# NetPilot VPN

## Technical Evaluation

**An NSS Group White Paper**

First published March 2002 (V1.0)

Published by The NSS Group
Oakwood House, Wennington, Cambridgeshire, PE28 2LX, England

Tel : +44 (0)1487 773307
Fax : +44 (0)1487 773168
E-mail : info@nss.co.uk
Internet : http://www.nss.co.uk

# TABLE OF CONTENTS



TABLE OF FIGURES

# The NSS Group

The NSS Group is Europe's foremost independent network and security testing facility.

Based in Cambridgeshire, England, and with additional labs and conference centre in the South of France, The NSS Group offers a range of specialist IT, networking and security-related services to vendors and end-user organisations throughout Europe and the United States.

The Group consists of two wholly-owned subsidiaries :

- *NSS Network Testing Laboratories*
- *Network Security Services*

**NSS Network Testing Laboratories** are available to vendors and end-users for fully independent testing of networking, communications and security hardware and software.

NSS Network Testing Laboratories also operates certification schemes for vendors and certification bodies, and currently provides certification of firewalls, VPN's, crypto products and PKI products.

Output from the labs, including detailed research reports, articles and white papers on the latest network and security technologies, are made available free of charge on the NSS web site at http://www.nss.co.uk

**Network Security Services** provides a range of security-related services to vendors and end-users including security policy definition, IDS, firewall and VPN implementation, network security auditing and analysis, and penetration testing.

# INTRODUCTION

Internet connectivity is seen as an essential element of the corporate computing infrastructure these days. Even the smallest of companies would be lost without e-mail or the ability to surf the Internet.

However, connecting to the Internet is still more complex than it needs to be. Even for the single user, the plethora of free Internet services and confusing array of options makes life far from easy. When you are faced with the task of connecting up a corporate network to, your problems are multiplied accordingly.

How do you provide the physical connection? How do you ensure that communications costs are kept to a minimum? How do you provide e-mail services for all your employees? How do you ensure that employees do not waste their time surfing non-productive Web sites? Is it economical to maintain your own Web site? How do you maximise security, maintaining the privacy and integrity of your internal network once it is connected to the outside world? How to you provide secure communications links between your branch offices?

The number and complexity of such questions has prevented many companies from taking the plunge and realising the benefits the Internet has to offer. The need for routers, mail servers, Web servers, file and print servers, Web caches and an army of experts to maintain them all just adds to the perceived difficulty – and, of course, cost.

Life has been made that much simpler in certain areas recently by the introduction of the network appliance – a hardware and software combination dedicated to a single task, such as Web or mail serving.

The appliance is also an attractive proposition for large companies, however, since it usually represents excellent value for money – one price securing both hardware and software to perform a specific task or range of tasks – as well as offering the lowest cost of ownership. Once again, the “one box, one task” philosophy means that configuration and management is simplified, and support problems are minimised.

Internetworking is becoming the technology platform for a growing range of business uses: secure access to global resources on the Internet and other public networks; secure remote access to the enterprise network for remote users and branch offices; and compartmentalisation of the internal network for enterprise-wide connectivity and security.

To meet the rapidly evolving connectivity needs of today's networks, corporations require an integrated network security solution that is flexible and extensible enough to meet their requirements now and in the future.

Organisations with large populations of mobile workers also need to be able to provide flexible yet secure (preferably encrypted) remote access to business applications which are located behind firewalls. The same is true of any organisation wishing to implement electronic commerce systems, but the traditional firewall implementation is not designed to allow such free movement of traffic.

# NETPILOT VPN

Equiinet, a UK company, has taken things one step further than the traditional “one box, one task” type of appliance by integrating all the functionality required by the average organisation when connecting to the Internet and combining it with a dedicated, custom-built hardware platform – a “Secure Internet Appliance”.

## Platform

There are two basic hardware platforms in the NetPilot product line, one based on the PowerPC processor (a desktop enclosure) and the other based on an Intel architecture (1U rack-mount case).

Slight variations in the hardware specification are available, creating “*Lite*”, “*Standard*” and *“Plus”* versions, but a common code base runs on all appliances. The only software variation is in the case of the VPN model, which adds site-to-site and remote client VPN capabilities to the standard offering.

The product line therefore consists of:

### NetPilot Lite

- *Desktop enclosure*
- *PowerQuicc processor and architecture*
- *1 x hard disk drive (minimum 5GB)*
- *1 x parallel printer port*
- *1 x serial port*
- *1 x 10/100 local Ethernet LAN port*
- *1 x ISDN BRI port (2 x 64Kbps dual channel operation)*

### NetPilot

- *Desktop enclosure*
- *PowerQuicc processor and architecture*
- *1 x hard disk drive (minimum 20GB)*
- *1 x 10/100 local Ethernet LAN port*
- *1 x parallel printer port*
- *1 x serial port*
- *1 x ISDN BRI WAN port (2 x 64Kbps dual channel operation)*
- *1 x 10Mbps Ethernet port for WAN connection (DSL, etc)*
- *1 x leased line WAN port for X.21 or V.35 to 2Mbps*

### NetPilot VPN

- *Desktop enclosure*
- *PowerQuicc processor and architecture*
- *1 x hard disk drive (minimum 20GB)*
- *1 x parallel printer port*
- *1 x serial port*
- *1 x 10/100 Local Ethernet LAN port*
- *1 x ISDN BRI WAN port (2 x 64Kbps dual channel operation)*
- *1 x 10Mbps Ethernet port for WAN connection (DSL, etc)*
- *1 x leased line WAN port for X.21 or V.35 to 2Mbps*
- *Includes site-to-site IPSec VPN and 3 VPN client licenses*

## NetPilot Plus

- *1 x Intel Celeron processor*
- *1 x hard disk drive (minimum 20GB)*
- *1 x parallel printer port*
- *1 x serial port*
- *1 x 10/100 local Ethernet LAN port*
- *1 x 10/100 Ethernet WAN port*
- *1 x ISDN BRI WAN port (2 x 64Kbps dual channel operation)*

## NetPilot Enterprise

- *1U enclosure with twin removable disk caddies*
- *1 x 700MHz Intel PIII processor*
- *256MB RAM*
- *2 x hard disk drives (minimum 20GB)*
- *1 x parallel printer port*
- *1 x serial port*
- *1 x 10/100 local Ethernet LAN port*
- *1 x ISDN BRI WAN port (2 x 64Kbps dual channel operation),* ***or***
- *1 x 10/100 Ethernet port for WAN connection (DSL, etc),* ***or***
- *1 x leased line WAN port for X.21 or V.35 to 2Mbps*

## NetPilot Enterprise VPN

- *1U enclosure with twin removable disk caddies*
- *1 x 700MHz Intel PIII processor*
- *256MB RAM*
- *2 x hard disk drives (minimum 20GB)*
- *1 x parallel printer port*
- *1 x serial port*
- *1 x 10/100 local Ethernet LAN port*
- *1 x ISDN BRI WAN port (2 x 64Kbps dual channel operation),* ***or***
- *1 x 10/100 Ethernet port for WAN connection (DSL, etc),* ***or***
- *1 x leased line WAN port for X.21 or V.35 to 2Mbps*
- *Includes site-to-site IPSec VPN and 5 VPN client licenses*

Multiple WAN interfaces can be supplied on each appliance, though only one can be operational at any one time. A nice touch on the desktop NetPilot model is the MDI/MDX switch on LAN port 2, which allows the external LAN port to be connected to a hub or directly to another PC or router without the use of a crossover cable.

Note that this evaluation concentrates on the *NetPilot VPN* and *NetPilot Enterprise VPN* devices, each with two Ethernet ports, running version 2.19.7 of the NetPilot software.

The software is based around a heavily modified Linux installation, and all the NetPilot models are designed to be operated without a keyboard or monitor. A number of status LEDs on the front panel of the standard NetPilot and NetPilot Lite models provide instant notification of power, network activity, disk activity, ISDN status, WAN interface activity, alarm status, and whether e-mails are waiting to be collected.

The Enterprise model provides a small, but clear, orange LCD display, seven push-buttons and six status LEDs on the front panel, via which it is possible to program important parameters such as the IP address and network mask, as well as view real-time status displays.

Twin removable disk drives are accessible behind a drop-down door on the front panel of the Enterprise.

From the basic Red Hat distribution, a significant number of the standard packages have been modified, and a number of new ones custom written from scratch to support some of NetPilot's more advanced features. For example, the file system has been reorganised to survive a power cycle without a proper shut down.

This must qualify as a brand new operating system – it certainly bears only a passing resemblance to the Red Hat Linux with which you may be familiar. Should you wish to attach a keyboard and monitor, however, you are still not permitted Root access to the device – only a text-based browser interface (Lynx) is available, which provides access to the normal browser-based admin interface. The whole thing has been designed to hide the complexities of the underlying OS and make it as simple as possible to use.

The nice part of the NetPilot is that it actually includes every piece of hardware and software you will need to service a small to medium-sized office in terms of Internet connectivity and networking. Amazingly, for the price, it includes Internet routing and shared connectivity, firewall, Web caching, Web server, FTP server, e-mail server, access control and URL filtering, DHCP server, Windows file and print server, DNS server, and management reporting. There is also, of course, the VPN version, which adds both site-to-site and remote client IPSec Virtual Private Network capabilities, and the Enterprise version, which is designed to support larger implementations.

In terms of connectivity, the basic machine typically comes with a 10/100Mbit Ethernet card (for the internal LAN connection), ISDN card, serial port and parallel port. The serial port can be used to provide X.21 connectivity, an additional ISDN Terminal Adapter or a dial-up modem, and the internal ISDN card can be replaced with an X.21 card, modem or additional Ethernet card if required. This latter option is for those who already have their LAN connected to the Internet and want the NetPilot to sit behind their existing router. The Enterprise model can support similar connectivity options, but does not come with an ISDN port as standard.

Multi-user Internet access can be through modems, ISDN connections or leased lines, and to minimise call charges, dial-up connections are automatically initiated when required, and cleared on inactivity. When a line is open calls can even be piggy-backed to save costs.

As a security measure, the ISDN card will never answer calls, and even makes it look to the external network as if there is no ISDN device attached to the line. Direct-dial remote access can be enabled if required, however.

The basic model typically supports 50 simultaneous users, although it may service a much larger population, with up to 150 e-mail boxes configurable. On its WAN side it is capable of running at up to 2Mbps on X21/V35 leased lines or at 10 Mbps when interfacing to external routers (for connection to ADSL, for example).

The larger more powerful Intel based Enterprise models typically support over 100 simultaneous users, again from a much larger total population, with up to 500 e-mail boxes configurable

## Configuration & Management

The NetPilot is just about as idiot-proof as you can get when it comes to installation. Once you have the hardware connected you need to configure the internal LAN interface to be accessible from a browser on your LAN (or directly-connected PC).

Whereas other vendors expect you to reconfigure a workstation on your network to talk to a factory-set IP address on the device, Equiinet realises that this is far from ideal. NetPilot is aimed at organisations with little or no IT expertise, after all.

Those who are not fond of a graphical interface – or who have not yet connected their NetPilot to the network – are welcome to connect a keyboard and monitor, or a second PC via the serial port, and use the text-based Lynx browser to configure the box.

Most will probably use the simple Ping utility included to assign the required IP address to the NetPilot and then use their favourite browser to configure it from the LAN. The Enterprise model can also be programmed via the front-panel buttons and LCD interface.

Once you have your browser talking to the NetPilot a simple connection wizard - the *Quick Configuration* program – configures your WAN link to talk to your ISP. Most of the major ISP settings are pre-configured, leaving you to select yours from a pull-down menu. In the unlikely event it is not there, you can enter the required settings manually from the details provided by your ISP.

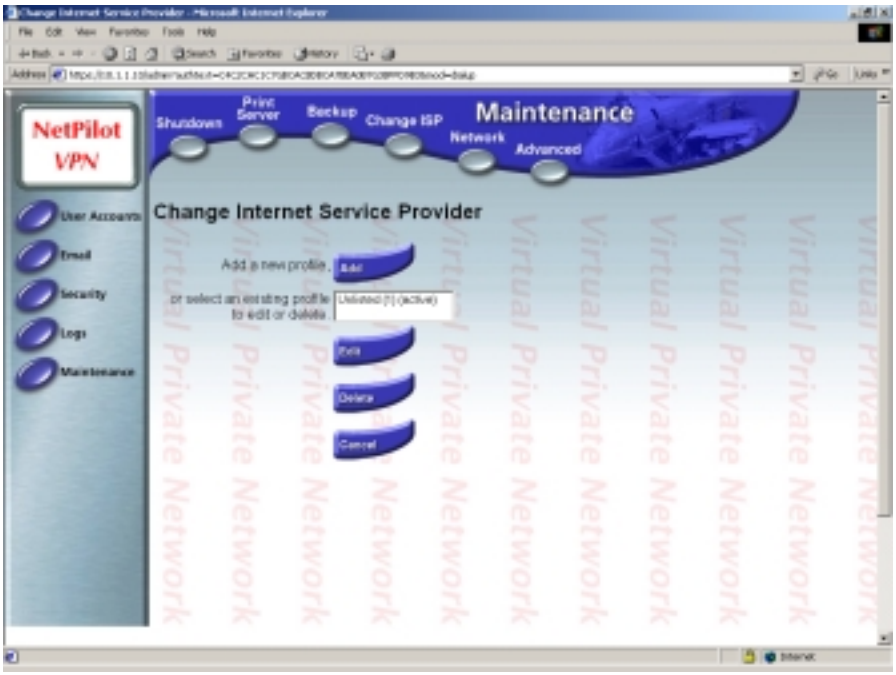


*Figure 1 - Configuring ISP parameters*

In all respects, the NetPilot is designed to take charge wherever it is appropriate. Once you have specified the Windows Workgroup in which it is to participate, for example, NetPilot ensures that it never loses the fight in a Browser election.

In many small offices, the fact that there is no dedicated file and print server means that the Master Browser PC – or the one with all the main office files on it – can sometimes be powered down and left that way, causing problems for other users. NetPilot ensures that it is always the Master Browser, and because it is always powered up, its shared drive and printer are always available.

Another example of the thought that has gone into making NetPilot fool proof is the DHCP server. If NetPilot detects that your network already has a DHCP server in operation, it simply disables its own internal one and configures itself as a client.

If, however, one is not detected, then NetPilot automatically configures and enables its own, thus solving all future IP numbering problems. A DNS server is also included, which can act as the main server for the organisation, or as a forwarder for an existing internal DNS server.

The only feature of NetPilot that requires more configuration than it should is related to the fact that it is not a transparent proxy. The browser on each desktop will need to be configured to perform its Web access via the NetPilot proxy server, though the process is made as straightforward as possible by the provision of a client configuration utility called the *NetPilot PC Configuration Wizard*.

This is a simple Windows-based application that can be run on each client PC on the network – even by a relatively inexperienced user – in order to configure e-mail client and browser settings to work correctly with NetPilot. The documentation (all on-line, in the form of PDF files provided on the accompanying CD) is also excellent.

Equiinet has not resorted to using Java for the browser-based management interface for the NetPilot, instead relying on HTML and scripting – far quicker and much more usable. An authenticated and SSL-encrypted link is provided between browser and NetPilot for secure administration over either the local network or the Internet, and it is possible to create *Admin* and *Site Admin* accounts with different levels of administrative access. Selecting an option from the list down the left hand side of the screen brings up a sub-menu of options along the top.

The main menu options are:

- *User Accounts*
- *Email*
- *Security*
- *Logs*
- *Maintenance*

## User Accounts & Group Policies

The *User Accounts* option is the key to the NetPilot's access control and Web monitoring facilities. Enabling user accounts means that users need to authenticate themselves to the NetPilot via a user name and password combination before they are allowed through the firewall, but it does provide the highest levels of control in exchange for this minor inconvenience.

Creating users and groups provides the opportunity to restrict activities (e-mail only, Web browsing only, or a combination of the two) as well as restrict browsing to specific sites (a "*white list*") or prevent browsing to undesirable sites (a "*black list*") on a per user basis. The site lists are maintained manually by the administrator.

Different policies can be created and named, and then applied on a per user or per group basis. Each policy can cover which service can be used (e-mail and Web), which sites are allowed or disallowed, what times of day browsing is allowed, and whether to block adverts (a real boon, getting rid of those annoying banner ads) and porn sites.

The porn filter is one area that needs further development in the version under test, and the company has taken this on board with the new release of the NetPilot software (version 2.20) which should be available by the time you read this. In the new release, Equiinet has developed a partnership with N2H2 (www.N2H2.com) to provide a subscription based URL filtering service, as well as increasing both the flexibility and the number of filtering options available. Equiinet now refers to this as *Boundary Filtering.*

If you don't want your users to have to authenticate themselves to NetPilot before they can browse the Web, you can have a single default policy that applies to the whole organisation. This can allow free access, or can restrict everyone by site or time of day as detailed in the previous paragraph. Extensive logs and activity reports are also available to show how users have been spending their time on the Web.

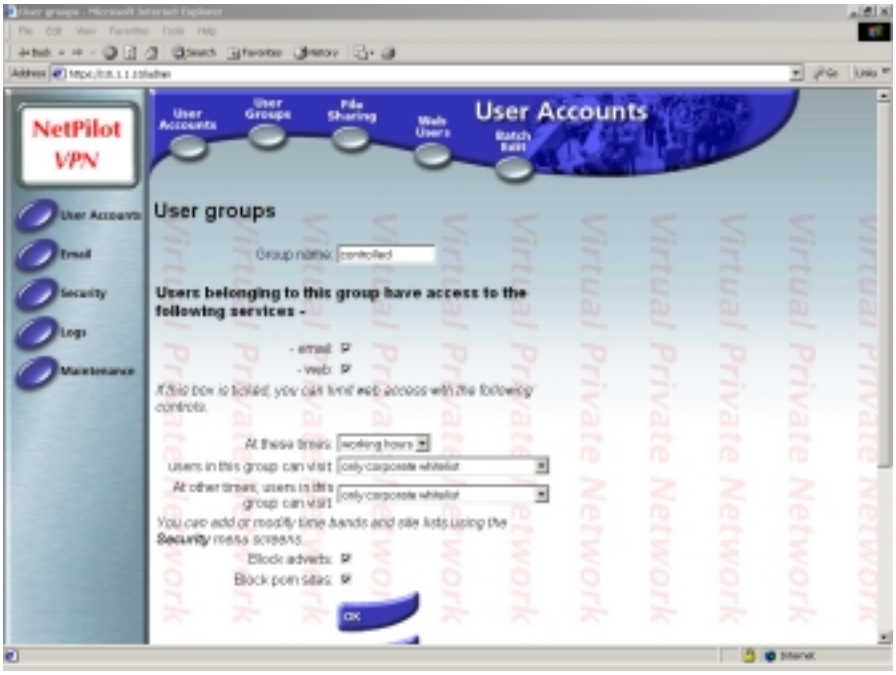


*Figure 2 - Setting group policies*

NetPilot's reporting and control facilities include time online, the number of incoming and outgoing emails by user, web usage by time of day and packets rejected by the firewall. Reports can be automatically collated and sent as a daily e-mail to system supervisors.

## File & Print Sharing

User accounts are also required if you wish to enable the file and print sharing features of NetPilot. Any printer attached to the parallel port can be made available to all Windows/Samba clients, and for each user created, a portion of the hard disk is allocated to that user as private file space. This can be accessed by the usual Windows-based drive mapping or via the built-in NetPilot FTP server.

Certain users can also be provided with access to the files that make up the corporate Web site, and the Web server can be configured to provide access to internal users only, or both internal and external users.

The NetPilot can thus be used to provide a pure intranet environment, or as the main corporate Web server. Creating a user called “anonymous” also provides anonymous FTP access from outside the firewall, should the firewall allow.

## E-Mail

As well as the Web server, FTP server, and file and print services, NetPilot also includes both SMTP and POP3/IMAP4 mail servers. The SMTP server can be configured to pick up mail from, and send mail to, an ISP at pre-defined intervals, thus optimising line usage and minimising costs by eliminating the need for individual users to dial in separately (and often constantly). Emails can be diverted if users are away, and any incoming mail without a user name will automatically be sent to an administrator.

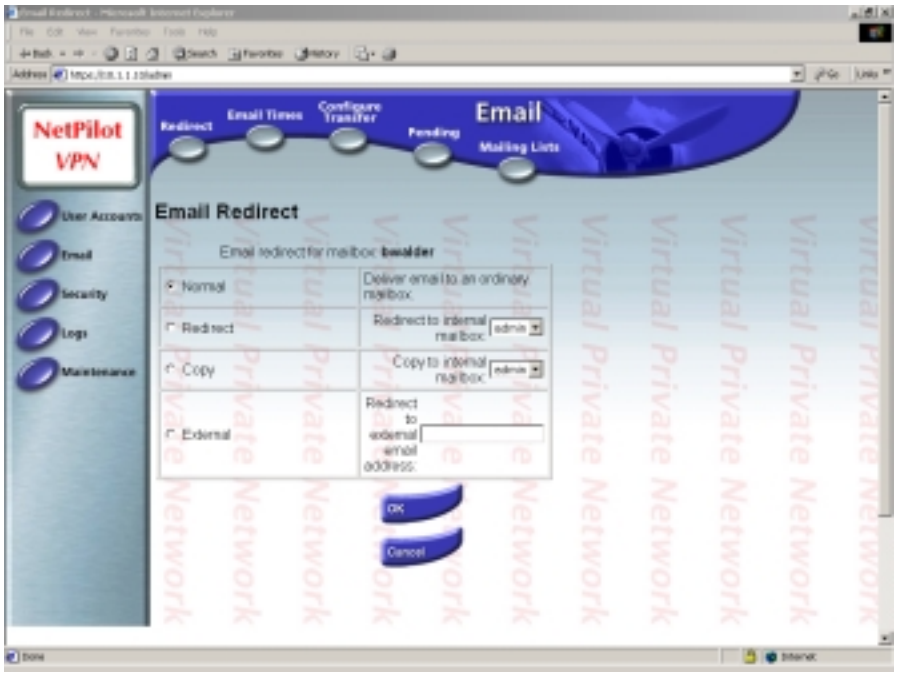


*Figure 3 - Configuring mailbox redirection*

Once the SMTP server has retrieved mail from the ISP it can be forwarded on to an internal SMTP server directly, or the mail can be stored in the appropriate user mailboxes on NetPilot for retrieval using any POP3 or IMAP4 client. Mail can also be redirected or copied to other mail servers (both internal and external) on a per user basis if required.

To save costs still further, when anyone browses the Web, NetPilot will piggy-back on the call, checking for incoming messages and sending outgoing mail at the same time. Mailing list capabilities are provided, and browser-based e-mail access is available on the Enterprise model only.

At part of Equiinet's push into the Secure Appliance market it has provided an e-mail client called *NetPilot SafeMail*, which is bundled with every NetPilot on an unlimited user basis. It controls both the content of the e-mail being sent or received, as well as placing restrictions on sender and receiver.

Version 2.20 of the software will see further enhancements to provide a *Boundary Scanning* capability. Through a partnership with Sophos (www.sophos.com) Equiinet will be able to offer the ability to scan incoming or outgoing e-mails for virus threats, or even check e-mails sent between local users.

## Boundary Caching

Another feature aimed at minimising costs is Web caching. Based on the popular Squid package, NetPilot introduces the concept of "*Boundary Caching*". Despite the fact that most European users will be connecting to the Internet via 64Kbps or 128Kbps ISDN or leased lines, they still lag far behind their counterparts in the US where 1.5Mbps or 2Mbps links are the norm. This means that European users will spend considerably more in downloading the same Web content than US organisations.

For some time Internet Service Providers (ISPs) have used web caches to recognise frequently-requested web sites, pages or parts of pages and store them locally to the ISP, thus removing the need to initiate a trans-Atlantic connection each time those pages are requested. Although this provides improved response times for European users, the main effect is to save on costly trans-Atlantic bandwidth for the ISP.

NetPilot provides the means to achieve cost savings in a similar way for the average company. In any organisation, users tend to surf the same groups of pages on a regular basis – think of financial organisations looking at the Financial Times' web site, for instance. The most efficient place for business caching is on the boundary between the office LAN and the Internet – inside NetPilot.

Imagine just ten employees in a company each downloading the latest version of Internet Explorer from the Microsoft Web site. Each user will download his or her own copy of the file, thus tying up the Internet connection for the best part of a day in total. With a Web cache, once the first user has downloaded the software, subsequent requests will be served directly from cache. Not only will this provide almost immediate response times for those users, making them that much more productive, but none of the subsequent requests causes the line to the ISP to be brought up, thus saving money too.

NetPilot's *Boundary Caching* works transparently and intelligently so that no configuration is needed by the user or network administrator. Importantly, it will also work in conjunction with the ISP's cache so that both are aware of the age and content of the information that is being carried by the co-operating device – considerably reducing the likelihood of a request to the originating server.

Where the time to live for Web page information is short, or where data is dynamic, NetPilot will refresh cache data regularly (or always go directly to the Web site), ensuring that stale data is never served from the cache.

In common with the “idiot proof” philosophy of NetPilot, there are almost no configuration options for the caching, the only one being the ability to adjust the size of the cache as a percentage of the disk space. This may worry those who like to control their network appliances, but Equiinet has decided to keep things as simple as possible throughout. There are a number of extremely useful statistics screens available showing how well the cache is performing, however.

## Firewall

The built-in firewall is a fairly basic (though no less secure for that) pure packet filtering firewall – stateful inspection capabilities will not be introduced until the product is moved to the Linux 2.4 kernel. As with the other aspects of the device, configuration and management of the firewall is entirely browser-based. If you are expecting the usual complex packet filter rules definition, however, you are in for a shock, because – also in line with the other features of NetPilot – the firewall has been made as foolproof as possible.

Whilst the firewall is nowhere near the most sophisticated offering of its kind that we have seen, it is certainly the only one we have ever come across that can literally be plugged in, have a couple of boxes checked, and be up and running and every bit as secure as some of its more expensive competitors in less than 10 minutes!

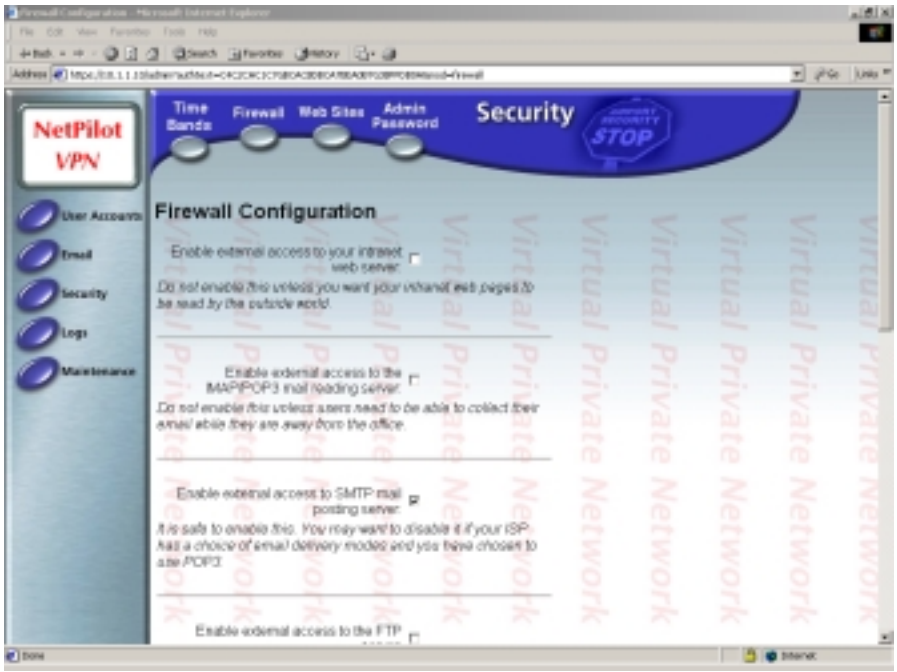


*Figure 4 - Simple firewall configuration*

How does it achieve this? Quite simply by placing heavy restrictions on what traffic is allowed through the firewall by making a few major assumptions.

The first is that no traffic at all is allowed from the external network to the internal protected network.

The second is that outbound traffic is unrestricted, the only exception being Web traffic, which is blocked on port 80 but enabled on port 8000. This forces all outbound HTTP traffic through the NetPilot proxy server, and is the reason why the users' browsers need to be configured to use a proxy.

IP addresses of all outbound connections are hidden using NetPilot's IP masquerading feature – also known as Network Address Translation (NAT) – where each outbound address is changed to the external address of the NetPilot itself.

The third assumption is that all traffic to the firewall is rejected unless allowed by checking half a dozen boxes on the firewall configuration page:

- *Enable external access to the NetPilot web server*
- *Enable external access to the NetPilot POP3 server (to provide access from outside the organisation for travelling employees)*
- *Enable external access to the NetPilot SMTP server (to allow SMTP to SMTP posting from your ISP)*
- *Enable external access to the NetPilot FTP server (allows access to the anonymous user share only)*
- *Enable external access to the management screens (should you wish to manage the NetPilot from outside the protected network)*
- *Enable encryption on management screens*

A single check box also restricts outgoing services to the following :

- *Telnet (port 23)*
- *FTP control (port 21)*
- *HTTP (blocked on port 80, allowed on port 8000)*
- *SHTTP/SSL (port 443)*
- *SMTP (port 25)*
- *DNS (port 53)*
- *ICMP*

Finally, another check box enables external access for Equiinet technical support to provide remote diagnostics and software updates over an encrypted link.

All the NetPilot's services – Web server, FTP server, mail server – run on the NetPilot box itself, which provides the equivalent of a De Militarised Zone (DMZ). CGI scripts and the FTP server run in a "virtual NetPilot" space within the device providing additional protection, and with the latest code release, both *active* and *passive* FTP are supported.

As you can see from this, it is fairly easy to make configuration simple when you make such sweeping restrictions. However, these settings are perfectly adequate for most installations, and the firewall stood up to our most persistent attempts to break through it or disable it using Denial Of Service attacks. At least the fact that configuration options are limited means that the risk of security holes due to poor configuration is eliminated.

For those who absolutely must go further, Equiinet has implemented a basic port forwarding capability. Accompanied by dire warnings all the way, the port forwarding page is well hidden in the *Advanced Maintenance* section of the configuration utility.

Even here things start off simple, since the first screen merely provides the means to specify an internal address to which all Lotus Notes, HTTP or FTP traffic can be directed.

According to Equiinet, these represent the most commonly requested “holes” that users want to punch through their firewall. Once the IP addresses have been entered, that particular type of traffic is restricted to the appropriate port number and the destination address specified only.

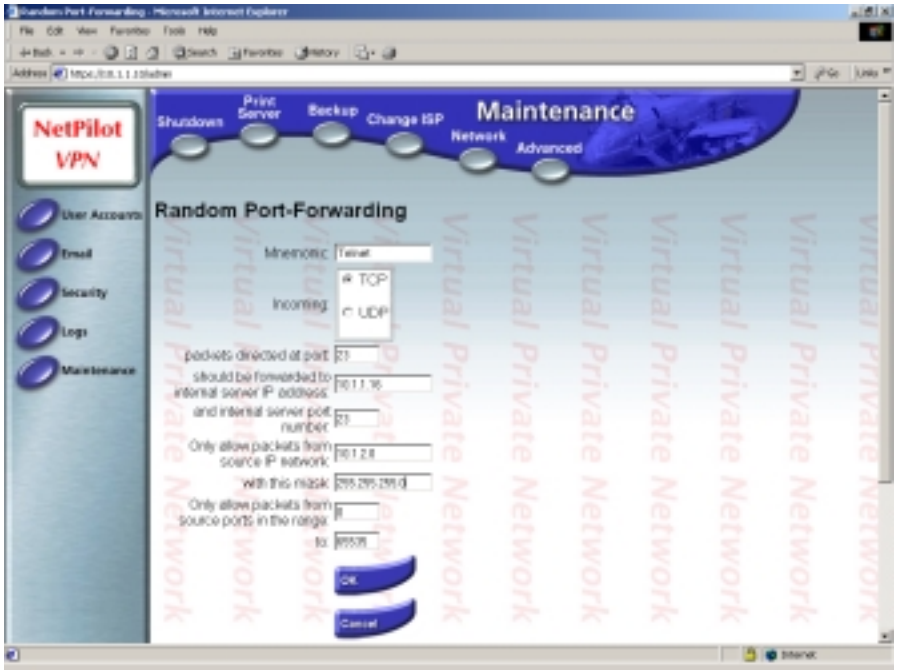


*Figure 5 - Configuring port forwarding*

However, you are then relying on the target server to implement sufficient security to prevent hackers from breaking out and wreaking havoc on your internal network. A better idea would be to implement a third network interface as a real DMZ (as opposed to the “virtual DMZ” inside the NetPilot) and allow external traffic to travel to that interface only. This, too, will be implemented as a new feature in the next release.

Finally, a facility also exists (accompanied by further dire warnings of possible security implications) to open specific ports to specific destination addresses. It is also possible to specify source IP address and port as an additional security measure, and should provide all the flexibility you are likely to need in allowing traffic through your firewall.

It would also be nice to see a similar filter definition screen for outbound traffic, providing the ability to enforce a more fine-grained control over what internal users are allowed to do than is presently possible.

As with most firewalls, extensive logs are available showing all rejected packets and alarms raised as a result of suspected Denial of Service attacks. These logs are far from pretty, and do not provide any form of selective filtering, thus making them very difficult to follow. But at least they provide the means to track nefarious activity.

Log rotation is based on both time and size of log file, and as each is rotated it can be e-mailed to the supervisor. A maximum of four backup logs files is held on disk along with the current log.

In the current release, the firewall remains fairly basic, although still very secure. If Equiinet wishes NetPilot to be taken seriously as a true, stand-alone, dedicated perimeter firewall device, some further development work is required to make the whole firewall capability much more flexible in general. An additional Ethernet interface designated as a true DMZ would also be an attractive addition. It bears repeating that this is not in any way a criticism of the *security* of the built-in firewall, merely its *flexibility*.

## Virtual Private Network

With the advent of the Internet, the opportunity has arisen to provide temporary links across the public network between companies and sites. Instead of creating a true private network over dedicated connections with all its attendant costs and management issues, we can make use of the Internet to provide a *Virtual Private Network* (VPN).

Rather than maintaining an expensive point-to-point leased line, a company can connect each office or Local Area Network to a local Internet Service Provider (ISP) and route data through the Internet, thereby using shared, low-cost public bandwidth as the communications backbone.

VPN's are not limited in the number of LAN's or nodes that can be included in the virtual WAN. For a company that has numerous sites to link, this can result in significant savings when compared to maintaining a network of leased lines.

This is technology that can be employed by companies of any size too. Not all companies require even as much as 64 Kbps for their Wide Area Network, and VPN's can be set up to work at speeds slower than is possible with leased lines. A small company or branch office can use standard analogue modems and cheap Internet accounts to create a worldwide private network.

Nor does a VPN need to be a permanent link. Dial-on-demand virtual networks can be created using analogue modems or ISDN for those sites that don't require a full-time connection. When a user on the LAN needs to access the WAN, a modem or router automatically connects to a nearby ISP and starts sending data across the Internet.

VPN links can be set up with little effort and removed just as easily. In addition, client-to-server VPN's can be created on demand between remote user PC's and a firewall or VPN termination device at head office. This provides the means for roaming users to have access to corporate networks no matter where they may be located.

Implementing a secure VPN to connect remote PC users to the local network results in significant cost savings for businesses. A VPN reduces the number of modems and telephone lines required centrally to support dial-in networking, and dramatically decreases long distance charges since remote PC users would connect to their local ISP instead of dialling direct to head office.

Of course, with all this sensitive corporate data flying around the public network, security becomes a primary concern. Unprotected data sent across the public Internet is susceptible to being viewed, copied or modified by unintended individuals or organisations. Data can be tampered with en route and valuable systems can be sabotaged.

Both ends of the tunnel must ensure beyond any measure of doubt that they are communicating with a valid host or client at the remote end of the link. Once the link has been established, data travelling within the tunnel must be encrypted to ensure that no one who may be eavesdropping the conversation can gain access to the raw data.

The most important considerations for Internet security are:

- ***Authentication*** *– verifying that the parties on each end of the link are who they claim to be*
- ***Privacy*** *– ensuring that transmitted content is not read or intercepted by unauthorised recipients*
- ***Integrity*** *– verifying that the transmitted data is received in an unchanged state*

The security risks involved in communicating over the Internet have deterred some enterprises from taking full advantage of Virtual Private Networks.

Doing business over the Internet — including transferring funds, obtaining and verifying credit information, selling and even delivering products — requires a reliable and effective security solution.

Current offerings in the VPN market place are more than capable of providing secure links between two locations. Some are only capable of establishing a link between two secure gateways, or firewalls, whilst others are designed to provide a client-server VPN, allowing individual remote and mobile users to establish secure links back to head office from their hotel room.

High levels of authentication and encryption – using digital certificates and powerful encryption algorithms – ensure that sensitive corporate data remains private.

# IPSec

One very important standard for the VPN world is IPSec, which defines a set of protection services and protocols that provide for end-to-end security in a VPN, whether over the Internet or in a private network.

## Traffic Security Protocols

IPSec defines extensions to the IP protocol in the form of two additional headers for IP packets. The *Authentication Header* (AH) verifies the authenticity of the packet's contents, providing authentication, integrity and anti-replay for the entire packet (both the header and the data).

The *Encapsulating Security Payload* (ESP) provides confidentiality by encrypting a packet before transmitting it.

An ESP packet consists of a control header, a data payload (which is an encrypted version of the user's original packet), and an optional authentication trailer (thus providing optional authentication and replay-detection services).

AH and ESP can be used with various authentication and encryption schemes, some of which are mandatory. The specification states that packets should be authenticated using either MD5 (Message Digest 5) or SHA-1 (Secure Hash Algorithm 1), both of which work by creating a unique “hash” or “digest” of the contents of the packet – a form of “digital fingerprint” that can ensure that the contents are not tampered with en route. Vendors are also free to add other encryption and authentication algorithms. For example, DES (56 bit) and Triple DES (where the data is encrypted three times using two or three unique keys for an effective key length of 112 or 168 bits) are commonly used for encryption. Some vendors will include other algorithms too, such as Blowfish, CAST, CDMF, IDEA and RC5.

AH and ESP can be used alone or in combination during an IPSec communication session. Both protocols use encryption keys to protect data. The difference between AH and ESP authentication is that AH authenticates the entire IP packet, including any tunnel header, while ESP only authenticates from the payload of the ESP encapsulation. This is acceptable for intranet packets that are encapsulated completely.

IPSec is policy-based, allowing the administrator to define different policies – each using different algorithms perhaps – for different tunnels. One example of how this can be used is to allow an administrator to enforce different levels of protection depending on whether the tunnel extends across the public network or is contained within a private network.

## Key Exchange

IPSec allows both manual and automatic key exchange. However, in order to maintain scalability when used on a wide scale, automatic key exchange is recommended.

Automatic key exchange is defined by a number of Internet drafts, but the main framework is described by the Internet Security Association Key Management Protocol (ISAKMP). ISAKMP is designed to be key-exchange independent; that is, it is designed to support many different types of key exchange. However, there is an Internet draft defining a specific public key-based approach for automatic key management, known as *Internet Key Exchange* (IKE).

There are four distinct methods of authentication in IKE: authentication with pre-shared keys, authentication with digital signatures, and two methods of authentication using public key encryption. IKE provides a facility for identification of different certificate authorities (CAs), certificate types (e.g. X.509, PKCS #7, PGP, DNS SIG and KEY records), and the exchange of the certificates identified.

## Security Associations

A Security Association (SA) is the method IPSec uses to track a given communication session. It defines how the communicating systems will use security services, including information about the traffic security protocol, the authentication algorithm, and the encryption algorithm to be used.

SA's also contain information on data-flow, lifetime of the SA and sequence numbering to guard against replay attacks.

IKE allows multiple policies to be defined with different configuration statements. SA's are then negotiated dynamically between two IPSec systems, coming to an agreement over which algorithms to be used and the level of authorisation for a range of addresses, protocols and ports that will be protected by the SA.

A given SA can use ESP or AH, but not both. If a connection needs both protocols, it needs to establish two SA's for each direction (four for a bi-directional connection).

## Tunnel and Transport Mode

Once a tunnel has been established, there are two possible modes of operation.

In *Tunnel Mode* the entire IP datagram (header and payload) is encrypted and transmitted between the two tunnel devices. The receiving device decrypts the packet and forwards the original datagram to the destination host. The advantage of this is that no changes are required to end systems in order to take advantage of IPSec security. Another advantage is that the encapsulation of the original IP header removes the opportunity for traffic analysis on the wire since the original source and destination addresses can be hidden.

*Transport mode,* on the other hand, is only used between VPN hosts. It encapsulates and encrypts only the data portion (payload) of each IP packet, but leaves the header untouched. When a host runs ESP or AH, the payload field is the data that normally follows the IP header (for example, a TCP or UDP header followed by user data). Transport mode is less secure than tunnel mode, since it does not conceal or encapsulate the IP control information.

Unfortunately, flexibility in the standard can result in interoperability problems, making life extremely difficult for the prospective VPN user. There is supposed to be a "lowest common denominator" which will ensure that any truly IPSec-compliant products should be able to communicate with each other, but at the time of writing independent IPSec certification is the only way prospective purchasers can be certain that products from different vendors will interoperate successfully.

## NetPilot VPN Configuration

Normally, configuring IPSec VPN tunnels is not an entirely straightforward operation, there being a large number of possible parameters that require setting correctly at each end of the tunnel. As with other areas of NetPilot, however, various assumptions have been made in terms of the default security policy, keeping the number of configurable options to a minimum. The administrator thus does not have to worry about the relative merits of DES or 3DES, AH or ESP, MD5 or SHA-1, or whether to use Perfect Forward Secrecy (PFS) – the NetPilot simply removes all of these choices (although the default choices are all documented fully for when it is necessary to create tunnels between NetPilot and third party IPSec devices). This makes the NetPilot VPN the easiest to configure and deploy that we have ever seen in our labs.

Any number of site-to-site profiles can be created and activated simultaneously, allowing complex multi-site *hub* or *mesh* tunnel arrangements to be supported. Each profile consists of a minimal number of parameters, though it is obviously important that the matching entries are made for each end of the tunnel.

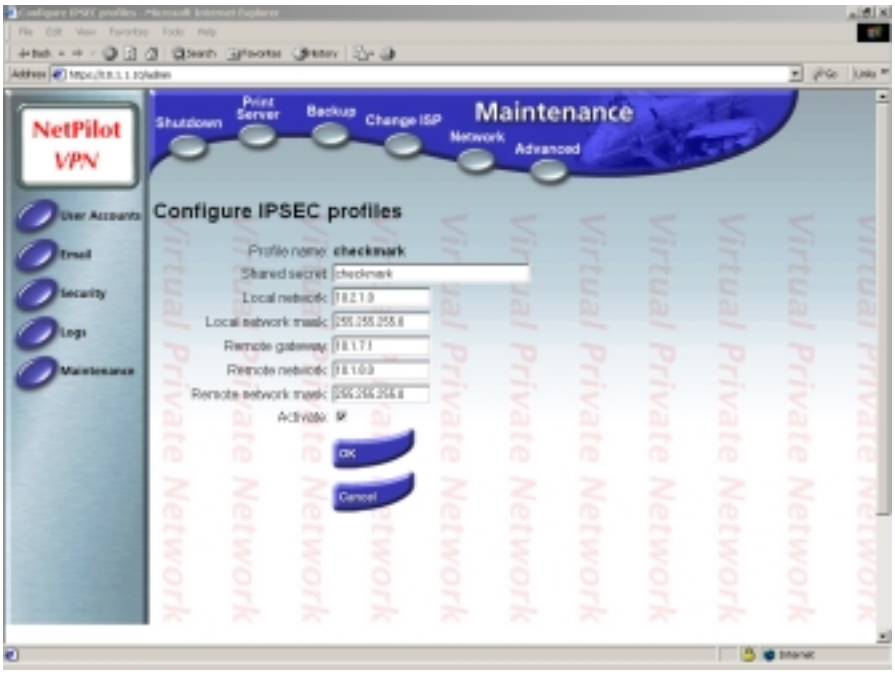


*Figure 6 - Configuring site-to-site VPN tunnels*

Digital certificates are not supported for IKE authentication, only pre-shared keys, and a lengthy random alphanumeric string is generated automatically each time a new profile is created – it is also possible for the administrator to create and apply his own shared secrets, of course.

In addition to a unique profile name and shared secret, each end of the tunnel also needs to know the IP addresses of the local and remote networks, and the remote security gateway address. Note that the WAN address needs to be fixed, at the time of writing, meaning that dial-up ISDN accounts could cause problems for VPN users.

Once all the entries have been created for one end of the tunnel, the NetPilot software helpfully displays the corresponding settings for the remote end, thus helping to reduce the possibility of error. A single checkbox can then be used to enable or disable individual profiles. From powering up the NetPilot, we had our first VPN tunnel up and running in less than three minutes!

Note that once a tunnel has been established between two sites, NetPilot can then control Web and FTP access via its firewall capabilities, perhaps preventing users from browsing Web servers at the remote end of the tunnel.

In addition to multiple fixed tunnel profiles, it is also possible to create one "*Road Warrior*" profile. This is to support mobile/remote clients, and thus consists only of the shared secret, and local network addresses.

Naturally the remote IP address will change as mobile users are assigned different dynamic IP addresses, and this condition is handled by the NetPilot device and the VPN client software. Note that although only a single profile can be created, it will handle multiple simultaneous sessions.

Equiinet includes a limited number of VPN client licenses as part of the package, based on the SafeNet/Soft-PK V5.1.3 product, one of the most widely used IPSec clients available.

A Windows-based application, SafeNet/Soft-PK utilises a relatively straightforward graphical interface in order to configure tunnels. Of course, this is not quite as fool-proof as the NetPilot configuration, but Equiinet does provide detailed documentation to get you up and running as quickly as possible. Additional client packs can be purchased as required in bundles of 5, 10 or 50.

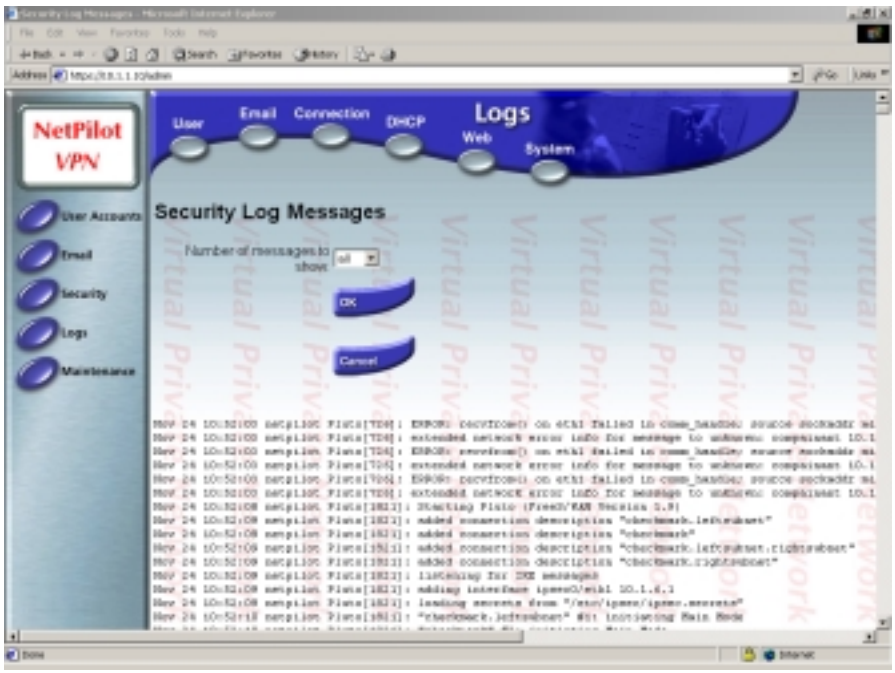


*Figure 7 - Viewing security logs to monitor tunnel activity*

The only real criticism we had on the issue of configuration is that the option is buried in the *Maintenance/Network* submenu rather than in the *Security* menu where we believe it belongs (along with the firewall capability). The other potential problem is that NetPilot does not support DES encryption, even though this is a part of the IPSec standard.

The reason for this is that the developers feel that DES is too weak for secure communications in today's networks and thus they do not allow it as an option. Laudable sentiments, but that does mean that NetPilot will not interoperate with other IPSec products which have not yet implemented 3DES. For NetPilot-to-NetPilot communications, of course, this is a moot point.

One final point which refers to the product as a whole, not just VPN – it is worth noting that since NetPilot is largely controlled by software, future product enhancements can be downloaded from the NetPilot web site free of charge and quickly applied via a straightforward option in the Maintenance menu.

# VERDICT

NetPilot is suitable for a wide variety of end-user companies, ranging from single site companies who have never used the Internet to large corporations who want an efficient means of interconnecting their branch and head offices.

Even if an organisation has only two PCs that require Internet access, NetPilot provides the means for both users to send e-mails - simultaneously or individually - and access the World Wide Web - again simultaneously or individually.

For organisations with multiple offices, or with a number of mobile users who require secure communication with head office, NetPilot provides one of the simplest IPSec VPN implementations we have ever encountered.

If you are the type that likes to fiddle with and tweak every single parameter and setting on your network devices then there is no way the NetPilot will appeal to you. NetPilot has been aimed squarely at installations with little or no IT expertise, where the simple plug and forget philosophy works extremely well.

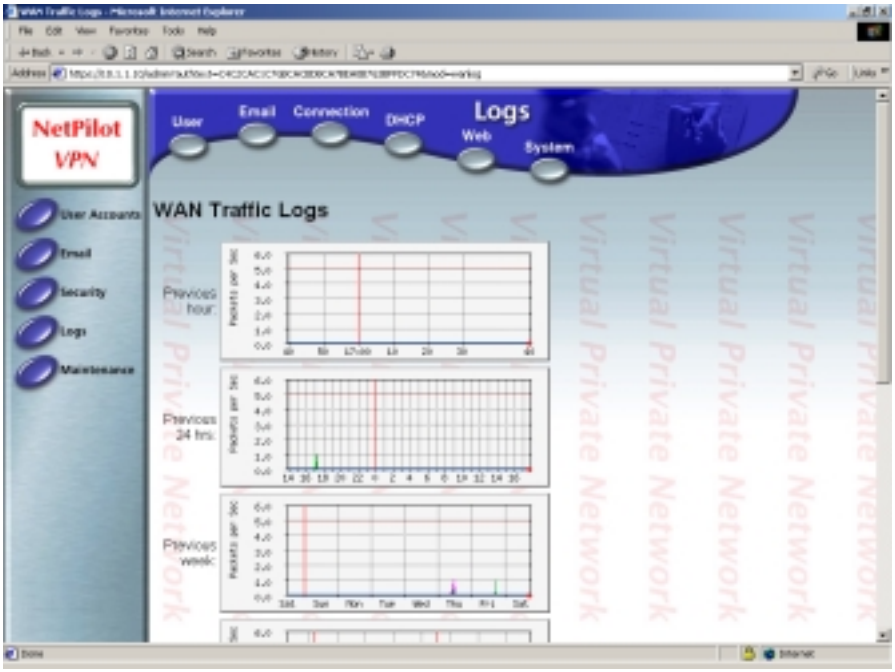


*Figure 8 - Viewing WAN traffic statistics*

You would be foolish to overlook NetPilot because it seems too simple, however. There has been a lot of work put in to making it all as automatic as possible, and when you look at the number of services and functions that have been crammed into the box, you begin to realise what a mammoth task it must have been to achieve that. The result is an extremely robust and user-friendly implementation of Linux and its main Internet services, and anyone who has ever been faced with an unfamiliar Unix or Linux prompt will certainly welcome the way that all that has been well hidden.

Behind the scenes, however, is a suite of industrial-strength software packages, providing all the services needed by the average organisation when connecting to the Internet.

At this price you could quite easily purchase NetPilot for any one of its major functions and consider the others as redundant, or as bonuses. Buy it as a Web server, and you get Web caching, e-mail and firewall thrown in. Buy it as a firewall, and you get and e-mail and Web server with it. Buy it as a VPN device, and you can disable everything else except the firewall. And so on. Use the functions you need, and leave the others disabled – it will work quite happily alongside your existing Web and e-mail servers if you like.

This "jack of all trades" approach may lead some larger customers to conclude that the NetPilot could be master of none. That would be grossly unfair, however, since as long as the built-in "restrictions" do not get in the way, the NetPilot will perform its allotted tasks as efficiently as any dedicated device. And almost without exception, it will be easier to manage.

Some improvements in the firewall and reporting capabilities to bring them more in line with the sort of features found on dedicated devices would certainly help to counter such objections, and allow the NetPilot to be much more easily deployed in larger organisations as a dedicated firewall or VPN device.

For many small-to-medium organisations, however, the all-in-one approach will continue to find favour. At the end of the day, with different boxes offering different maximum capacities (but the same software base), NetPilot is flexible enough to fit into any size organisation, providing all the Internet connectivity and services you are likely to require.

NetPilot VPN earns the "**NSS Approved**" award.

## Contact Details

**Company:** Equiinet

**E-mail:** info@equiinet.com

**Internet:** www.equiinet.com

**Address:**
Edison House
Edison Road
Dorcan
Swindon
Wiltshire
SN3 5JX

**Tel:** +44 (0)1793 603700
**Fax:** +44 (0)1793 603701

# APPENDIX A

## How We Tested

Our standard firewall testing suite is designed to ensure that firewalls achieve a basic level of protection against a number of common hostile attacks, both from inside and outside the realm of protection.

### Configuration

- The firewall is configured to provide the various services and enforce the various restrictions specified in this document
- Firewalls can be provided either as a complete turnkey hardware and software solution, or as software only to be installed on our own PC (the specification of which will be provided on request)
- All firewalls are to be provided initially with an “out of the box” configuration. This is to allow us to form an objective opinion on (a) the amount of effort needed to configure the product from scratch, and (b) the likelihood that an end user may mis-configure the product
- Software-based firewalls will be installed on a “clean” version of the native operating system. The firewall machine will be “wiped” and returned to a steady state after each test. Firewalls from different vendors will not be installed side by side on the same machine
- Firewall vendors will be encouraged to provide advice on the most appropriate means to achieve the necessary configuration. If no such advice is forthcoming, NSS Group staff will attempt to provide the best configuration possible from information contained in the manuals.
- Firewall vendors will be encouraged to visit the testing lab to effect the necessary configuration under direct supervision of NSS Group laboratory staff
- In the event multiple methods of achieving the same result are available, the vendor should advise on the most secure option
- It is assumed that the underlying OS will be “hardened” and/or have the latest security fixes applied during firewall installation. No patches or configuration options will be allowed which are not available to the general public either in a current release or via a recognised and generally available support source

### Test Environment

NSS Network Testing Laboratories maintains a dedicated test network for Checkmark accreditation (a network diagram is available on request).

- The test environment consists of three distinct networks – the external (Internet), DMZ and internal (protected)
- The external network consist of a Telnet host, Web server, FTP server, DNS server, SMTP/POP3 server and a “hacker” client
- The DMZ network consists of a Telnet host, Web server and FTP server
- The internal network consists of a Telnet host, DNS server, SMTP server, file/print server, Web server and a “hacker” client

- Machines on the internal and DMZ networks are not configured in a secure manner – they rely totally on the protection of the firewall
- The firewall is the only link between the DMZ, internal and external networks
- Firewalls that support DMZ services internally rather than on a separate subnet are also allowed. Vulnerabilities in the actual services will not be deemed cause for failure of the certification process unless those vulnerabilities provide external access to the protected network in some way.
- The link between the firewall and the external network is via a simple router. No packet filtering will be configured on this router – all protection must be provided by the firewall
- A network monitor, protocol analyser and security monitor is installed on the external, DMZ and internal networks
- The configuration of all machines remains constant between tests. The machine designated as the firewall will be "wiped" and returned to a steady state after each test.

## Services

The firewall is to be configured to allow the following services, typical of most installations:

- *Telnet (outbound, no restrictions)*
- *Telnet (inbound denied)*
- *FTP (inbound to DMZ (or equivalent) only)*
- *FTP (outbound, no restrictions)*
- *HTTP (inbound to DMZ (or equivalent) only)*
- *HTTP (outbound, no restrictions)*
- *SMTP (inbound to corporate mail server only)*
- *SMTP (outbound, no restrictions)*
- *DNS (internal clients to be able to resolve both internal and external addresses freely)*
- *DNS (no internal addresses to be resolved from the external network)*
- *POP3 (internal clients to be allowed to retrieve POP3 mail from the external network)*
- *POP3 (no external POP3 access to internal servers is allowed)*
- *ICMP (inbound denied)*
- *ICMP (outbound denied)*
- *"Stealth mode" (if available) should be enabled*
- *No other traffic of any description to be allowed onto the protected network or DMZ*

## Management

Management of the firewall will be evaluated using the following criteria:

- Local console must be secure
- Management console should not be open to the external network
- The firewall configuration should be fully protected and tamper proof (except from an authorised management station)

- Full authentication is required for the administrator for local administration
- Full authentication and an encrypted link is required for remote administration. If the remote link cannot be encrypted, there should be the ability to disable it.

## Tests

A range of tests will be carried out using commonly-available firewall scanning tools (NAI CyberCop Scanner, ISS Internet Scanner, SecureScan NX, Nessus, etc.) as well as custom-built utilities. All tools will be configured with full knowledge of both the firewall and network configuration:

- Check that firewall management console is not available to any users unless authenticated
- Check that the remote management link (if available) is encrypted or can be disabled
- Check that the firewall configuration is fully protected and tamper proof
- Check that the firewall is resistant to a range of known Denial Of Service (DOS) tests
- Check that the firewall has no known vulnerabilities.
- Check that the underlying OS is hardened and not vulnerable to known OS-specific attacks
- Check that all specified outbound services (and no others) are available from internal clients
- Check that all specified inbound services (and no others) are available to external clients
- Check that the firewall does not allow uncontrolled access to either the internal or DMZ networks
- Check that DNS names can be resolved from internal clients
- Check that external DNS queries do not reveal information about the internal network
- Check that the firewall does not pass mis-configured packets to the internal network or DMZ

Tests will be repeated in the following manner:

- *Stage 1: Probe the firewall from the Internet*
- *Stage 2: Probe the protected network from the Internet*
- *Stage 3: Probe the DMZ from the Internet*
- *Stage 4: Probe the firewall from the protected network*
- *Stage 5: Probe the Internet from the protected network (test security policy)*
- *Stage 6: Probe the DMZ from the protected network*
- *Stage 7: Probe the firewall from the DMZ (if available)*
- *Stage 8: Probe the protected network from the DMZ (if available)*

## VPN

Multiple sets of the above penetration tests are executed against NetPilot VPN boxes both with and without VPN tunnels active to prove the resistance capabilities of the VPN product.

The following tests are also be performed in an attempt to validate the cryptographic qualities of the product:

- *Stage 9: Ensure all data passing through tunnel is encrypted and integrity is maintained*
- *Stage 10: Analyse encrypted data for obvious patterns or weaknesses*
- *Stage 11: Attempt to replay encrypted packets with amended contents and ensure that these are rejected and reported*
- *Stage 12: Confirm integrity of crypto functionality via implementation questionnaire*

## Results

Protocol analysers, network monitors and advanced security monitoring tools are used during initial configuration and throughout the testing, both to validate the configuration and confirm the test results.

- No access to protected servers is permitted from the “untrusted” network
- No internal data is to be allowed outside the protected network
- No “illegal” traffic is to be permitted on any protected segment
- No access to the management console or NetPilot configuration files is to be allowed
- Log files to log all rejected packets and port scans
- Device is to remain running through DOS attacks (both generic IP and OS-specific attacks). Where it is recognised that a particular DoS attack has no defence, the device should terminate “gracefully” (leaving connections securely closed).
- Log files to remain intact through any log flood or DOS attacks
- The management console must remain available and secure
- The VPN should only allow tunnels to be negotiated between two trusted hosts
- All data travelling through the tunnel is to be encrypted and integrity maintained
- Encrypted data to show no obvious signs of patterns, repetitions or other weaknesses
- Crypto implementation proved via questionnaire