settings** on the menu page. Then choose AC to edit the security profile to fit your games or applications.

Select the applications and protocols you want to be able to pass through the firewall. For some applications you need to state the IP address of the computer on your LAN that should receipt the traffic. It is the IP address to your local computer you should enter. In Windows choose **Start**, **Run**, and enter **winipcfg** to find out what IP address your computer is assigned.

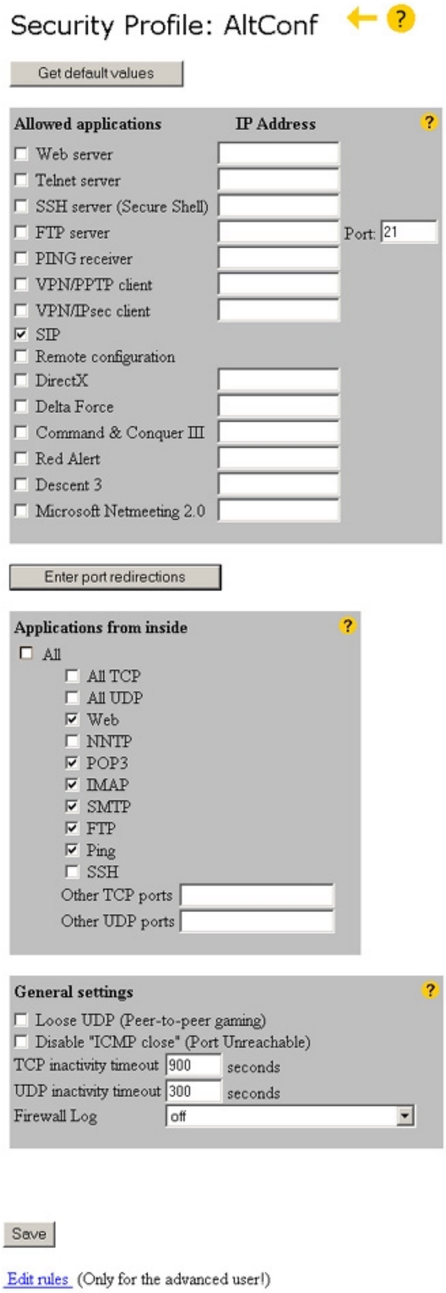
Under **Allowed applications** and **Port redirection** you state the applications, ports and protocols you want to allow to pass **in** through the firewall.

Under **Applications from inside** you state applications, ports and protocols that you want to allow to pass **out** through the firewall.

Once an application, port or protocol has been let through the firewall, a two-way connection is established through the firewall and data can pass in both directions.

Advanced users may manually redirect ports and even edit the rules controlling the firewall.

Read more about the firewall settings in the web-based user manual on **www.igmanual.com**. There is also lot information available on the built-in help pages accessible through the questions marks on the web interface.



Security Profile: AltConf

Allowed applications	IP Address	
□ Web server		
□ Telnet server		
□ SSH server (Secure Shell)		
□ FTP server		Port: 21
□ PING receiver		
□ VPN/PPTP client		
□ VPN/IPsec client		
☑ SIP		
□ Remote configuration		
□ DirectX		
□ Delta Force		
□ Command & Conquer III		
□ Red Alert		
□ Descent 3		
□ Microsoft Netmeeting 2.0		

Applications from inside

□ All
- □ All TCP
- □ All UDP
- ☑ Web
- □ NNTP
- ☑ POP3
- ☑ IMAP
- ☑ SMTP
- ☑ FTP
- ☑ Ping
- □ SSH
- Other TCP ports
- Other UDP ports

General settings

□ Loose UDP (Peer-to-peer gaming)
□ Disable "ICMP close" (Port Unreachable)
TCP inactivity timeout 900 seconds
UDP inactivity timeout 300 seconds
Firewall Log off

Edit rules (Only for the advanced user!)

Do not forget to click Save and change the profile to AC if you make any changes!

Using the Online User Manual

Once your Internet connection is up and running, you can easily access the online user manual for complete and up-to-date information about your firewall.

1. Surf to the built-in web page of your firewall.
2. Click **Online User Manual**.

Note!
You can also read the Online User Manual from any computer with Internet access, at **www.igmanual.com**

Technical specification

System supprt	Independent of operating systems.
Configuration	Built-in web server.
Protocol	IP, PPPoE, TCP, UDP, FTP, DHCP, HTTP, SSH, PPTP, IPSec, SIP
Measurements	180x130x25 mm
Weight	0,3 kg
Ports	EXP: Expansion port for future usage. ET1: 1 x 10/100 Base-T (RJ 45), IEEE 802.3 and 802.3u compatible ET2: 1 x 10/100 Base-T (RJ 45), IEEE 802.3 and 802.3u compatible USB: USB specification 1.0 and 1.1
Power supply	9V DC, 600 mA
Firewall	Generic rule-based packet-filtering, Stateful inspection, Port redirection, NAT+PAT
Smart card reader *(option)*	ISO 7816-1/2/3/4, Asynchronous Cards (T=0, T=1)
SIP support	IETF protocol for sessions over Internet (e.g. IP Telephony), RFC2543
SIP proxy	Firewall awareness (controls the firewall), Parallel Forking, Session Timer
SIP registrar	SIP-clients are automatically registered, so that the proxy can forward calls and media streams to the correct recipient.

INTERTEX END USER SOFTWARE LICENCE AGREEMENT

BY ENTERING INTO A BINDING AGREEMENT FOR THE PURCHASE, LEASE, HIRE OR OTHER USE OF INTERTEX SOFTWARE, WHETHER OR NOT EMBEDDED IN PURCHASED HARDWARE, ALL AS SPECIFIED IN SUCH AGREEMENT, AND WHERE THIS END USER SOFTWARE LICENSE AGREEMENT IS EITHER ATTACHED TO SUCH AGREEMENT OR TO ORDER CONFIRMATION OR SIMILAR DOCUMENT SENT TO YOU ON OR BEFORE DELIVERY, YOU HAVE AGREED TO THE TERMS OF THIS LICENCE AGREEMENT (NO LATER THAN) UPON ACCEPTING DELIVERY.

1. THE LICENCE

INTERTEX Data AB, Rissneleden 45, 174 44 Sundbyberg, Sweden (“INTERTEX”), authorizes you (the “Licensee”) to use the software programs (the “Software”) specified in the purchase/lease/hire or similar agreement (“the Purchase Agreement”) for the use of such Software, and to which this License Agreement is appended or otherwise connected, and/or which is embedded in hardware equipment specified in the Purchase Agreement, and the Licensee accepts a non-exclusive, non-transferable Licence to "Use" (as hereinafter defined) the Software on or connected to a single computer system (the "System") for use by the maximum number of concurrent users and for the maximum number of concurrent sessions as specified in the Purchase Agreement, upon the terms and subject to the conditions contained herein.

2. USE OF THE SOFTWARE

For the purposes of this Licence "Use" shall mean and include:

(i) utilization of the Software by copying, transmitting or loading the same into the temporary memory (RAM) or installing into the permanent memory (*e.g.* hard disk, CD ROM or other storage device) of the System for the processing of the System instructions or statements contained in such Software;
(ii) in the case of Software embedded in hardware equipment; by operating the hardware equipment;
(ii) storing the whole or any part of the Software on the System or other storage unit or disk;
(iii) utilizing (but not copying) the instructional and/or operational manuals relating to the Software.

For the purposes of this Licence "concurrent use" shall mean simultaneous use of the Software by the number of users of the Licensee specified in the Purchase Agreement PROVIDED however that Software installed on a file server for the sole purpose of distribution to other workstations or computers is not being Used for the purposes of ascertaining the number of concurrent users.

3. LICENSEE'S UNDERTAKINGS

The Licensee may not perform any of the acts referred to in (i)-(iii) below except to the extent and only to the extent permitted by the applicable law to the Licensee as a lawful user of the Software and only then for the specific limited purpose stated in such applicable law or hereunder. Licensee may not

(i) copy the Software (other than for normal System operation) or otherwise reproduce the same provided that the Licensee may copy the Software for back-up purposes;
(ii) translate, adapt, vary or modify the Software;
(iii) disassemble, decompile or reverse engineer the Software

The Licensee further undertakes:

(iv) not to provide or otherwise make available the Software in whole or in part (including where applicable, but not limited to program listings, object code and source program listings, object code and source code), in any form to any third party without prior written consent from INTERTEX;
(v) within 14 days after the date of termination or discontinuance of this Licence for whatever reason, to destroy the Software and all updates, upgrades or copies, in whole and in part, in any form including partial copies or modifications of the Software received from INTERTEX or made in connection with this Licence, and all documentation relating thereto.

4. LIMITED WARRANTIES

Limited warranties are granted to the Licensee by the reseller of INTERTEX products from which the Licensee has purchased the Software, in accordance with a separate Warranty Statement attached to the Licensee's purchase agreement or to order confirmation or included in the delivery.

5. LIMITATION OF LIABILITY

Without prejudice to the Licensee's rights against the reseller according to a separate Warranty Statement as provided in Section 4, the Licensee hereby acknowledges that software in general is not error-free and agrees that the existence of such errors shall not constitute a breach of this Licence. THE SOFTWARE IS FURNISHED AS IS AND INTERTEX DISCLAIMS, TO THE EXTENT PERMITTED BY THE APPLICABLE LAW, ALL WARRANTIES WITH RESPECT TO THE SOFTWARE, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR PURPOSE.

INTERTEX shall not be liable for any loss or damage whatsoever or howsoever caused arising directly or indirectly in connection with this Licence, the Software, its use or otherwise, except to the extent that such liability may not be lawfully excluded under the applicable law. Notwithstanding the generality of the preceding sentence, INTERTEX expressly excludes liability for indirect, special, incidental or consequential loss or damage which may arise in respect of the Software, its use, the System or in respect of other equipment or property, or for loss of profit, business, revenue, goodwill or anticipated savings.

In the event that any exclusion contained in this Licence shall be held to be invalid for any reason and INTERTEX becomes liable for loss or damage that may lawfully be limited, such liability shall be limited to the licence fee paid for the Software.

INTERTEX does not exclude liability for death or personal injury to the extent only that the same arises as a result of the negligence of INTERTEX, its employees, agents or authorized representatives.

6. COPYRIGHT, PATENTS, TRADE MARKS AND OTHER INTELLECTUAL PROPERTY RIGHTS

The Licensee acknowledges that any and all of the copyright, trademarks, trade names, patents and other intellectual property rights subsisting in or used in connection with the Software including all documentation and manuals relating thereto are and remain the sole property of INTERTEX. The Licensee shall not during or at any time after the expiry or termination of this Licence in any way question or dispute the ownership by INTERTEX.

.

7. TERMINATION

INTERTEX may by notice in writing terminate this Licence if the Licensee is in breach of any term, condition or provision of this Licence or required by the applicable law and fails to remedy such breach (if capable of remedy) within 30 days of having received written notice from INTERTEX specifying such breach. Termination, howsoever or whenever occasioned shall be subject to any rights and remedies INTERTEX may have under this Licence or under the applicable law.

DECLARATION OF CONFORMITY

according to EN 45014

The manufacturer Intertex Data AB, Rissneleden 45, 174 44 Sundbyberg, Sweden, herewith declares the firewalls/modems in the Intertex IX66 Internet Gate series are in compliance with the essential requirements and other relevant provisions of the following EC directives:
1999/5/EC **Radio & Telecommunications Terminal Equipment Directive (R&TTE)**
and that the following harmonised standards and/or technical specifications have been applied:

Electromagnetic Emission:	**EN 50081-1:1992, EN 50081-2:1993, EN 55022:1998**
Electromagnetic Immunity:	**EN 50082-1:1997, EN 61000-6-2:1999, EN 55024:1998**
Safety:	**EN 60950**

Stockholm September 30, 2001

Karl Erik Ståhl

Karl Erik Ståhl, President Intertex Data AB

DECLARATION OF CONFORMITY

according to FCC Part 15

The firewalls/modems in the Intertex IX66 Internet Gate series comply with Part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) the devices may not cause harmful interference, and
(2) the devices must accept any interference received, including interference that may cause undesired operation.

NOTE: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment cause harmful interference to radio or television reception, which can be dermined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Any changes or modifications not expressively approved by Intertex Data AB could void the user's authority to operate this equipment.

To preserve the environment, you should return the product to where you purchased it or directly to an accredited electronics recycling station.

Intertex uses accredited companies and organisations for recycling and disposion of electronics, packing materials and emballage.

Notes:

Notes:

This product is developed and manifactured by Intertex Data AB

Distributed by:
ABP Technology Partners
1203 Crestside Drive, Suite 300, Coppell, TX 75019
USA

www.abptech.com