TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

CAPITA
• Education Services •

Technical Guide – SIMS.net Remote Working

Module	Standard Architecture
Author	Phillip Hamlyn Chief Architect
Revision Number	3.0
Last Edited	11th June 2004

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

CAPITA
• Education Services •

Purpose

This document is issued by the CES Architecture team to act as a guide to the capabilities and recommended practises for operating SIMS.net in a distributed environment. It covers discussion of client-server and browser technologies and their applicability to our customers.

This document is intended to be made available to CES customers.

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

Background

SIMS.net is a highly efficient and scalable product suite designed specifically to be bandwidth efficient and use only standard communication protocols to run out-of-the-box on LAN and wireless LAN networks with the minimum of resource usage. It is fully capable of running on connection speeds of as little as 28kbps[1] and giving an acceptable end-user experience, there are many ways to exploit this efficiency of design, the internet, dial-up Remote Access Services, Terminal Services etc. which is best and what are the security implications of them ?

Bandwidth Efficient Design of SIMS.net

What is the definition of "bandwidth efficient" and how is it achieved in SIMS.net ?

The CES architecture team define a product to be "bandwidth efficient" if it uses the minimum amount of transferred bytes for the user to carry out iterative transactions. This means

1. The application should request data from the network only when the user explicitly asks for it

   This is why SIMS.net does not automatically fill Browser windows with all the data available but asks for the user to enter some search criteria first.

2. The application should cache data that it requires if the user carries out iterative transactions

   For instance; reading multiple students details downloads the list of registration groups only once irrespective of the number of students looked at.

In addition a bandwidth efficient application should make as few calls to network resources as possible. "IP Lag" on a wide area network[2] is an irreducible overhead on each network call and poor resource usage can lead to this lag becoming performance damaging. This means

3. The application should batch up database calls instead of making them one at a time.

   Saving a student and associated contact and medical information is made in SIMS.net in a single database call rather than one call per item changed.

   Loading the academic year structure is carried out in a single network call.

Bandwidth efficiency is a measure of the quantity of calls across the network and the quantity of data passed as part of that call. Too many calls across a wide-area network incur damaging levels of lag, and calls which return too large an amount of data consume bandwidth. In addition to their raw bandwidth consumption, on a wide area network some kind of encryption of data will be operating and the cost in time and processor power required of encrypting the data is proportional to the volume of data being handled. In an encrypted wide area network, like the internet, bandwidth efficiency is doubly important to give good transmission speed through narrow links (like modems) but also to allow the encryption routines on the client and server to operate efficiently.

How does this benefit the customer ?

Bandwidth efficient applications are faster to operate than bandwidth hungry applications and required lower speed connections to operate. This means that expensive infrastructure such as Wide

---

[1] This does not include retrieval of stored documents from the SIMS document server which may take time proportional to the size of the document stored, which is outside the control of CES.

[2] This is the amount of time taken for the packets to pass through the various routers and transmission media. It varies but can be as high as 0.2 seconds. Five sequential database calls will therefore seem to the user to have a delay of one second. SIMS.net avoids sequential database calls by highly efficient database access coding.

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

Area Networks across Local Education Authority or School Consortia can be used for education traffic instead of administrative traffic.

Bandwidth efficient applications also work very successfully on the low bandwidth wireless networks that are becoming popular within schools. Wireless network hubs can be as low as 4mbps compared to a standard minimum hub of 10mbps or 100mbps, and the wireless hub needs to share this bandwidth in an unplanned manner between whoever is in the proximity. Standard wired hubs have a planned number of connected users and can be deployed accordingly. Wireless network hubs can therefore benefit greatly from applications that are bandwidth efficient.

How does this compare to "thin client" and internet browser applications ?

Thin Client

Thin client applications (Windows Terminal Server and Citrix Metaframe) are used as a way of managing application deployment over a network and comprise of a central Terminal Server and multiple lower specification client machines[3]. The Terminal Server runs a virtual session of Windows on behalf of every client machine and sends the screen image of that Windows session to the client machine. This setup is extremely easy to maintain since a standard virtual Windows environment can be set up for every user on a network without reference to the varying specifications of hardware present on the network.

There are several issues with this configuration

- The Terminal Server needs to be a reasonably high specification of hardware (after all it is running a whole networks worth of users applications) and can lead to some complication in installation, and active management of the server is necessary to achieve a balanced performance.
- There is a requirement to send the entire screen to the client computer when the user requests some data. This transmission is normally cleverly compressed and only the changes to the screen are sent, but nonetheless it includes both the data the user wanted to see and the screen image of the application providing it. This is not as efficient use of bandwidth as the same application used in client-server mode since in that configuration only the data is sent to the client machine.
- Every time the user alters the view of the virtual Windows session (by moving or resizing a window for instance) network calls must be made first to transfer the intent of the user, then to show them the result of their interaction (on a standard client-server configuration these network calls are not made because it all happens in the client PC). In order to make this an acceptable experience the connection can be a low bandwidth but should have as little transmission lag as possible. This is not a good start for an internet based distributed environment where neither large bandwidth nor low lag can be guaranteed.

SIMS.net is not normally tested on thin client configurations due to lack of time and resources, but since it is a standard Windows application there is no expectation that it will not work successfully.

[3] In the future Microsoft are indicating that they see this type of setup being used for "Smart Devices" being a touch screen, minimal operating system footprint, RAM, a low speed processor and a radio LAN card. These are much closer to the original intention of "thin client computing" championed by Sun Microsystems.

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

Internet Browser Applications

CES made an active decision not to deploy browser based applications within schools because of many factors,

- Incompatibilities between browser versions and vendors
- Restricted scope for user interface design
- Poor integration with other applications

Internet browser applications suffer from some of the problems of Thin Client configurations

- Each time the user requests data from the server, the entire screen is resent back to the client application along with the data requested. This requires a higher bandwidth than a client-server application which only requires the data itself.
- Browsers use HTML to describe their screens and data content. This protocol is uncompressed and text based which is part of its strength; but it is also a very inefficient protocol for transmitting data and screen descriptions. In addition to this the server cannot carry out the kind of clever compression algorithms used in Thin Client configurations because browsers aren't equipped to cope with partial or compressed data.
- There is a single server within the network generating screen layouts and integrating them with the requested data, for every user, in response to every request, on an ad-hoc basis. This over-centralisation can lead to tricky deployment (an Internet server is required) and requires further load balancing between the internet server and the database server.

Browser based applications are best used when one of the following is needed

1. Anonymous access where the user doesn't have or doesn't want to install the application software (as is the case with Parents Gateway).
2. The destination operating systems cannot be known by the system designers.

Recent developments mean that it is possible that the future of internet browsers as an application hosting environment may be narrowed even further[4] to that subset of applications designed for use by the public on the public internet.

Using SIMS.net For Remote Working

The design of SIMS.net has made it possible to use it over low bandwidth networks such as dial-up modems in a more bandwidth efficient manner than either thin-client or browser based alternatives. How can a customer make use of this ?

- A teacher marking papers can work at home and submit the marks directly into SIMS.net via a standard dialup internet account.
- A multi-site school can run SIMS.net through their broadband internet connection.

[4] Microsoft have extended the browsers capabilities with the .net technology such that a Windows Internet Explorer browser will down automatically download and execute Microsoft .net applications without security risks. This facility is not well used at present and will of course only work on a Windows operating system that has the Microsoft .net framework installed. Unfortunately, or perhaps from a security point of view, fortunately, applications downloaded like this must be given explicit permissions to access the workstations hard disk drive or any other non-browser resource (including talking to other applications like Microsoft Office).

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

- An LEA or technical support consortia can host the SIMS.net database and document servers remotely from the schools they serve centralising backups and giving the ability to guarantee service provision, and distribution of system updates. The schools need only have an internet connection to be able to reach their data, not a dedicated broadband link.

The Threat Environment

Transmission Interception

Because SIMS.net contains sensitive personal data CES do not consider it reasonable to send this data unencrypted over a publicly accessible network. The Local Area Network within a school is physically secure from intrusion attempts and we do not consider the traffic on it to be under threat from "packet sniffing"[5]. In the case of a large school we would expect the administrative and academic networks (i.e. student and teacher networks) to be logically or physically separated to prevent enterprising students from seeing administrative data in transmission.

Sensitive personal data sent over the public internet should be encrypted using public/private key encryption either via Secure Sockets Layer (SSL, seen in Internet Explorer by the end user as "Certificates"). Microsoft SQL Server by default sends all its data out on port 1433 unencrypted but it is possible to change the port number with Internet Information Server to a port that is secured using SSL and thereby encrypt all traffic between a client computer and SQL Server.

Point of Presence Attack

SQL Server

If SQL Server was exposed to the internet by loading it onto a PC which had a live internet connection, anyone in the world could attempt to connect to it. This is what happened when the "slammer worm" was released. All that stands between a hacker and the data held in the database is the system administrator user name and password. Assuming the system administrator user name and password are human readable this can be cracked using a "dictionary attack" within a few hours or days.

SQL Server can be told to log failed connection attempts and you can interrogate this log to spot such an attack, but the only remedy is to remove your SQL Server service from the internet until you can get your firewall to block the IP address from where the attack is originating.

Because of the active monitoring and management required for this CES do not recommend diverting resources by deploying SIMS.net in this manner unless you already have application similarly deployed and are already doing this monitoring. Care should be taken on small establishments that the SQL Server and internet connection server are firewalled to prevent internet traffic from being able to reach the SQL Server port.

In addition to the possibility of dictionary attack the protocol (ADO) carrying the login and data requests has not been secured to the degree that HTTP has and could itself be the subject of buffer overrun and other kinds of attack. There is no way of preventing this.

Internet Information Server

IIS has been the subject of continual attacks and new vulnerabilities are discovered monthly. The time lag between a defect being exploited and Microsoft making a fix available constitutes a window of

[5] Some brands of wireless network card do not have encryption capabilities and broadcast their data to any listening wireless network device.

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

vulnerability which needs to be carefully evaluated by a network administrator such that any exploits which may have occurred during this time lag are dealt with after the fix is employed.

Such is the reputation of IIS that it has become a magnet to attackers using predefined scripts to scan for, and exploit, every single known vulnerability that's ever existing in IIS. The ease with which an inexpert but motivated ICT student could mount a serious penetration attempt on a public IIS server means that IIS needs active expert management to guard against threats. In some larger schools this expertise may be present but for the majority of Capita's customers this would be an additional administrative burden.[6]

Solution 1 : Internet Using Virtual Private Network

A Virtual Private Network (VPN) is an encryption and authentication protocol which can be installed on client and server machines and allow them to use the internet as though is were a Wide Area Network without any of the machines being physically connected to each other.

All traffic between the nodes of the network is strongly encrypted as are all attempts to log into the network. Centrally a VPN server handles the incoming connections (from anywhere in the world through the internet) and authenticates and services the encrypted Secure IP packets.

Windows 2000 and XP have support for this build into the operating system and can operate a VPN out of the box.

Software VPN servers like Windows 2000 and XP have a limit to the number of concurrent connections they can support, and this number is related to the actual volume of data being transmitted by the workstations. Using SIMS.net this data volume much smaller than with the equivalent browser based system (in our tests somewhere between 5-6 times more efficient) but at some point a software VPN server will become saturated and start providing poor performance. This will be the situation where a school's internet access is provided by a local Grid arrangement through their LEA or other support provider. In this scenario the VPN server would be located at the "edge of the internet" within the remit of the LEA rather than the school. The LEA VPN Server would have to be able to handle a considerably larger volume of traffic than the software-only Windows XP VPN Server is capable of handling and so a hardware VPN server would need to be installed. Hardware VPN servers carry out the same basic task as hardware-based Firewalls and Routers with the addition of carrying out the encryption and decryption tasks in hardware rather than the operating system software, and are available from many vendors.

This method of communication works over dial-up, infrared, direct cable, ADSL, ISDN connections and is CES recommendation for operating SIMS.net remotely. SIMS.net users benefit from the careful attention to bandwidth consumption designed into the product which means that only the absolute minimum of data is being transmitted over this secure link and reducing the overhead of encryption and decryption that is entailed.

Solution 2 : Dialup Access Using Remote Access Services

A Remote Access dialup allows a user to dial into their place of work to a designated telephone number and get a network connection. Because this method is a direct connection from the workstation to a server it doesn't use the internet for its data transmission, and therefore is inherently

[6] Other web servers are less attractive to attacker – partly because they are less popular, and partly because they are mounted on more secure operating systems. A school using one of these web servers should carry out similar active management of them even though they're less vulnerable.

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

secure. This method is best used for occasional offsite working as it requires a modem at the server for each incoming call. In addition to this limitation the call must be placed from the workstation directly to the school incurring related local or long distance call costs.

SIMS.net users again benefit from the low bandwidth consumption of the application because SIMS.net is fully operable over a dialup link like this.

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

Appendix 1 : VPN Configuration Links

The following links detail how to set up a Virtual Private Network under Windows XP and Windows 2000. Windows 98 requires a free update from Microsoft and follows a slightly different configuration pattern.

Note that the Virtual Private Network server does not need to be a server edition of the operating system, but must be either Windows 2000 Professional or Windows XP Professional or above. The operating system edition for the workstation is not restricted.

Windows XP : Guide to setting up a Workstation for a Virtual Private Network

HOW TO: Configure a Connection to a Virtual Private Network (VPN) in Windows XP

Microsoft Knowledge Base Article 314076

Windows 2000 : Guide to setting up Workstation and Server for a Virtual Private Network

HOW TO: Install and Configure a Virtual Private Network Server in Windows 2000

Microsoft Knowledge Base Article 308208

Virtual Private Networking with Windows 2000: Deploying Remote Access VPNs

Microsoft Technet Article, general discussion of various configurations for a VPN.

http://www.microsoft.com/technet/treeview/default.asp?url=/technet/itsolutions/network/deploy/depovg/vpndeply.asp

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

Appendix 2 : How-To Set Up SIMS.net on a Windows XP Virtual Private Network

Generally

The Virtual Private Network (VPN) facility of Windows XP is a protocol layer which lies on top of any existing Dial-up Network or Local Area Network facilities. It allows you to open a TCPIP port to the internet and control who and what can connect to that port, and what network resources that user can consume. All traffic in and out of the port is encrypted.

SIMS.net and the Internet

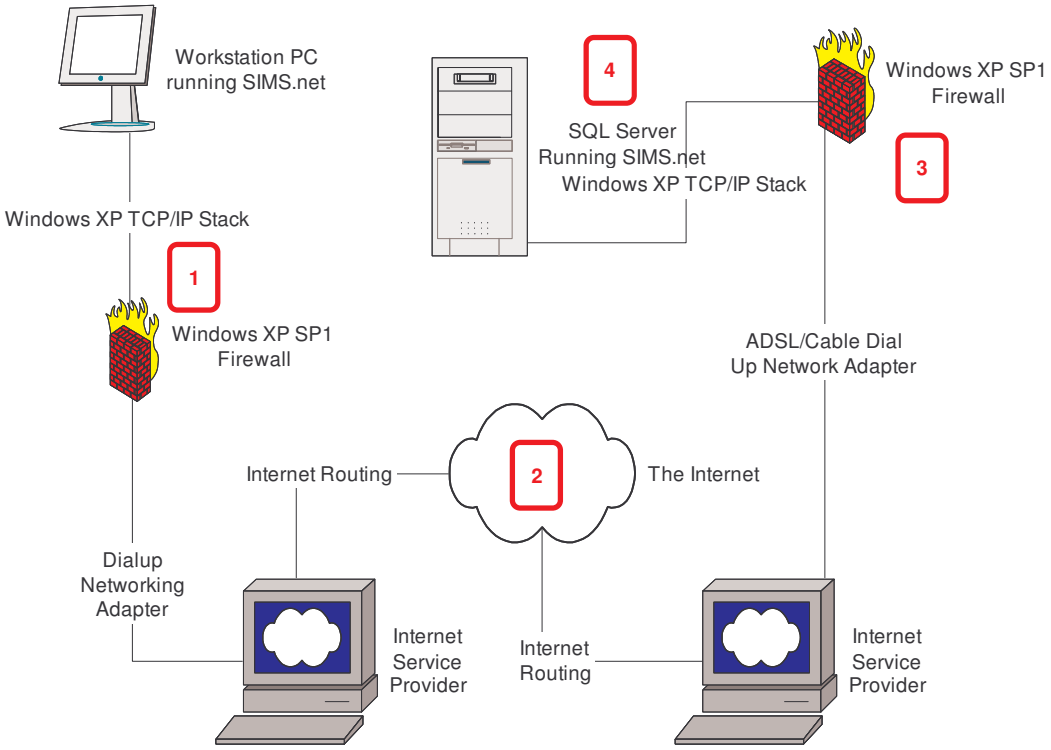
To configure SIMS.net to connect over an internet dial-up connection you must alter the text file "Connect.INI". The entry for Server= can be altered to any DNS name (i.e. Server=myschool.freeserve.co.uk) or any valid IP address (i.e. Server=124.343.23.111). SIMS.net will attempt to connect to the SQL Server (assumed to be on Port 1433) leaving the operating system to resolve this address through a domain name server or router.

CES only tests SIMS.net using TCP/IP as the transmission protocol between the SIMS.net and SQL Server. SQL Sever also supports other protocols which can be enabled or disabled using the "Server Network Utility" installed with SQL Server and MSDE. The following examples assume the communication is TCP/IP.

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

Example : What Not To Do

You could set up SIMS.net to operate over the internet as follows



Although is an uncomplicated setup there are many weak points. (SIMS.net will work extremely well in this scenario – it uses TCP/IP to communicate with the SQL Server irrespective of the number of hoops it needs to jump through. As long as the SQL Server can be pinged from the client, SIMS.net will work fast and efficiently).

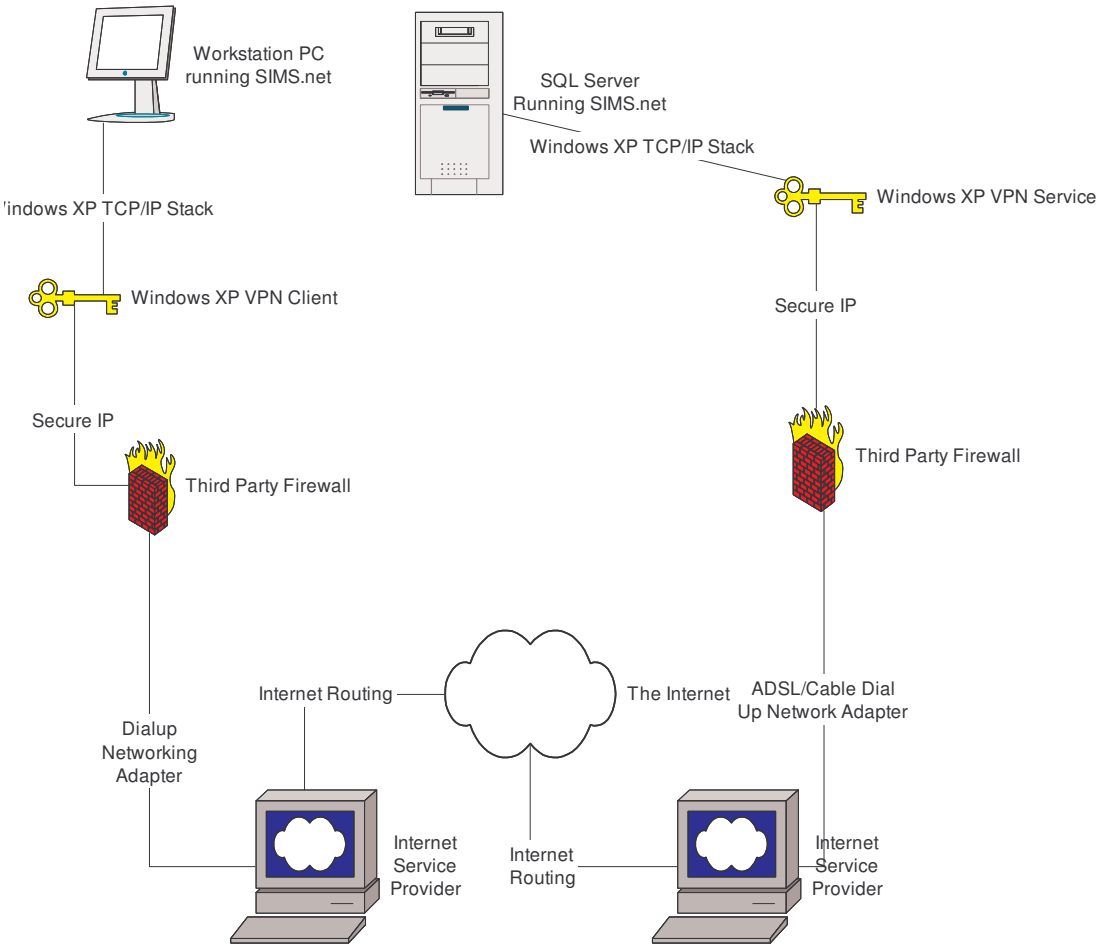
1. The Windows XP SP1 Firewall doesn't allow fine control of outgoing communications. Although the setup above assumes that it is SIMS.net which is originating the communication with the distant SQL Server, in reality any application on the workstation (including viruses or email worms) could be initiating the communication. This might seem a distant or outlandish possibility but in reality it does occur.
2. The Dialup Network Adapter and the route from the workstation to SQL Server is not encrypted – anyone can intercept and view (and modify) the information contained in the TCPIP packages. Again this seems unlikely but the possibility that this information might travel some way through an establishments network before reaching its destination – perhaps using Wireless broadcast networking links on the way, and through a forest of expert ICT students means that the possibility certainly exists.
3. The Windows XP SP1 Firewall at the server does not control access to the SQL Server based on incoming IP address. The fact the packet has got that far is enough for XP to pass it through to SQL Server. Anyone could have originated the incoming packet.

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

4. The packet passed into SQL Server through the SQL Server port (typically 1433) is assumed to contain a valid set of ADO instructions but this is not checked and this can lead to buffer overrun attacks or other exploitations.

Example : The Correct Configuration

The following configuration is achieved by following the instructions later in this Appendix. It gives the same level of flexible connectivity but controls access and encrypts data sent across the public internet. For the sake of simplicity the SQL Server is assumed to be on the same PC as the internet gateway for the establishment – this may be so in smaller customer sites but equally the gateway can be a completely separate PC.



The key differences here are

1. All communication outside the firewalls is encrypted using Secure IP[7] and therefore intercepting and examining the packets would reveal no information. They are also digitally signed so cannot be altered in transit.

[7] I have used the example of IPSec (Secure IP) here but in reality there are several supported encrypted protocols in use, some more secure than others and some supported on Windows 98 and others not.

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

2. A third party firewall[8] is in place allowing a finer degree of control over what applications and users get access to the internet. This means that a program on the Workstation has to be specifically authorised to access the internet by the user, who will then get the chance to spot and block a Trojan.
3. The Windows XP VPN Client requires the workstation user to identify itself to the Windows XP VPN Server prior to consuming any resources. It is this identification process which then allows the two to exchange encryption keys. The incoming workstation user is mapped to a predefined Server user – and in Windows XP the entire process can be subordinated to the Windows integrated security such that the workstation user maps to a domain user on the servers network.

The additional benefit given by this configuration, other than security and authentication, is that the entire resources of the LAN are available to the dial-up workstation, not just the SQL Server instance required by SIMS.net. Some LAN facilities such as Windows Explorer are not particularly suited to a slow dial-up connection but SIMS.net has been specifically designed to be bandwidth efficient. Of course full LAN access may not be acceptable to an establishment whose workstations are not trusted LAN clients (family machines owned by teachers who are working at home for instance) and the fine tuning available when mapping the VPN user to a predefined server user can be used to restrict what individuals have access to.

Setting Up the XP VPN Server

The following instructions assume a single machine hosts the SQL Server and the incoming internet connection (ADSL).

Firewall Configuration

Using the Windows XP SP1 firewall SQL Server will automatically be accessible from the Internet if it is located on the same machine as the firewall. SQL Server expects to act as a server and the XP firewall will allow any installed application to receive internet traffic. In order to prevent SQL Server being accessed from the internet you should install another firewall product. Free firewalls such as ZoneAlarm are available and some virus protection packages such as Norton Internet Security also contain firewall products.

You should configure your firewall to refuse SQL Server internet access.

You should explicitly allow the workstations IP Address, range of addresses, or DNS name to be allowed by the firewall, otherwise their incoming connection will be blocked by the firewall.

Setting up the VPN

Create a new network connection using Start … Settings … Network Connections … New Connection Wizard. Choose "Set up an advanced connection" then "Accept incoming connections". You will then be shown a list of network adapters some of which may already be ticked. This is confusing since a VPN connection is automatically applied to all network adapters irrespective of the list and selections shown here. Ignore this screen and press Next.

Select the radio button "Allow virtual private network connections". You will then be presented with a list of known users and you should select the ones who are allowed to connect as VPN clients. The

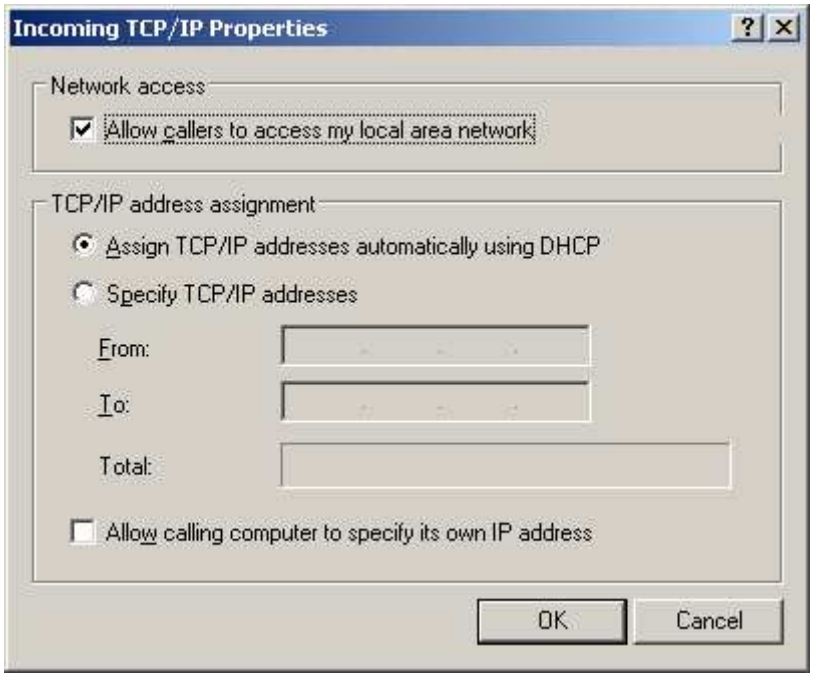
[8] Windows XP will include a more controllable firewall in later service packs, but for the present its basic firewall is not sufficient to prevent Trojan attacks and preventing server oriented application such as SQL Server exposing themselves to internet traffic.

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

next screen shows a list of the network protocols that will be allowed through the VPN – this deserves further explanation.

Since the purpose of this example is to internet users to log onto the LAN their traffic will be TCP/IP. However the wizard page is not showing how they will connect to the VPN server, but what kind of network protocol they will be using within the LAN. The VPN facility can be used to carry protocols other than TCP/IP between the workstation and the VPN server by wrappering them up within the TCP/IP protocol. The VPN server will un-wrapper the incoming TCP/IP packets and forward them onto the LAN as their original protocol. If you are using TCP/IP as your internal LAN protocol you should tick the TCP/IP option here. If you're using IPX/SPX or Netbios you can select these as well.

Highlight each of your selected protocols in turn and press the Properties button. The screen will look like this.



This is shown with the default options selected. The interesting area here is "TCP/IP address assignment". In order to reach the internet the workstation will already have had a TCP/IP address assigned by their Internet Service Provider. It is this IP Address which you have unblocked in your firewall. This screen does not refer to that IP Address however, it refers to the IP Address that will be assigned to the traffic from the workstation once it's forwarded to the LAN by the VPN server.

If you use DHCP to dynamically allocate IP Addresses within your LAN already you can leave the settings as default. If you assign IP Addresses manually you should check the "Allow calling computer to specify its own IP Address" which will then allow the workstation to use its nominated LAN IP Address (not the ISP assigned IP Address) within your LAN.

In most scenarios the workstation will either be a "stranger" (i.e. a teachers personal home machine) in which case it is unlikely to have anything other than an ISP IP Address because it doesn't normally connect to a LAN and you can safely either assign it a DHCP IP Address or specify a range to assign from. Otherwise the workstation will be a standard LAN laptop which is temporarily using the internet because the operator is away from the LAN, in which case it will already have been given a TCP/IP address by the LAN administrator and should be allowed to specify its own existing IP address by checking the last box.

Beware than many firewalls will by default refuse to allow routing by the VPN server and must be explicitly advised that routing the internet TCP/IP packets to the LAN and transforming the IP Address as it is forwarded is allowed.

Setting Up the XP VPN Workstation

Create a new network connection using Start … Settings … Network Connections … New Connection Wizard. Choose "Connect to a network at my workplace", the "Virtual Private Network Connection".

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

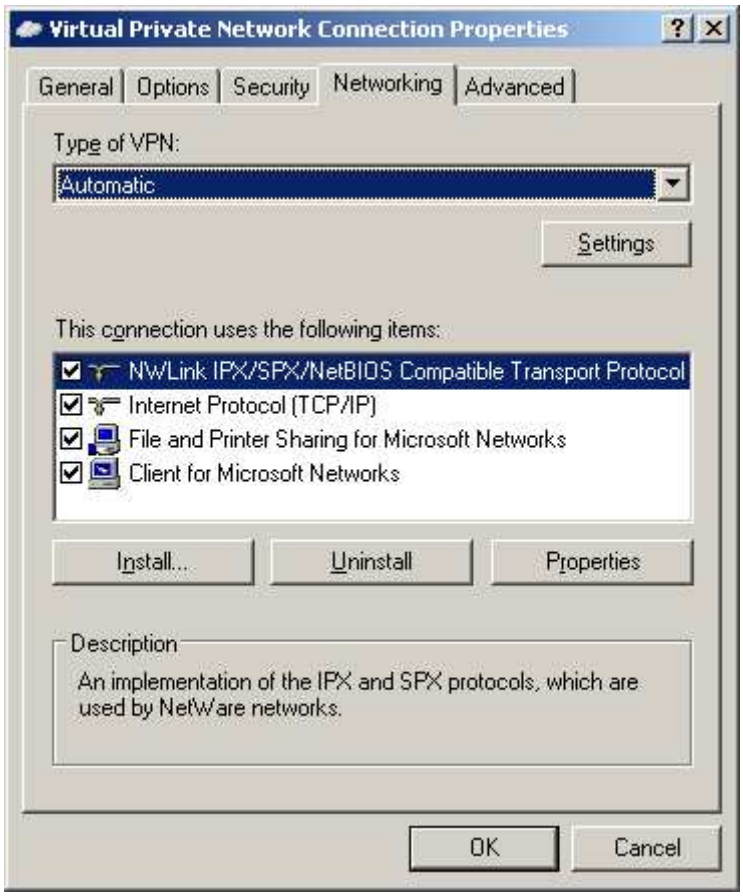
Enter a useful name for the connection such as "School VPN".

The next page asks which connection the VPN will be used over. Typically this will be your default dialup connection. Something to remember here that you can dial the internet separately to the VPN and use it to browse public web servers; however once you activate your VPN connection your internet connection on which it sits will no longer to able to "see" the internet because you will be operating within your LAN environment. Confusingly if you can browse the internet from within your LAN when physically connected to it then once you've connected via VPN this facility will be available to you.

The Wizard will then need to have the IP Address or DNS name of the VPN Server entered. Typically this will be "myschool.freeserve.co.uk" or "myschool.birminghamlea.net" or an IP address.

Continue to the end of the Wizard and then Finish. Unfortunately the Wizard doesn't give you the opportunity to set your detailed network settings so immediately go to Network Connections … and open the Properties tab of the newly created VPN connection.

The first three tabs (General, Options, Security) can be left as default but the Networking often needs some adjustment.

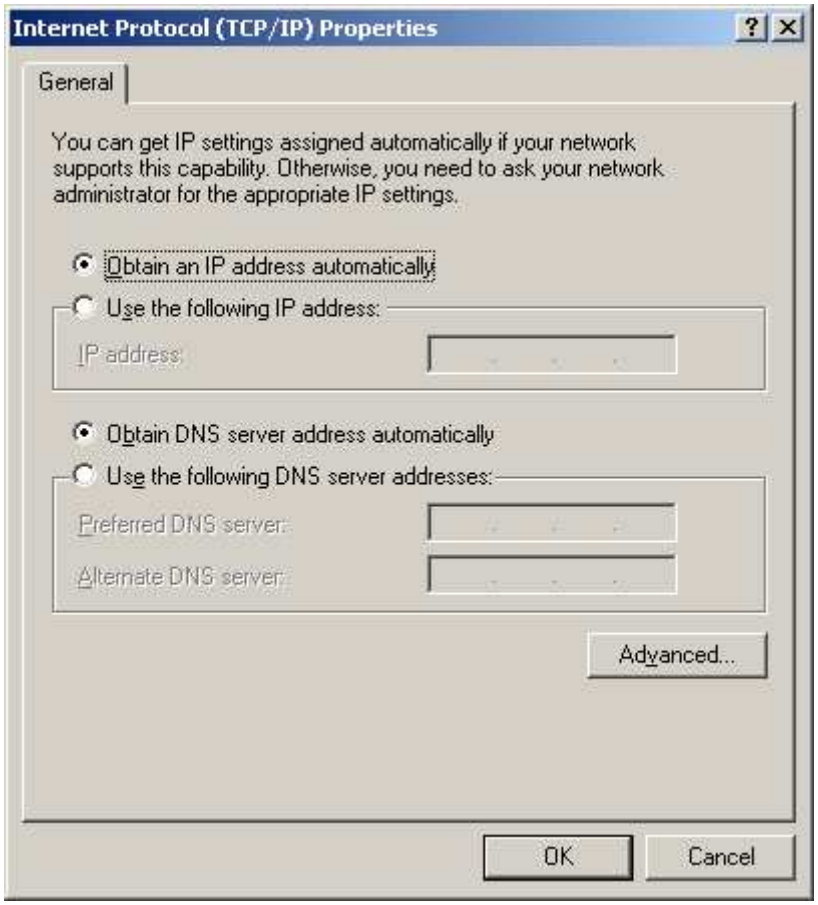


The list of protocols shown on this screen are those that will be wrappered up by the VPN service and forwarded for un-wrappering by the VPN server. We almost certainly want TCP/IP but the other protocols should match those chosen when setting up the VPN Server. If you select a protocol here which is no supported by the VPN Server you will be informed on connection of this and invited to take it off this list automatically.

If you only want to use SIMS.net over the VPN then you can de-select File and Print Sharing.

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

Select TCP/IP and then Properties.



This screen allows you to specify the IP Address that you will use within your LAN. It cannot be the same as the IP Address used to connect to the internet.

If you are normally assigned a dynamic IP Address, and this is what you specified on the VPN Server you can leave the defaults as shown. If you have a specific IP Address assigned by your network administrator and you've specified this on the VPN Server you should enter it here.

Press the Advanced button and enter the WINS tab. An important setting here is "Enable Netbios over TCP/IP" which allows compatibility with older versions of Windows. Generally speaking this setting should be set to "Enable" which it defaults to.

Using the XP VPN Workstation

Starting the VPN connection should either automatically dial your ISP or prompt you for the connection details (phone number, user name etc.). Once this is complete a second dialog box will appear prompting you for your LAN login credentials. The VPN Server will only accept those which are authorised to use the VPN connection – this may be a subset of all those authorised to use the LAN.

Once you've logged in the various facilities of the LAN are available for you to use including the SQL Server database. You can startup SIMS.net and use it as normal and the IP Address or machine name listed in Connect.INI will be resolved by the VPN Server and it will connect as normal.

If it's the first time you've used SIMS.net over the internet and you are using a dial-up account you should go into the User Options screen and check the box "I use a slow connection…" which will allow SIMS.net to screen out the download of student pictures and other high bandwidth information.

TECHNICAL GUIDE - SIMS.NET REMOTE WORKING

Troubleshooting a VPN Connection

The most common problems are firewall related. Most firewalls will default to the most restrictive policies available and a good start to troubleshooting is to momentarily disable the firewall whilst attempting to connect from the workstation – if it works then the problem is firewall related. If it doesn't its connection related.

Typical Firewall Problems

- Your firewall is not accepting the IP Address of the workstation either because it is dynamically assigned and outside the range that the firewall has been instructed to accept.
- Your firewall is not allowing routing of the VPN data from the VPN server to the LAN.

Typical VPN Problems

- You cannot "see" SQL Server although you can "see" shared resources such as drive shares. This is because SQL Server is listening for TCP/IP traffic but you've connected only with IPX/SPX, or vice versa.
- You have a dynamically assigned IP Address. SQL Server 2000 has a fault which prevents it from responding to dynamically assigned IP Addresses (Microsoft Knowledge Base article 306199) . You must install SQL Server 2000 SP2 to correct this.