the Internet

a solution to the wide area networking needs of business

Nick Hutton

WAN consultant

the Internet

a solution to the wide area networking needs of business

CONTENTS

APPENDIX

The background

Businesses have been exploiting wide area networks for a number of years as a means of information and resource sharing within their organisations.

In the meantime, Internet technology has been emerging as an enormously powerful medium for international business use. And security has also become a vastly more significant issue in the corporate arena.

Is the Internet now the logical way forward as a medium for the growing demands on wide area networking? Can it truly offer the advanced levels of security that any company needs in transmitting and receiving sensitive data to and from the farthest reaches of its operations?

This paper seeks the answers as we anticipate the needs of business and industry in the new millennium.

Executive summary

Wide area networks (WANs) have served business well. They have enabled commercial enterprises to share information and resources to a much greater extent and to rationalise overheads through centralisation of business support functions.

But there are inherent problems associated with their application. Today there are growing pressures on WANs, both because sheer volume of information has begun to overload systems, and because their vulnerability to hostile attack is now much greater.

So what does Internet-based technology offer in solving the growing problems of wide area networking – while capitalising on the existing investment in information and resource sharing?

COVERAGE

Coverage is the single biggest technical advantage Internet backbone has to offer the prospective customer of a global WAN. An Internet-based virtual private network (VPN) has the unrivalled size of the interconnected system. There is hardly an area of the globe that the Internet cannot reach.

This kind of access is very costly to provide in the private arena, since the company will be expected to install and support dial-up equipment and software. With an Internet VPN, providing this kind of access to third parties is simple and cost-effective.

SECURITY

A primary concern must be whether the public Internet can possibly be secure enough to carry company-sensitive information. The answer lies not in the network itself, but in the measures taken to secure information both at the boundaries of the organisation and in transit across the Internet.

There is a wide range of affordable security technologies which can protect the company's need for privacy and access control – while exploiting all the benefits of speed and global reach offered by the world-wide network. Encryption products ensure privacy; authentication devices and techniques can prove user identities; and there is a vast array of firewall products to give the customer detailed access control.

COST SAVINGS

An Internet VPN offers major cost savings over a dedicated private leased-line network, both through reduced – and still reducing – costs in Internet connection and in providing the facilities of global reach.

CONCLUSION

Clearly the future of WAN activity must take account of these exciting developments. As Internet technology emerges, so does the compelling case for Internet-based VPNs. And that is what this paper is all about.

Who is this paper for?

It will be of special interest to IT and telecommunications managers who are considering, or already operating, a wide area network (WAN). It is also for IT managers who are anxious that their networking strategy is in step with current and future trends in technology development.

Architects of management information systems (MIS) will find it helpful too, particularly those tasked with linking remote sites but who may not have considered a corporate WAN or a virtual private network (VPN) as a viable solution for their organisation.

IT professionals face many challenges, from those created by changing company structure and a more demanding workforce to the needs of finance directors who have an ever-keener eye on cost control. This paper explores some of the opportunities for meeting the needs of IT users across the enterprise. It also examines how Internet-based VPN technology can be implemented as a replacement for the conventional corporate WAN.

The business case for the corporate WAN

Corporate WANs have proliferated across Europe over the past five years. The attraction is that a wide area network can enhance business processes by allowing remote offices to share corporate information and resources. They have also been shown to lower the cost of doing business, thereby enhancing competitive edge in delivering higher-quality services to the customer.

EMPOWERMENT

Making data and decision-making expertise available enterprise-wide enables companies to provide customers with more effective information faster than ever before. Employees are empowered by a greater ability to fulfil obligations to internal departments and external customers.

A good example is the automotive industry, which has long understood the value of collaborative groupware tools in the product development process. WAN technology has enabled manufacturers to marshal design, engineering, marketing and financial capabilities on a national and international basis.

DIRECT COST SAVINGS

Ironically, WANs have been both a facilitator and a product of corporate downsizing. Slower growth, greater competition and a need to cut overheads has created the need to share information more rapidly and effectively.

WANs also offer economies of scale. It is no longer critical to have all business support functions under one roof. A central purchasing or legal department can service many different sites, eliminating much duplication of work.

For example, a manufacturing firm can order efficiently on a just-in-time basis, because its ordering department’s information systems can gather information and product schedules across geographic boundaries. Indeed, JIT philosophy itself is fostering a growing demand for rapid, accurate communications across the organisation.

The changing face of WANs

Originally WANs were application-specific, often built as transactional networks for financial systems or as store-and-forward relay networks used for sending updated database records to branch offices overnight.

But the potential for driving other information through the WAN was quickly recognised. Other newer applications were retro-fitted to WANs. Though their arrival didn't always sit comfortably with the design goals of the transactional network, performance was usually good enough – especially given the low cost of piggybacking data on the existing network compared with building a second application-specific network.

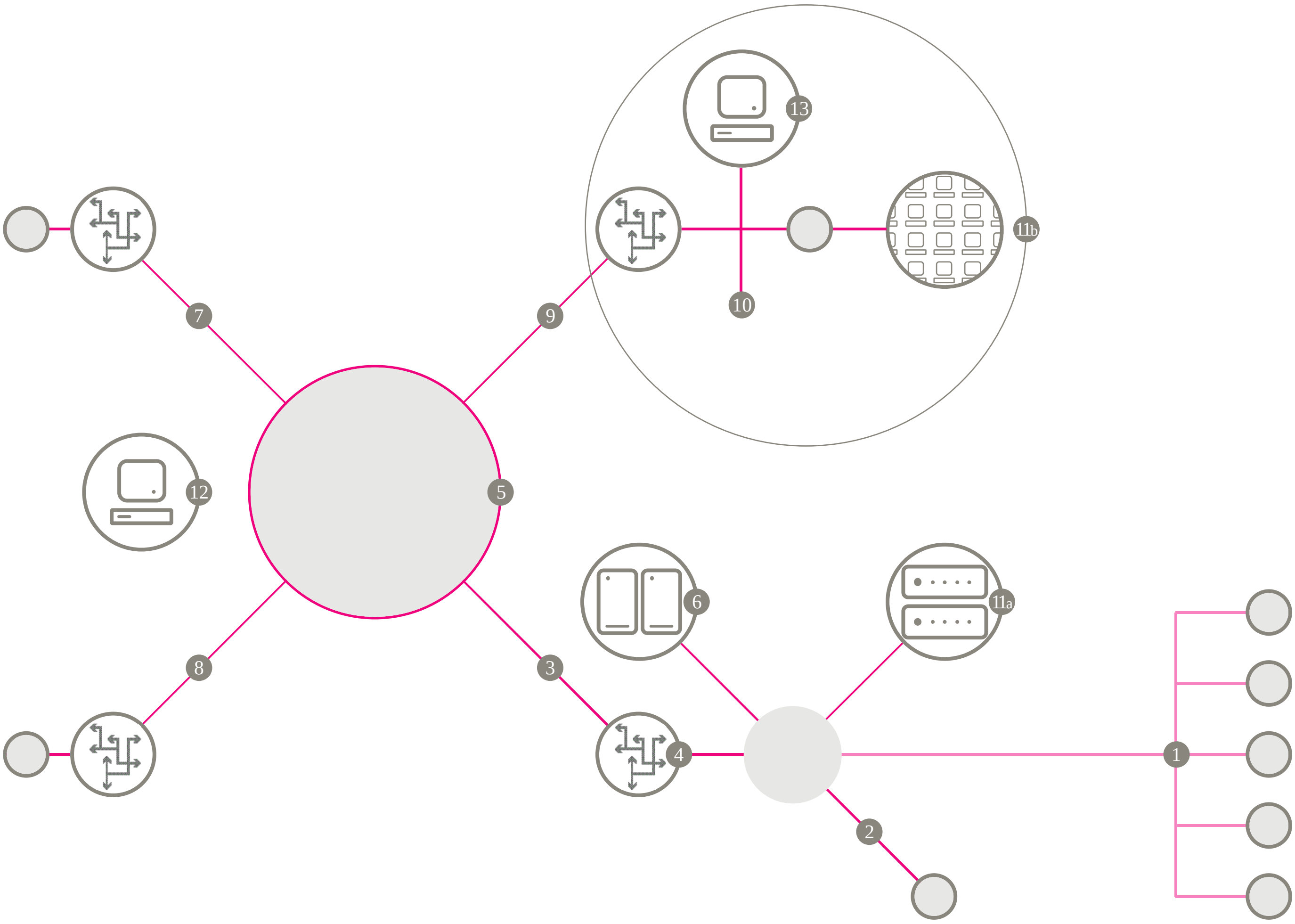
Of course the existing WAN wasn't always able to satisfy demands made by additional applications. Many organisations now have several dedicated WANs linked to specific application software – one for stock file distribution, another for transactions, others for interactive sessions, private email and so on. Many of these companies are now connected to the Internet too.

And here's a key consideration. Failure to predict future use could easily result in a number of discrete legacy networks – which could have been unified with more thought during the planning phase. Many an MIS department is now faced with consolidating legacy networks into a single more manageable corporate WAN. Not an easy job, considering that many of these networks are mission-critical and downtime is not an option.

Today the corporate WAN has adapted to become a more generic communication tool. Application-specific WANs are seldom built these days unless there are exceptional circumstances. Open standards and off-the-shelf devices have replaced the dedicated, proprietary hardware and software which held together older corporate WANs.

A model of the conventional WAN

The author has worked as a security consultant on many corporate networks and the example illustrated here is typical in his experience. Though by no means a worst-case scenario, there are several security problems with this WAN, and much could be done to improve matters. Most of these problems will have grown out of the unplanned-for nature of changing WAN use.



1. Midnight lines – the store-and-forward network used for transferring inventory data – are held open almost continually. This network pushes out directives to the branch offices using a midnight line system of regular modems. Initially this network was only live for short periods, late at night, when end-of-day batch queues were uploaded. However, since terminal access was piggybacked on the network, to support demand for real-time database queries, the lines are now live for much of the day.

   The network has minimal security. Anyone who can find the phone numbers (using a war-dialler) is able to log in. The modems are of the early programmable type and can be reconfigured online easily by an unauthorised user. He can then connect to the DP centre PAD and move freely inside the DP centre LAN.

2. The data centre link to the finance/billing operation is via an X25 CUG connection. This link enables the billing application running on the mainframe to call the finance office from a PAD prompt, automatically log in and begin transferring the day's records to process.

   Traffic is not encrypted and passwords used to initiate the log-in are sent as clear-text. Once an unauthorised user has access to the X25 PAD at the DP centre he can capture the password information, plus any transactional records he is interested in. The PAD can also support debugging on its LAN interface, allowing the unauthorised user to observe general LAN traffic on the local segment, filtering it for passwords.

3. The data centre link to a shared FR/SMDS cloud. The private frame relay link into the cloud permits some other sites to access the DP centre. Since this connection is solely for private company use, it is given little security protection.

   Although the provider of the FR offers an Internet PVC as an additional service, the DP centre has not taken up the option – even though any misconfiguration of the FR switch could allow PVC leakage of Internet traffic on to the private network. Furthermore, if an Internet PVC was added in the future, additional equipment and software would be required to ensure privacy for critical private traffic.

4. Data centre router controlling inbound access to the LAN.

5. Single provider frame relay or SMDS network.

6. The mainframe, which runs mission-critical applications, is secured using sophisticated RACF software designed to allow tight control of what data individual users are allowed to access. But the operating system and its major applications have no protection from external network-bound attacks.

7. This is the call centre link to the FR/SMDS cloud. The support analysts need this access to diagnose faults with branch office links and to carry out general IT support for the wider organisation.

   An Internet-access PVC has been enabled for call centre servers to allow direct access to the support services of the company's IT suppliers. Patches can be fetched and applied within hours. However, since the site doesn't advertise any services, or even receive email, they have employed only basic router filtering methods at their border with the FR WAN.

   Unfortunately the local IT supervisor is unaware of the fact that allowing the fetching of files from Internet servers leaves the site open to types of attack that even a properly configured router is unable to guard against.

8. Stateside data centre link to FR/SMDS cloud; Internet PVC also enabled.

9. The UK head office link to the FR/SMDS cloud is chiefly for management reporting from the DP centre and for communication with the stateside operation.

   The marketing department has approval for a pilot WWW site, hosted on an otherwise empty segment off the network's central switching hub. Traffic from the Internet PVC is only switched to the WWW server segment, since general desktop Internet access is not permitted.

   However traffic to and from the WWW server and the desktop LAN flows freely, to enable employees to surf the server and use web publishing tools to build and maintain the site. If the experimental WWW server were to be compromised, an attacker could easily jump back through the switched hub into the desktop LAN.

10. Intelligent switching hub used to partition WWW server and LAN.

11a &
11b The modems used for remote access by IT staff and board members. Dial-up access to the DP centre is required for the on-call operators, so simple terminal access to the servers is possible from the dial-up PAD. Once again, security could be improved. The telephone numbers are never changed. More worryingly, head office has a similar arrangement to give senior managers dial-up access to their desktop email.

   That connection exposes the vulnerable LAN servers which use featherweight security and generally have no restrictions on the scope of drive shares. The DP centre doesn't have similar LAN systems; the site is stocked with dedicated legacy servers and fixed terminals.

12. The mobile workforce is unable to connect to the supporting IT structure. There is no provision for remote or mobile users. They either have no connectivity at all, or are left to manage with desktop modems in an uncontrolled manner.

13. The public-facing WWW server, accessed through the Internet PVC.

So why is an Internet-based VPN a viable solution?

The key question for an IT or telecoms manager considering the options for implementing a WAN will be: can VPN technology offer more than a conventional WAN?

Here we answer that question from a variety of angles.

COVERAGE

An Internet VPN offers at least equal national coverage as a private WAN. But an Internet solution offers the advantage of truly global coverage.

Firstly, the Internet is a network of networks where, through peering agreements, any ISP is able to route traffic to any other provider. It is achieved through selective peering between major providers, rather than full meshing. On the other hand, this kind of inter-provider exchange is unheard of outside the Internet world. Even providers of metropolitan connectivity refuse to exchange private traffic with one another. And the public X400 system allows only email to be exchanged.

Secondly, the Internet industry has recently seen a wave of mergers and acquisitions. This has given some service providers the ability to offer global coverage within the borders of their own backbone network. It is this change in the marketplace, and the consolidation among tier-one providers, that is enhancing the network coverage available.

Coverage is still (and will always be) the single biggest technical advantage Internet backbone has to offer the prospective customer of a global WAN.

COST AND RESILIENCE

An Internet VPN offers major cost savings over a dedicated private leased-line network. Typically, leased-line customers pay for their connection based on a fixed fee for connectivity plus a per-mile distance based charge for the circuit. As distances become substantial the cost of leased lines increases significantly. This is accentuated if a meshed or triangulated topology is needed for resilience.

Meanwhile, Internet access is based on customers using a shared backbone network. Typically customers pay a fixed cost for their connection to the nearest ISP PoP (point of presence) plus an additional charge according to bandwidth requirements.

The fact that the Internet is a single global network means market forces and competition drives down the cost of access further. That leaves prospective customers the freedom to strike either individual deals with local access providers, or single global deals with tier-one players.

The ISP business is now so competitive that it is moving towards commodity pricing for connections. Because the Internet is based on open standards and open protocols, different vendors compete against each other to lower connectivity prices.

EMPOWERMENT

The use of standard utilities and protocols makes it easier to train new workers in network application use, since many qualified individuals will have already worked with standards-based technologies when using or managing such a network. The universal use of SNMP is a case in point.

Some support functions can also be offloaded with an Internet VPN. A huge audience of technologists on the network news system are able to help you solve problems and share experiences – and cut the cost of problem resolution for your systems. This wealth of experience helps IT managers avoid making costly mistakes. Direct access to the support machinery and technical libraries of every IT OEM is also available at no charge.

All this means that, on a daily basis, time-to-fix for in-house MIS help desks can be lowered substantially.

FLEXIBILITY

An Internet VPN offers greater variety of access methods than traditional private WANs. This enables customers to take advantage of local variations in the cost of different access methods, dial-up, ISDN, leased lines with a variety of billing schemes and speeds. Also, an Internet VPN offers greater flexibility to those responsible for implementing the roll-out of software across the enterprise.

The Internet has been shaped by incremental change and consensus, not by the private agenda of any one government, corporation or individual. It can deliver async terminal access, file transfer, store-and-forward, streaming audio/video and, most recently, multicast services. And it penetrates virtually every sector of life all over the world. .

Even systems which don’t conform directly with Internet standards are able to take advantage of the network through protocol tunnelling and application proxying.

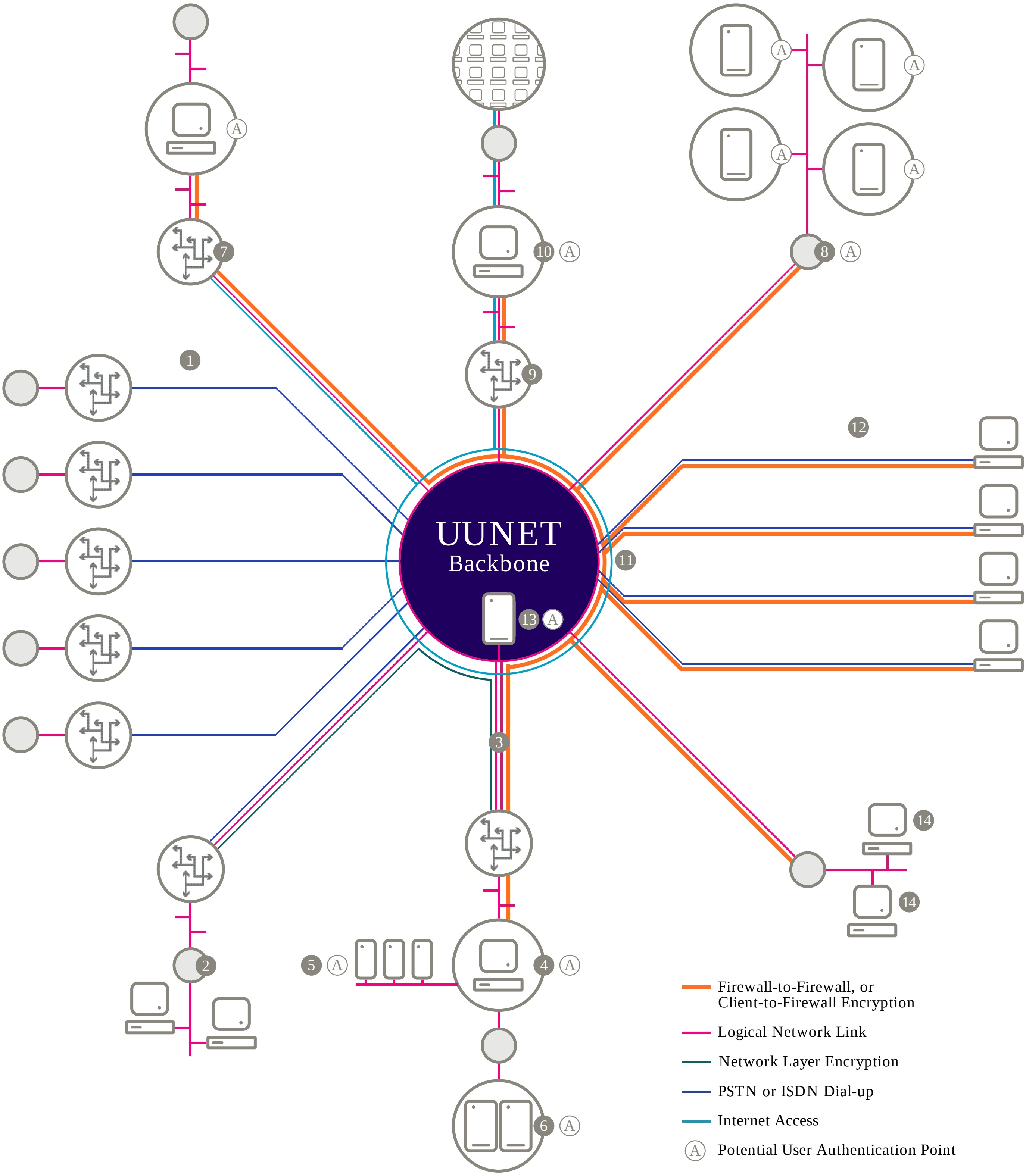
MANAGEMENT

A standards-based network allows easier outsourcing of network management. ISPs and outsourcing houses can leverage their own centralised expert workforce to gain economies of scale in managing other networks.

An Internet-based outsourcing service allows for easy substitution of vendors in a competitive situation and savings can be passed on to the customer. Outsourcing can range from the provision of email relays and host name services to full capacity planning, monitoring and administration of servers. Pioneers are now even formulating Internet-based outsourced disaster recovery services.

UUNET implementation of an Internet VPN

Here is a sample network topology showing a viable alternative to the typical private WAN we looked at earlier. There are several points of interest on the diagram and we shall visit and elaborate on each of them.



1. The 64Kb ISDN links from branch offices to the Internet use routers offer dial-on-demand and access control. Since the branch offices don't need access to the Internet, in general these routers are set up to offer CUG-like functionality.

   Access control lists offer simple traffic filtering. Further security can be gained by activating network-level encryption between the branch office routers and (say) the data centre router. This would be sensible if commercially-sensitive information were being transmitted. The only access permitted is for the specific task of stock data exchange with the data centre.

   The dial-up link itself is secured using PAP/CHAP authentication, preventing unauthorised users from dialling up and compromising security. If the links were very heavily used, or if the access pattern changed from intermittent file transfers, then ISDN access could be switched to a variably-billed leased-line service where sites pay for access on a per-megabyte basis, rather than via online call minutes.

   An ongoing cost analysis is possible and the changeover can be made without downtime. These routers are leased, and management of them is undertaken by the chosen ISP.

2. The 256kb/sec leased-line connection links the finance operation to the corporate Internet VPN.

   Since the only access required is back into the data centre systems, general Internet access is restricted as in (1). However, this site's use pattern dictates that a higher amount of bandwidth is sometimes needed than for the branch offices. As a result, a variably-billed tariff is suggested for the line. During the day there is only a trickle of data, but during the end-of-day batch period after midnight there is a burst of data.

   This data is business-critical and delay is not acceptable. For these reasons an ISDN backup service is also deployed. Although offering less bandwidth than the leased line, there is sufficient capacity to cope with any temporary outage in the leased-line service.

   Network-level encryption can be enabled on the managed router, or if the billing systems are on modern platforms, encryption and authentication can be integrated with their operating systems.

3. The 4Mb link from the data centre to the Internet VPN is configured using dual redundant 2Mb lines. Since the link is in use continually at high capacity, a fixed tariff has been selected. Payment levels are the same regardless of service use.

4. The firewall protecting the data processing centre can be configured to block inbound access from the wider Internet. It may selectively allow access to the DP systems for parts of the corporate's external sites. It can act as an encryption tunnel end-point for client systems with appropriate software, and it can challenge both automated processes and real users for authentication using fixed passwords, one-time passwords or digital certificates.

   Generally the inbound access to the DP systems will be very limited; however, the firewall also controls access to the mission-supporting servers (5) which are accessed from a wide range of computers around the corporate VPN.

5. This network segment serves the web server, email gateway and major supporting infrastructure for the company intranet. It is centrally located near the administrator's base at the DP centre, protected from unauthorised access by the firewall and the border router at the DP site. All access to these servers is logged. If the company wishes to audit its own users tightly, it can challenge them for authentication before letting them into the systems.

6. The legacy mainframe system is protected from outside access by the firewall system, leaving its security administrators to concentrate on managing internal use of its inbuilt accounting and auditing functions.

7. The 512Kb leased-line link from the call centre is accessed via a firewall, ensuring that engineers remain protected while they access valuable Internet resources. This set-up enables engineers to download patches from vendors and push them securely out to remote corporate sites.

8. The 45Mb leased-line link to the UUNET-US data centre is very heavily used by customers accessing the public face of the company. Flexible pricing options allow the US parent company to provide a high-capacity service at an acceptable cost. The US parent is currently considering offsite backups over this connection as a cost-saving measure. Meanwhile, offsite backups are currently shipped by courier to a secure warehouse facility.

9. The 256Kb leased-line link to the UK headquarters provides access to the private corporate VPN and the wider Internet. Because not all users require Internet services for their job, the firewall system enforces user-level restrictions on surfing. Since the company also has strict policies on pornography and other areas of computer misuse, detailed logs are kept of users and the sites they have visited.

10. The firewall system segregates and selectively encrypts traffic from the head office LAN. This offers real security in isolating private traffic from the public Internet data using proven encryption technology.

11. The UUNET global dial-up network allows authorised users worldwide to connect securely to their private company resources.

12. Remote worker using the UUNET dial-up network are issued with a list of international access numbers for UUNET PoPs. Using these they are able to establish a reliable connection to the information they need. The chosen ISP provides access to huge modem pools and handles all the management of the dial-up infrastructure.

13. Rather than house the public corporate WWW server within the data centre, the company has decided to co-locate it at its ISP's premises. The benefits of this include reduced cost of management, increased bandwidth for less expenditure and a faster, cleaner upgrade path as traffic levels increase.

14. Outsourced web design bureau. The ISP network is connected to the global Internet via a number of peering points. This high-performance, resilient network gives the customer high levels of service availability and access to the most ubiquitous data communication medium in the world.

Does the proposed solution fit the business requirement any better than a private WAN?

Every customer's requirement is different. There is no single solution to replace all existing WANs. However a summary of all the detail covered reveals a number of trends in the characteristics of an Internet-based VPN when compared to the traditional methods of building WAN infrastructure.

USER MOBILITY

Since ISP networks are designed to be resold to thousands of companies (often worldwide) they can offer uniform connectivity to nomadic users straight out of the box. One single network sign-on connects them to their ISP's backbone in any country.

VARIETY OF ACCESS METHODS

Unless an ISP has targeted a specific niche market for its services, it is likely that a wide variety of connectivity options will be provided. Since ISPs start with single-user dial-up products and progress to high-capacity leased lines with a variety of billing options, there is usually something in the portfolio for every need.

COVERAGE

Linked to user mobility, an important feature of an Internet-based VPN is the unrivalled size of the interconnected system. There is hardly an area of the globe that the Internet cannot reach. There is currently a move in both service and manufacturing industries to get closer to the customer, allowing them more direct access to stock tracking systems, help desk and order-entry mechanisms.

This kind of access is very costly to provide in the private arena, since the company will be expected to install and support dial-up equipment and software. With an Internet VPN, providing this kind of access to third parties is simple and cost-effective.

The UPS OnLine Tracking software offers you a full range of tracking options-right from your desktop" – http://www.ups.com/europe/cgi-bin/uolt.cgi?eu!eng!eng!olindex

STANDARDS

Without standards the Internet simply wouldn't work. They enable vendors to compete on a level playing field, eliminate customer lock-in and reduce day-to-day interoperability headaches.

COMPETITION

The Internet continues to show phenomenal growth. Whenever there is such competition in the IT industry, vendors try to fragment the market along lines of functionality. Generalised Internet access is split into personal use and business use, while security can be split into access control (firewalls), authentication technology and intrusion detection.

With standards in place, the customer is free to pick the best-fit solution. Analysts predict eventual widespread consolidation – we are already seeing the start of this with activity from major industry players. Over-capitalised start-ups and smaller operators without a niche are predicted a finite life expectancy. Through competition list prices are driven down, and through consolidation providers' costs fall as economies of scale rise.

However, seasoned professionals will know that it can't be all good news. Two burning questions have not yet been answered:

- How can a system using the public network possibly be made secure?

- How can the Internet be relied upon for an enterprise-critical WAN?

So let's now answer those burning questions.

Security: conventional WAN vs Internet VPN

If a shared public network is used for confidential data, security will certainly be of paramount importance. Defining and measuring security is a complex task, but it is possible to check a given solution against several basic criteria to ensure that key security targets are met:

PRIVACY

Customers sharing the same network infrastructure should not be able to read private data sent from one site to another, even if they are somehow able to intercept it.

The conventional WAN addresses security through true dedicated point-to-point leased lines (expensive), or frame relay/SMDS PVCs. Customers are often unaware that, in an FR/SMDS scenario, the only thing isolating their private network links from other customers and Internet feeds is the configuration of an FR switch. If the switch were compromised, or poorly configured, traffic could leak from one set of PVCs to another.

In either case encryption devices would offer true privacy, but are seldom deployed. One of the benefits touted for 'private' shared networks is that there is no need for encryption devices and enhanced security. However customers are increasingly hostile to the 'trust us' model of privacy as they become more IT literate and the value of data to their organisation increases.

Customers now have a better understanding of how a provider's network offers connectivity to its customers. This leads them to believe that without dedicated encryption technology there is no such thing as a private network.

Encryption of data passing between systems on the WAN only protects information being transmitted; it does nothing to secure the operating systems and application generating the traffic. The ability to scramble confidential information in transit is of no consequence if an attacker can easily gain access to the end systems and monitor the data before it is sent. For this reason it is vital that privacy and access-control are used in tandem.

The Internet VPN achieves security through either application-level encryption on client systems or, more commonly, through network layer encrypting gateways or routers.

Customers using the Internet as a VPN medium have always been aware that the trust-us model of privacy promoted by some ISPs is inadequate where company-confidential data is involved. Privacy/encryption technology has migrated from bespoke software/hardware black boxes to mainstream firewalls and is now implemented in some router products.

Typically firewalls can be deployed at network perimeters and client software is used for mobile workers or small sites. Strong, proven encryption is available using algorithms such as DES, IDEA and Blowfish.

AUTHENTICATION

Access to any resource on the network should be granted, subject to authentication, to either the individual user or individual device. The method of authentication chosen for any given resource must not be easily forged. For instance, simple IP addresses cannot be used; they are too easily spoofed.

The conventional WAN tackles authentication generally through simple network address validation or lightweight LAN authentication/directory services. The trust model for a PC LAN has always been quite open. Server systems trust each other to share resources, either using no specific authentication at all, network address validation or simple fixed passwords.

It is unusual for a user to be quizzed further after the LAN server has enough information to offer him the correct drive shares and printer access. This kind of lightweight identification of users and systems does not sit comfortably with the risks of opening your discrete LANs to unchallenged access from any employee. These implementations also ignore any of the risks associated with the use of a shared FR/SMDS-type network, such as PVC leakage and MITM or replay attacks on fixed repeatable passwords.

The Internet VPN. It has always been accepted wisdom that, when enabling inbound connections from the Internet to your LAN, you should authenticate connections rigorously. Since the authentication challenge may also be issued across network boundaries to a user on the other side of the world, a great deal of thought has gone into guarding against MITM and replay attacks.

The ‘trust no-one’ model of security is well established and has stimulated such technologies as one-time passwords and digital certificates. Simple network address validation was disregarded as a suitable method of authentication some years ago, so additional packet authentication headers may be added to traffic as the IPSec standard defines.

INTEGRITY

Proof is needed that authenticated data sent over a private channel has not been tampered with. Integrity is key for mission-critical applications such as billing systems and electronic commerce.

The conventional WAN's data integrity has traditionally been a function of whatever application software is using the network. Examples such as checksummed EDI documents passed from server to server are common. This works well in closed communities, where there is control over all components exchanging data, but is not a workable solution when wider communication is a requirement.

Without open generic standards for integrity-checking, any solution is either going to be limited to a single application, such as EDI document exchange, or limited to a single community such as a particular industry.

The Internet VPN. It has taken some time for standard integrity mechanisms to emerge on the Internet. Stronger network level checksums are implementable via the IPSec additions to TCP/IP, but higher level standards tend to be application-specific, though certainly not limited to a particular community. Truly generic fingerprinting and certification of data will draw closer as certification authorities, public key hierarchies and directory services become more widely used.

ACCESS CONTROL

The technologies used to build an Internet VPN should offer a 'granular' level of access control to administrators. This ensures that access is only granted to those sanctioned by managers responsible for operating the company servers and LANs. Access control should also be subject to transaction tracking and audit trails.

The conventional WAN. Access control in private WANs is often a low priority where 'getting things working quickly' takes precedence over 'getting things working securely'.

Once again this is reinforced by the 'trust us' supplier model of WAN security and the open nature of information sharing within most LANs. If any kind of access control is implemented, it tends to take one of two forms: either network-level router filters providing limited granularity of control; or simple file/drive share permissions whose underlying method of authentication is by easily-forged network address. In either case there is rarely a comprehensive audit trail kept.

The Internet VPN uses a combination of routers and firewalls for access control. In conjunction with the enhanced authentication already explained, it is possible to maintain a satisfactory security policy with detailed auditing of access. Importantly, these technologies don't require extensive changes to existing LAN systems.

Of course there is a cost associated with access control, but the benefits are considerable – and not just from a security aspect. Many companies implement firewall technology to allow management of their users' Internet access, and to provide more intricate management of network use.

But how can you rely on an Internet-based network?

Since no single ISP owns the Internet, providers cannot normally commit to service-level agreements for connectivity which is only partly under their management.

This presents the customer with a problem when the Internet connection is not performing as it should. The onus is on the customer to prove who owns the fault and who is failing to match up to their SLA. Blame loops can occur where one provider insists that a loss in performance is down to some other part of the connectivity outside their network, such as name-server problems, upstream routing congestion or overloaded web-server hardware.

In assessing whether such a network is really a suitable foundation for corporate communications, it is vital to recognise that an ISP's own backbone is not the Internet.

The global Internet comprises two building blocks: the network backbones of many ISPs; and the neutrally-owned peering points through which different ISPs exchange traffic. Peering points are spread all over the globe. If an ISP wants to talk to the rest of the world outside its own network, then at some stage the traffic must cross one of these peering points, or NAPs.

Importantly, it is possible for an ISP to have an excellent performance and reliability record within its own network, whilst suffering latency and data loss due to a poor peering strategy with the rest of the world. This occurs quite frequently with smaller ISPs going for niche markets, due to their inability to operate internationally and co-ordinate network management on a 24–7 basis.

Typically it is also much easier for an ISP to attach a particular service-level agreement to connectivity within its own network. Once traffic crosses a NAP its delivery is out of their hands. Pragmatists will point out that most congestion and packet loss tends to occur at these busy Internet 'roundabouts', and not within a particular ISP backbone.

The practical solution to this lack of SLA ownership is to use a single ISP for your whole Internet VPN. This greatly simplifies contracting and implementation but raises the bar for smaller ISPs who do not have global connectivity.

In either case the single ISP or group of suppliers should provide relevant SLAs and be able to offer statistics, reporting and service management to qualify any such claim. It should not be left to customers to carry out their own service monitoring and performance testing.

Conclusions

SECURITY

With a wide range of affordable security technologies on the market, an Internet VPN is certainly an attainable goal. Encryption products ensure privacy; authentication devices and techniques can prove user identities; and there is a vast array of firewall products to give the customer detailed access control.

Suppliers know that, to get the business community on to the Internet, security is an absolute priority. Conventional private WANs have attracted much less scrutiny than Internet-based solutions – and still tend to use insecure address-based authentication and access control for restricting user activity. With carefully designed architecture, Internet VPNs can be made as secure as traditional WAN implementations. And one mustn't forget that the most security breaches come from inside an organisation's own perimeters.

RELIABILITY AND PERFORMANCE

Explosive growth in the number of companies connecting to the Internet is driving a continuing cycle of infrastructure upgrades. This, coupled with consolidation in the ISP market and partnerships with telecoms providers, prevents some ISPs from being swamped by demand for bandwidth.

Performance bottlenecks at NAPs continue to pose a problem for ISPs without global networks. But when considering an Internet VPN running on a single ISP's network, the picture is more favourable.

It should be possible for any ISP to provide evidence of network performance, and to back this up with a suitable SLA. With a properly-funded network from an established ISP, performance monitoring and capacity planning will have been in place for some time. The customer can expect suitable service levels when compared to those of a traditional WAN.

However, ISPs still have ground to make up over private network providers in respect of the reporting aspect of QOS/SLAs. Even if excellent performance is offered along with stable, resilient connectivity the customer requires something more tangible than a single Network Status = GREEN web page.

> *"UUNET was selected on the basis of a blue chip supplier that could provide Abbey National with the service and support required, 24 hours a day, seven days a week. Abbey National must trust its supplier to maintain the quality of service it promises to its customers. UUNET has the expertise and experience that makes Abbey National confident in its choice of supplier."*
>
> Abbey National
> http://www.abbeynational.co.uk/chile.cgi?id=new&hr=index.hot

Questions to ask your ISP about Internet VPNs

- Do you have a full network map available to customers?
- What is your backbone upgrade strategy
- How do you manage performance?
- Do you have extensive, global peering agreements?
- Do you have an SLA, is it adequate for your needs?
- Can you provide 24–7 cover?
- Do you provide reporting on performance and service utilisation?
- Are you experienced in network security?

Glossary

FR
(frame relay)

A wide-band packet-based data interface standard that transmits bursts of data over WANs. Frame relay packets vary in length from 7 to 1024 bytes. Data oriented, frame relay is not usually used for voice or video.

SMDS
(switched multi-megabit data services)

SMDS is a public high-performance, packet-switched connectionless service. Offered internationally, it is based on specifications issued by Bellcore for the USA and by the European SMDS Interest Group (ESIG)

Tier-one provider

An internet service provider with numerous points of direct access to the worldwide network of Neutral Exchange Points. A provider owning and operating its own network and reselling bandwidth to smaller ISPs or to customers direct.

ISP
(internet service provider)

A company providing connectivity to the Internet, usually through a variety of access methods to a shared network backbone over which the IP protocol operates.

WAN
(wide area network)

A network with nodes separated by relatively large distances. WANs can service national or international user communities.

LAN
(local area network)

A network normally spread over a single building or campus.

MAN
(metropolitan area network)

A network which may extend across a single city.

VPN
(virtual private network)

An Internet VPN is a specific type of VPN that delivers a private IP service over a public infrastructure. Note that the key element is delivery of IP services to the end users.

Midnight line

A phone line lease scheme allowing the customer to use the line for a prolonged time-slot in the small hours of the morning for a fixed fee. Such connections were often used to update central data processing sites from outlying branch offices in a cost-effective manner.

SNMP
(Simple Network Management Protocol)

A communications protocol used in the monitoring and management of communications devices and services. SNMP utilises three basic request primitives: Set, Get, and Get-Next for configuration and performance information; and one asynchronous notification: Trap for alarm and status information. Originally designed for TCP/IP. Most popular SNMP software: SunNet Manager, HP OpenView and IBM NetView/6000.

PoP
(point of presence)

A location at which the data circuit from a customer is connected to the ISP’s backbone network.

MITM
(man-in-the-middle) attack

A form of attack through which the hacker is able to gain some advantage by observing and perhaps altering the stream of data passing between the user and the end system to which he is connected.

War-dialler attack

A hacker uses a computer and modem to dial all of the phone numbers for a company, whilst recording which numbers have other computer modems attached to them. These systems are then attacked in order to gain entry to the corporation’s LAN. Such attacks can be quite sophisticated and employ random dialling patterns to evade triggering suspicion.

Replay attack

A replay attack is a form of attack where the hacker observes a legitimate user carrying out some regular function (such as logging in) and then uses the transcribed information or captured session to recreate the action himself. Fixed username/passwords are often the information such an attack will compromise.

PVC
(permanent virtual circuit)

A circuit that is defined in a static manner with static parameters but which is not tied to a given physical path through the network.

DES
(Data Encryption Standard)

DES is a symmetric cryptosystem. When used for communication, both sender and receiver must know the same secret key, which is used both to encrypt and decrypt the message. DES can also be used for a single-user encryption, such as to store files on a hard disk in encrypted form.

IDEA

(International Data Encryption Algorithm)

IDEA is a strong cryptosystem using a 128-bit key, found to be highly resistant to linear cryptanalytic attacks and immune from differential cryptanalysis. IDEA is generally considered secure and both the cipher development and its theoretical basis have been openly and widely discussed. The cipher structure was designed to be easily implemented in both software and hardware.

Blowfish

Blowfish is a symmetric block cipher that can be used as a drop-in replacement for DES or IDEA. It takes a variable-length key, from 32 bits to 448 bits, making it ideal for both domestic and exportable use. Blowfish was designed in 1993 by Bruce Schneier as a fast, free alternative to existing encryption algorithms. Since then it has been analysed considerably, and it is gaining acceptance as a strong encryption algorithm.

IPSec

(Internet Protocol Security)

A developing standard for security at the network or packet-processing layer of network communication. Earlier security approaches have inserted security at the application layer of the communications model. IPSec will be especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPSec is that security arrangements can be handled without requiring changes to individual user computers.

OTP

(one-time password)

Reusable passwords are vulnerable to many attacks, including keystroke monitoring, social engineering, brute force attacks and network monitoring. OTPs are always changing; even if an attacker does record a user’s password, it is of no use.

CUG

(closed user group)

The ability of a shared network to allow a subset of connecting customers to exchange with one-another, while remaining isolated from the wider network population.

SLA

(service level agreement)

The stated level of service the customer can expect of the connectivity being purchased from the ISP. This information may detail technical information such as latency, bandwidth and downtime levels.

QOS
(quality of service)

Linked to the SLA, QOS is an umbrella term used to label the specific performance attributes of a customer’s network connectivity.

NAP
(neutral access point)

A shared network hub where ISPs may exchange traffic with each other subject to their peering policies. There are many such peering points distributed over the globe.

PAD
(Packet Assemmbler/ Disassembler)

A hardware device which generally permits character based asynchronous terminals to access systems on a shared office network.

PAP/CHAP

A software based token authentication technology, often used by dial-up routers to prove their identity to the call-answering hardware at the remote site. The use of such a system reduces the risk of unauthorised systems connecting successfully with your dial-up equipment.

For more information…

- about outsourcing employees' dial-up access, while retaining a central control mechanism, see the UUNET MultiDial site: http://www.uk.uu.net/products/multi-dial/
- about locating Internet servers on UUNET's backbone, see the UUNET Co-Locate site: http://www.uk.uu.net/products/co-locate/
- about encryption and access control solutions, see the UUNET Firewall site: http://www.uk.uu.net/products/firewalls/

Suggested further reading

- Informed reporting on communications technology worldwide
  http://www.telecoms-mag.com
- Leading analysts' commentary on telecommunications strategy
  http://www.infonetics.com/
- Search for articles on Internet VPNs
  http://www.techweb.com/search/search.html
- Firewall-l VPN information centre
  http://www.checkpoint.com/vpn/index.html
- Cisco Systems VPN information centre
  http://www.cisco.com/warp/public/779/servpro/solutions/vpn/index.htm

sales@uk.uu.net

UUNET

A WorldCom Company

www.uk.uu.net

UUNET Internet House 332 Science Park Cambridge CB4 4BZ United Kingdom