



## **VPN (Virtual Private Network)**

Traditionally, multiple site organisations that want to communicate with each other have connected via leased-line or ISDN dial-up from each remote site, which are both expensive options. Equinet has now enhanced its NetPilot Internet Server Appliance to ensure it is ideal for this type of application, while providing a great deal of added functionality. More and more businesses are setting up Virtual Private Networks. The Equinet solution provides a highly secure VPN across the very cheap public network that is the Internet, using a server appliance with all the functionality you need in one box - router, firewall, email server...and the list goes on.

By installing the VPN option in conjunction with NetPilot or NetPilot Enterprise, organisations can establish totally secured VPNs between their sites using existing Internet connections. Secure networks can be easily established. Other Internet activities, such as web browsing and the transferring of email to and from other destinations around the world, can still continue. If sites already have permanent (non-dialup) connections to the Internet, then you need no more than a NetPilot plus a VPN software upgrade at each site to establish totally secure VPNs.

It's also possible to establish VPN connections from remote sites that have NetPilots with ISDN connectivity, to a centrally located NetPilot or Enterprise which has a permanent Internet connection via leased line or DSL. Note a fixed, static IP address, is required whether the NetPilot or Enterprise is connected through a fixed leased line, DSL or dial up ISDN. (Only VPN single user client configurations can operate with a dynamic IP address).

The NetPilot VPN implementation also provides remote access to, and administration of, NetPilots and associated local networks. All these functions are achieved at low cost - using the Internet - and are totally secure. Also provided is the functionality to remotely access email on NetPilot or an office mail-server on its LAN, from anywhere in the world. From home or hotel, an office network is securely accessible for the cost of a local phone call if Internet access is available - no more direct dialing to a RAS server is required. A suitable IPSec client installed on the PC or Notebook being used to remotely access the NetPilot is required for this capability.

IPSec VPNs IPSec, which stands for Internet Protocol Security, is a solution that addresses the issues relating to the security of data being sent across the Internet. In reality, it's a complex suite of industry standards defined by the Internet Engineering Task Force (IETF), with the assistance of many vendors, to tackle data encryption and integrity. In practice, it's a tool users of the Internet can employ to ensure the security of data and the authenticity of the sender when transmitting and receiving information across public networks such as the Internet.



### **A Total Security Gateway Solution**

NetPilot's Checkmark accredited firewall is further enhanced with the addition of IPSec. As well as providing total security for the local network, NetPilot plus IPSec can offer the same security for data traveling between networks across the Internet.

### **What NetPilot and IPSec offers**

The most common use of IPSec is to provide Virtual Private Networks (VPNs), but Equinet's NetPilot implementation of IPSec also provides remote access to, and administration of, NetPilots and associated local networks. All these functions are achieved at low cost - using the Internet - and are totally secure, to protect against electronic eavesdropping and man-in-the-middle attacks.

### **Virtual Private Networks**

By incorporating IPSec, organisations can establish totally secured VPNs between their sites using existing Internet connections. A labyrinth of secure networks can be established in no time at all without the cost of expensive permanent site-to-site connections or the disruption caused by cabling installation engineers. And what's more, other Internet activities, such as web browsing and the transferring of email to and from other destinations around the world, can still continue in conjunction with this. If your sites already have permanent connections to local Internet access providers, then you need no more than a NetPilot plus IPSec software upgrade at each site to establish totally secure VPNs. It's also possible to establish a VPN from a site that has an ISDN connected NetPilot, note a fixed static IP address is required.

### **Remote Email Access**

An IPSec upgrade to NetPilot also provides the functionality to remotely access email on NetPilot or an office mail-server on its LAN, from anywhere in the world. From home or hotel, an office network is securely accessible for the cost of a local phone call if Internet access is available. No more direct dialing to a RAS server, no more dedicated office telephone lines for RAS, and no more waiting for another user to drop the line - many can share the same Internet connection. All that's required is an IPSec-upgraded NetPilot installed at the office and permanently connected to the Internet. A suitable IPSec client installed on the PC or Notebook being used to remotely access the NetPilot is also

### **Remote Administration**

NetPilot, and the network resources it protects can now be securely administered over the Internet from remote locations. Support centres can easily administer many NetPilots simultaneously over a single Internet connection. Even network resources located behind NetPilot could be securely supported. All that's required is to apply the NetPilot IPSec upgrade to the NetPilot, and ensure that it has a permanent connection to the Internet. 24 by 7 by 365 couldn't be made easier either. Out of hours support for customer and client NetPilots, and local network resource could be provided by engineers located at home if their PC is equipped with a suitable IPSec client, and they have local access to the Internet. (note - client may not work through local router or firewall).



### **Interoperability**

As IPSec is the de facto standard used by virtually all vendors of firewall and Internet security devices, it allows for interoperability between these products. NetPilot's IPSec solution should enable its NetPilot product range to establish a VPN with other vendors' products supporting IPSec with 3DES encryption.

### **Performance characteristics**

As with any Internet connection, the performance seen by a user depends upon many factors, which include the size (bandwidth) of the local Internet connection, the size of the Internet connection at the remote site, the number of other simultaneous users at both sites, and the quality of all connections in-between.

When using a VPN the same factors come into play. For the aforementioned reasons it is not possible to give definitive performance characteristics, but as a guide, we would suggest the following as typical.

NetPilot with a 128Kbps Internet connection  
Maximum tunnels passing data simultaneously - 3  
NetPilot Enterprise with a 2Mbps Internet connection  
Maximum tunnels passing data simultaneously - 20

It should be noted that NetPilot does not limit the number of active configured tunnels. Many more than indicated above could be achieved if the Internet connection is used for no other purpose, and data passing through the tunnels is low and of a sporadic nature.