EVALUATION

NHS
Purchasing and Supply Agency

Centre for Evidence-based Purchasing

Report 05094

A beginner's guide to virtual private networks in a Picture Archiving and Communication System environment

March 2006

www.pasa.nhs.uk/cep

Health and social care working together

About evaluation reports

The Centre for Evidence-based Purchasing provides independent and objective evaluations of medical devices available on the UK market. Specialist centres, mainly in NHS Trusts, do the evaluations under contract to the NHS Purchasing and Supply Agency (NHS PASA). Results are available on our website (www.pasa.nhs.uk/cep).

Our evaluations are usually of products supplied by the manufacturer. We expect these products to be representative of those on the market but cannot guarantee this. Prospective purchasers should satisfy themselves about any modifications that might have been made after our evaluation.

The Centre for Evidence-based Purchasing (formerly the Device Evaluation Service) transferred from the Medicines and Healthcare products Regulatory Agency to NHS PASA on 1 September 2005. We are currently undergoing extensive redesign to help us provide the information that purchasers want in the way they want it presented. Please visit our website to keep updated.

Meanwhile, newly published evaluation reports will continue to be e-mailed to subscribers and posted on our website.

How to obtain evaluation publications

To order evaluation reports or to sign up for our e-mail alert service contact:

Centre for Evidence-based Purchasing
Room 152C, Skipton House
80 London Road
London
SE1 6HL

Tel: 020 7972 6080
Fax: 020 7972 5795

E-mail: cep@pasa.nhs.uk

All evaluation reports published since 2002 are available in full colour to download from our website: www.pasa.nhs.uk/cep

Visit our website for a comprehensive list of publications, details of forthcoming evaluations, services and contacts.

A beginner's guide to virtual private networks in a Picture Archiving and Communication System environment

Lead Author
Christopher Dube

Contributing Authors
Dewinder Bhachu, Jonathan Turner,
Keith Stean.

PACSnet
Bence-Jones Offices
St George's Hospital
London SW17 0QT

Tel: 020 8725 3315
Fax: 020 8725 3293

E-mail: query@pacsnet.org.uk

For more information on PACSnet visit www. PACSnet.org.uk

Contents

Summary

The implementation of information technology (IT) in the health sector has been growing at a tremendous rate. Nowadays many healthcare workers are mobile and work from different locations much of the time. Having access to clinical systems from remote locations can be an aid to improve productivity.

Virtual private networks (VPNs) are a way to connect to private networks securely over a public infrastructure, such as the internet. A clinician working from home or a remote site can access a Picture Archiving and Communication System (PACS) and review images and reports via VPN. By using VPNs hospitals can communicate securely with other companies or business partners over the internet.

This report outlines the basic concepts of VPNs, the advantages and disadvantages of VPNs, and the different types of VPNs. It touches on some of the devices used in setting up VPNs.

Also included in this report are the common protocols used in the creation of VPNs and a brief explanation of some of the encryption standards that can be employed.

The use of a VPN is examined through a case study of East and North Hertfordshire NHS Trust which has successfully implemented a VPN and has more than 10 remote users who are actively using it to connect to a PACS web server.

What is a virtual private network?

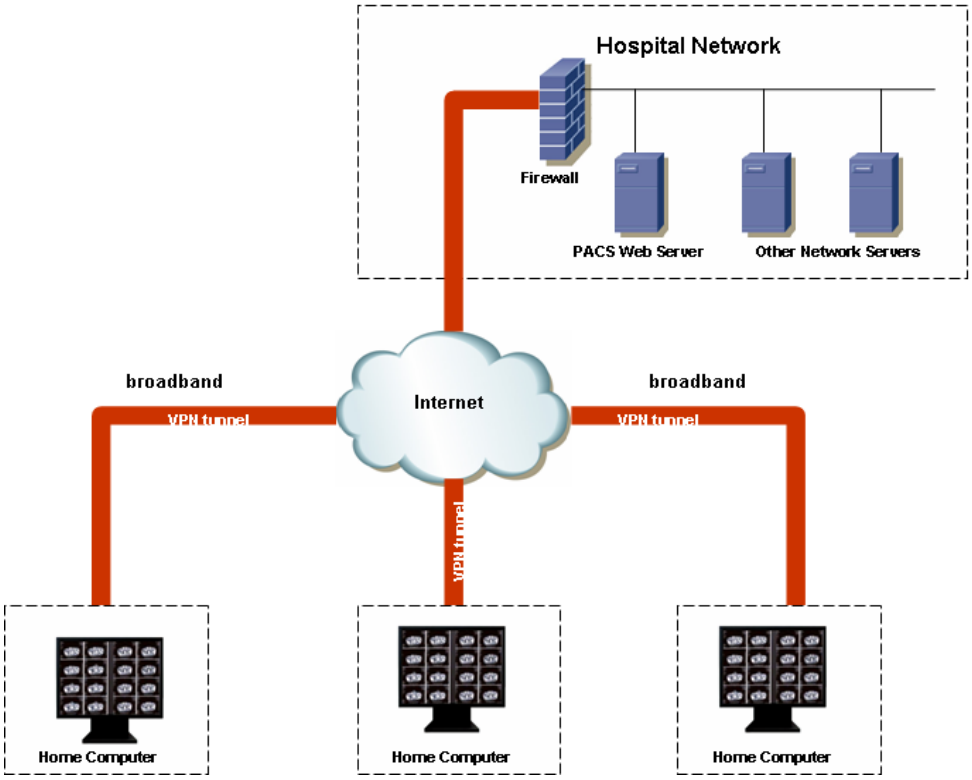
The main concept behind a VPN is to connect users to a private network via a public network such as the internet. This can be done in a secure way so that data moving across the VPN cannot be viewed or altered.

In the healthcare sector VPNs are changing the way many clinicians work. Today's VPNs provide a faster and cheaper way for a clinician working from home or a remote location to access medical images on a PACS and reports stored on a radiology information system. The clinician can also access network resources such as e-mail, and file and print services.

In a VPN data moves through a tunnel which is created between nodes. Tunnelling is a process of placing an entire packet [2] within another packet and sending it over a network. In addition, encryption of data will ensure that no information can be accessed by unauthorised individuals whilst carried over the internet. A well designed VPN should incorporate good security measures.

Figure 1 shows a simplified diagram of how VPNs can be used. Users such as consultants are able to connect to the hospital network from their home computers.

Figure 1. Virtual private network



The user's home computer is connected to the internet with a relatively fast connection such as broadband. This could be Asymmetric Digital subscriber Line (ADSL) or cable. When the user's personal computer (PC) wants to establish a VPN connection, the log on credentials are verified by an

authentication server on the hospital network. If authentication is successful a secure tunnel is created and the connection is allowed through the hospital firewall to the PACS web server.

The user can then view images on the PACS and the associated reports. Hospitals can also connect to external private companies and GPs over VPNs. These external companies can be suppliers or companies which offer services the hospital requires.

Advantages of virtual private networks

Low cost of virtual private networks

Compared with private networks VPNs are cheap to setup and run. Private networks such as leased lines, frame relay and Integrated Services Digital Network (ISDN) costs thousands of pounds more to run every year. According to the Cable and Wireless VPN calculator, a 50-user VPN using ADSL broadband with a contention ratio of 20:1 will cost a fifth of the cost of running 50 dedicated ISDN lines [1].

ISDN is charged according use and by the minute. The Cable and Wireless estimation is based on the usage of ISDN for two hours each day [1]. However a VPN can be used all day and if the same is done for ISDN lines the costs could be very high. With VPN the return on investment is quicker than the traditional wide area network (WAN) and this can eliminate the need for dedicated leased lines.

Increase in bandwidth with the advent of broadband

The last few years have seen an increase in the uptake of broadband by home users and small businesses.

Broadband is now more affordable by most of the home users. The idea of paying a fixed price for an always-on connection to the internet is very attractive to most users. Another benefit of broadband is that the same telephone line can be used for both voice and data transmission. The only downside with ADSL broadband is that the upload speed is still significantly low compared to the download speed. This has an impact on the performance of a PACS web server if it is connected to the internet via an ADSL link.

Reduction in cost of network services

With broadband the service provider is responsible for maintaining the connection to the internet. Equipment, such as switches and routers, used over the internet is maintained by the service provider. The users only pay a fixed amount of money every month for the broadband. With VPNs the operational cost for maintaining a virtual private network is less than that of a traditional WAN.

Extended geographic connectivity

The internet has global network coverage and organisations can take advantage of this global infrastructure. By using a VPN an organisation can extend geographic connectivity if it has offices around the country or world. For example a hospital in the Falkland Islands can communicate with a hospital in the United Kingdom through a VPN.

Improved productivity

VPNs help to improve productivity as some employees can work from home or from anywhere where there is internet access. With some VPNs dedicated equipment and software is not needed. By using VPN, clinicians do not need to come back to the main hospital site if they are on-call or at a remote site which is VPN enabled. A radiologist on call will be able to provide a report quicker if a VPN is available to access the hospital PACS network. This improves patient care and cuts down on the travelling time to the main hospital.

Speed of implementation

Most of the infrastructure for the internet is in place and this makes it quicker to implement a VPN because all an organisation needs is a link to the internet. The connection to internet can be broadband which is now available in most towns.

Disadvantages of virtual private networks

Despite the numerous advantages, there are disadvantages which need to be taken into consideration if an organisation is thinking of implementing a VPN.

Security

The internet has evolved to be an open system with no tight control over access and this is why it is so popular. This is a major concern to healthcare professionals especially when such an open system will be used to move confidential and patient data. In a healthcare context, there is a need to ensure that the data moving across a VPN is not compromised in any way and is only viewed by authorised people.

When implementing a VPN a good understanding of security issues over a public data network is essential. A security policy should be in place, for example the use of firewalls and secure ID authentication. The remote users using a VPN might have computers riddled with viruses, worms, Spyware, and keystroke logging software which is a major security risk.

Limited, non-uniform standards

There are a large number of vendors who provide VPN solutions and most of them have their own proprietary VPN standards. The standards in VPNs are limited and this can result in incompatibility when using software and hardware from different vendors.

Availability

VPNs go through networks which a hospital does not control. If there are problems such as outages or bandwidth fluctuations there is little the hospital can do. The hospital has to wait until the problem has been resolved by the internet service provider (ISP).

Performance

Performance is not always guaranteed when using a VPN which utilises the internet as the underlying network infrastructure. With ADSL broadband performance of the VPN will also depend on the contention ratio of the service the remote user is assigned. The remote user's VPN may be created with a reduced bandwidth if the contention ratio is high. Contention is when the bandwidth available is shared by a number of broadband subscribers.

A contention ratio of 50 to 1 means the broadband bandwidth may be shared by up to 50 subscribers. Broadband with a contention ratio of 1 to1 is available but is more expensive.

Deploying a virtual private network

Implementing a VPN can be a daunting task. There are so many vendors each with their own customised VPN. Some of the vendors work with other VPN partners and can customise a VPN according to a particular specification. This chapter details some of the points to consider when an organisation decides to implement a VPN.

Public data network

A public data network should be in place for a VPN to be implemented. This can be the internet which has become the natural choice for most organisations. The fact that this public network already exists makes it cheaper for using a VPN. A network provided by a service provider can also be used for a VPN.

VPN client software

Some VPNs use special client software installed on the remote user's computer. The software is usually installed by the hospital's IT department or by the company providing VPN services.

Secure ID tokens and digital certificates.

Used in the process of authentication secure ID tokens are for identifying the legitimacy of a user's credentials. Some tokens used in VPNs generate a single-use code. The code changes regularly and is used in the authentication process.

Digital certificates can also be used for authentication. Digital certificates are like electronic identification cards which are tamper proof. They are issued by a certification authority (CA) and downloaded onto a remote user's computer. A digital certificate will contain a public key, expiry date, serial number and other information used for identification.

Firewall

A firewall is a device or piece of software that is intended to prevent unauthorised access to a network. Firewalls are normally installed at the edge of a network. For secure VPNs it is vital that both the remote user and the central office have a firewall installed and configured properly. Firewalls protect networks from external threats by filtering the traffic coming in to and out of the network. Most home users will have a software based firewall system installed on their laptop or PC. Some broadband routers have built-in firewalls.

Access control server (ACS)

The main purpose of an access control server is to provide authentication, authorisation and accounting. They are therefore also known as AAA servers. If

an ACS is used, any remote user not authenticated by it is denied a connection. The ACS can maintain an audit trail, tracking users as they log on. ACS can also be configured to authenticate devices such as routers and wireless access points. AAA servers use security protocols to administer security function. The security protocols used by the ACS include remote authentication dial-in user service (RADIUS), and terminal access controller access control system (TACACS+).

VPN termination and initiation

In order to create a VPN there is an initiation and termination of the VPN. This is done by devices used for the VPN. There are a number of devices which can initiate/terminate a VPN. Some of the devices can be used to do both and others are used only for the termination of VPN tunnels. The equipment used in VPNs is discussed in the chapter on VPN devices.

Antivirus software

With the rapid increase in the spread of viruses and worms it is now essential for computers to be protected from infection. Infection of computers can result in reduced performance of the computer equipment and network, compromising confidential data and possibly a complete shutdown of the network. It has now become mandatory in most NHS Trusts for antivirus software to be installed on personal computers.

Some organisations will not connect a computer or laptop onto their network unless it has up to date antivirus software installed. Once connected the computers should be updated on a regular basis as determined by the IT department.

Desktop security software

Some VPN vendors install security software on the remote workstation or laptop to prevent the theft of data. The security software will do a pre-connection security assessment. During the assessment the software will check to determine if antivirus and firewall software are running. The software will also check for keystroke logging software on the desktop PC. Once a breach in security has been detected no VPN connection is allowed until the responsible IT department has rectified the breach.

Software updates and security patches

Software such as operating systems and application software may contain vulnerabilities and exploits which are usually found after the software has been in use for a while. These bugs or security holes may compromise systems if they are not fixed. Security updates should be applied as soon as they are released. Failure to do this quickly can result in the exposure of confidential data to hackers.

Types of VPNs

There are a number of ways VPNs can be classified. The most common types are ‘remote access’ VPNs and ‘site to site’ VPNs.

Remote access VPN

In a remote access VPN, a single VPN gateway is involved. The remote user usually has VPN client software on the workstation to connect to the central network. Remote access VPNs can be divided into ‘client initiated’ VPNs and ‘network access server’ VPNs.

Client initiated VPN

Remote users use client software to make a secure connection to the organisation’s network. If installed on a laptop a clinician can use the VPN from any site provided there is an internet connection.

Network access server VPN

With a network access server VPN a service provider is outsourced to provide the required VPN. Users connect to the service provider’s network access server first before they are connected to Trust’s network. The network access server determines who is allowed to establish a VPN to the Trust’s network. A connection policy can also be set up on the network access server. This policy can also determine what resources a user is allowed to access on the Trust’s network.

Site to site VPN

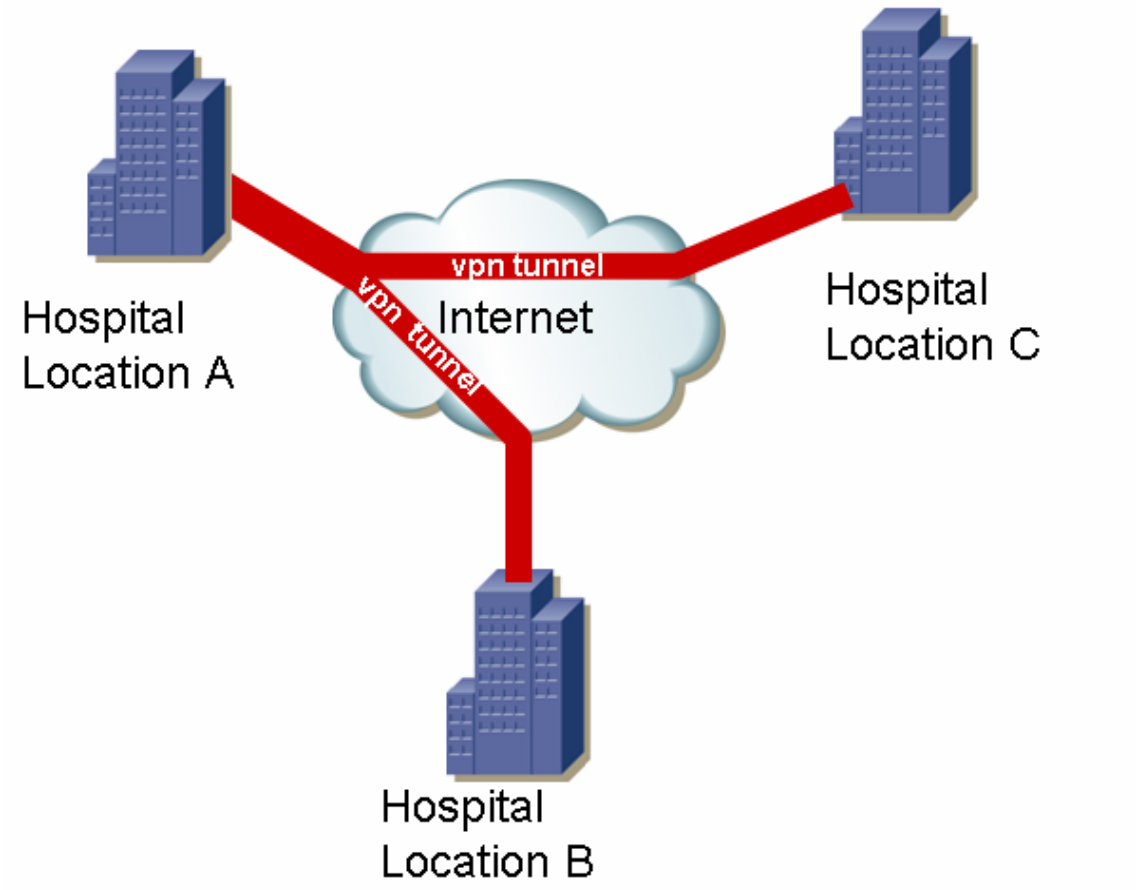
Site to site VPN can be classified as either **intranet** or **extranet.**

Intranet VPN

With this type of VPN there will be a number of VPN gateways at different locations within the same organisation. The different locations will be able to communicate with each other as if there was just one private network.

In Figure 2, the hospital is located on three sites, A, B, and C. Hospital A is the main location. Each location has a local area network (LAN) and an intranet VPN should be able to connect all these LANs together over a public infrastructure. The hospital sites would then communicate securely over the public infrastructure.

Figure 2. Site to site intranet VPN

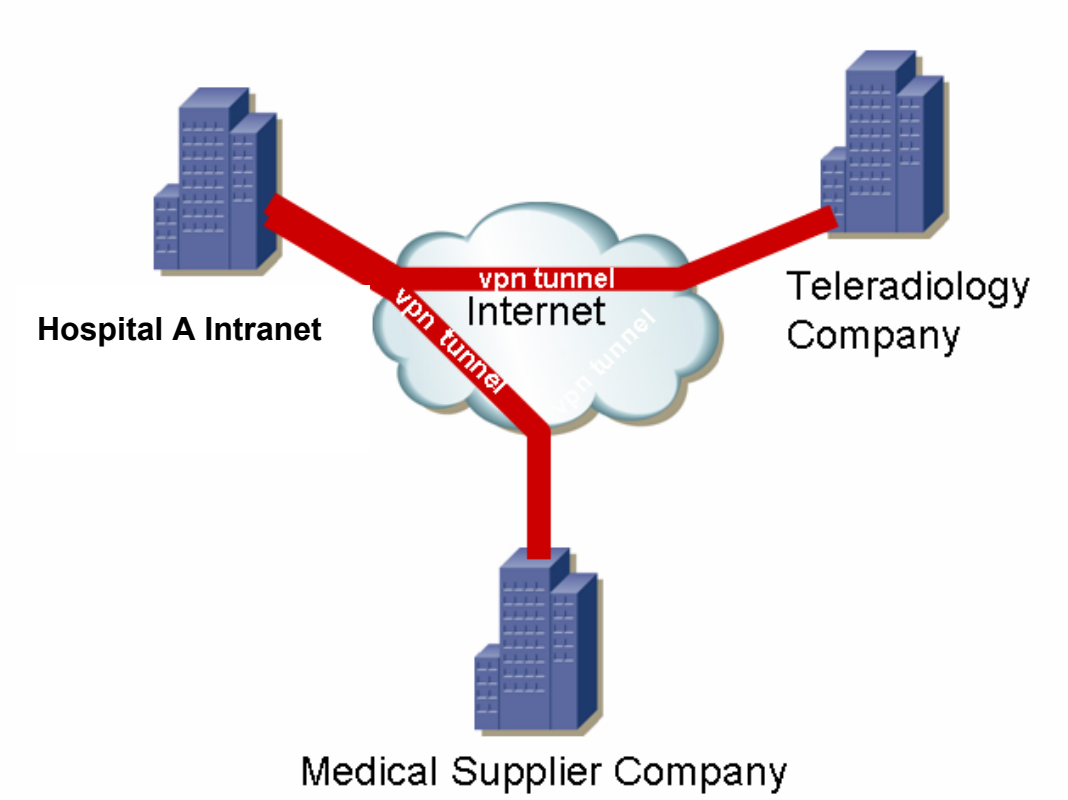


Extranet VPN

An extranet is required when an organisation has close relationships with third parties, such as suppliers or business partners. By using an extranet VPN these third parties are able to connect securely to the organisation's intranet over a public infrastructure.

In Figure 3, hospital A might use an extranet VPN if their radiology images are reported by a teleradiology company which the hospital has contracted. In this instance the teleradiology company offers radiology reporting services to a number of hospitals. Once a procedure is complete Hospital A will transmit the images over a secure encrypted VPN to the teleradiology company. The radiologists at the teleradiology company are able to look at the images as soon as they are received, carry out the report and send the report back to Hospital A.

Figure 3 Site to site extranet VPN



This setup works well because the hospital does not have to worry about having a radiologist on site at night and they get the report quickly especially for urgent cases. With this example the teleradiology company is the external partner. The Hospital will have firewall restrictions on how much access the teleradiology company has on their network via the VPN.

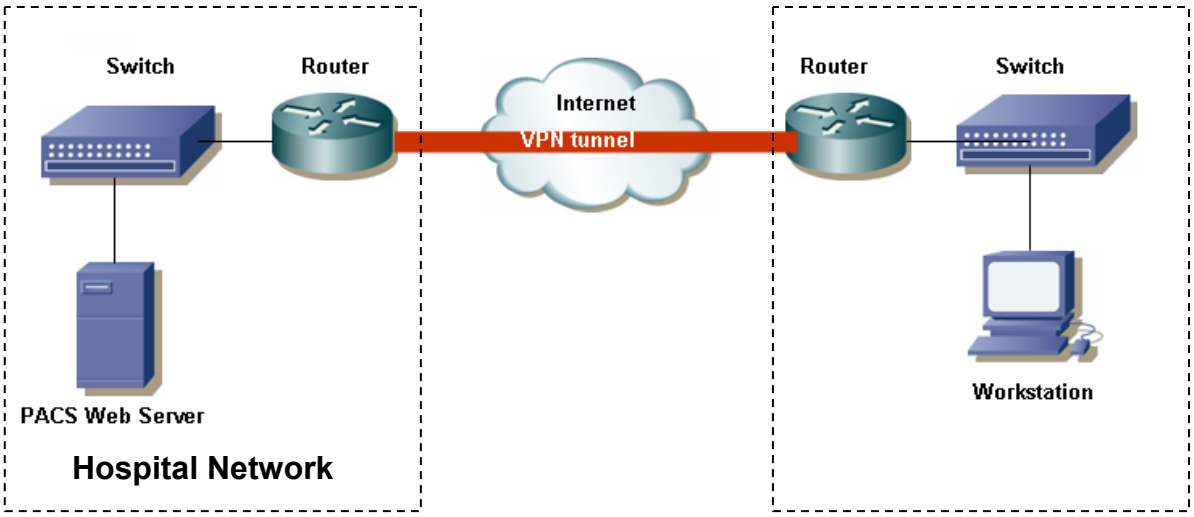
VPN devices

There are numerous devices which can be used when VPNs are set up. VPN devices can be connected in a number of ways. The aim of this section is to illustrate some of the ways in which VPN devices can be connected. The devices described in this section form the core of some VPNs and there might be additional equipment which is required but not mentioned in this section.

Router to router connection

In a router to router configuration the VPNs are not flexible when compared to software based VPNs but once configured they are easy to use. They provide the highest data throughput of all VPN systems. The disadvantage of this setup is that matched routers at both ends of the tunnel are required. In Figure 4 the VPN is created between the two routers. Some routers can also act as access control servers.

Figure 4. Router to router

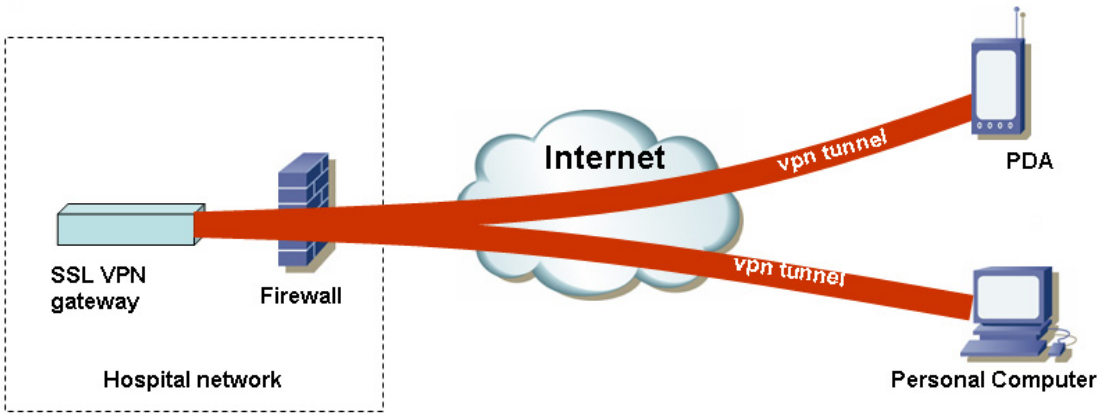


Secure socket layer (SSL) connection

SSL VPN uses the SSL encryption function already built-in to web browsers such as Netscape or Microsoft's Internet Explorer. This type of VPN allows users to access the Trust's network from anywhere provided there is an internet enabled computer. Some SSL VPN gateways can allow both access to web based applications and client-server applications.

In Figure 5 the SSL VPN gateway terminates the VPN tunnels from the personal computer and personal digital assistant (PDA). This type of VPN has been growing in popularity as special software is not needed on the remote user's personal computer. IT administrators do not have to configure any software on users' personal computers, laptops or PDAs.

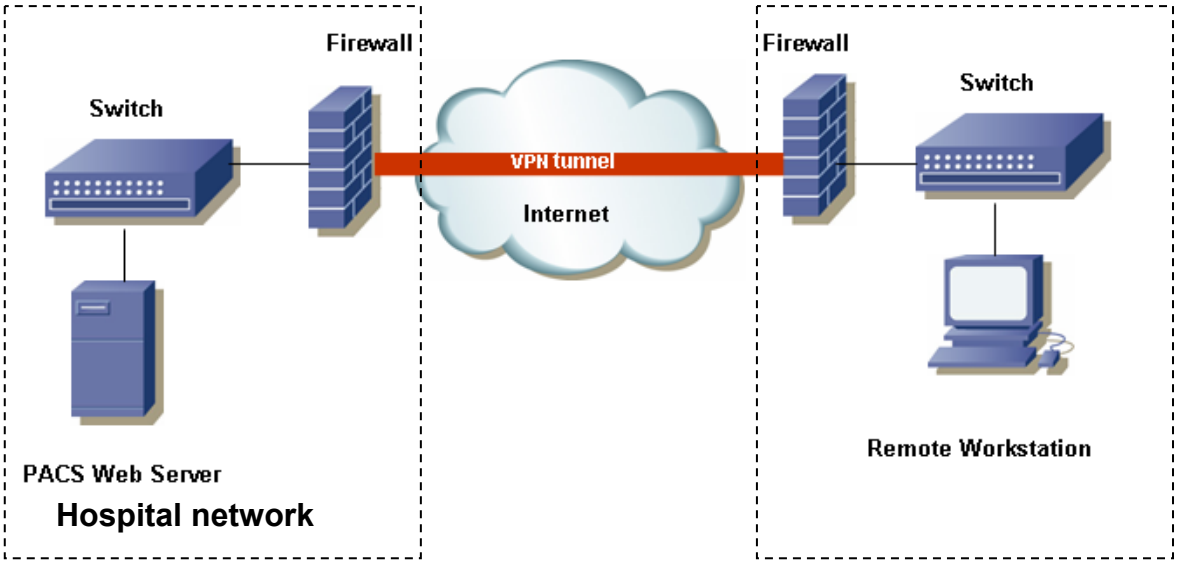
Figure 5. Secure socket layer (SSL) connection



Firewall to firewall connection

Figure 6 shows a VPN setup which utilises firewall devices. With this set up the VPN is created between two firewalls. One firewall creates the tunnel and the other terminates the VPN connection. All the traffic moving between the two firewalls is encrypted. The firewalls also check the traffic using an access control list. Any traffic not defined in the access control list as genuine is discarded.

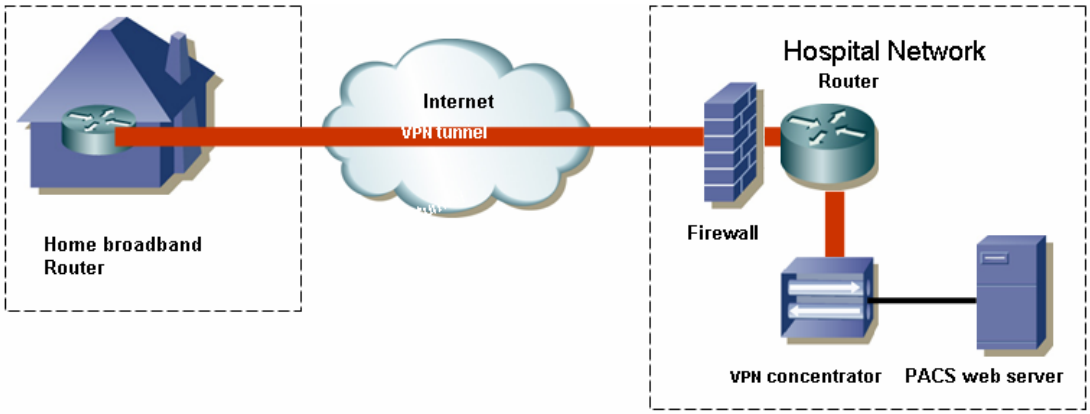
Figure 6. Firewall to firewall connection



Router to concentrator connection

Figure 7 shows a VPN concentrator on the hospital network terminating the VPN tunnel from the house of a clinician or radiologist. The VPN concentrator can create a lot of VPN tunnels enabling multiple users to connect simultaneously. If an organisation has a large workforce of remote users then the VPN concentrator will be the best choice to go for. VPN concentrators can also provide encryption; some VPN concentrators can provide Secure Socket Layer (SSL) and Internet Protocol Security (IPSec) VPN connectivity on a single platform. VPN concentrators offer high performance, high availability, reliability and cost savings for remote access solutions.

Figure 7. VPN concentrators



VPN Protocols

VPNs rely on tunnels to move data and these tunnels are created by tunnelling protocols. There a number of protocols which can be used and the choice depends on the type of VPN deployed and the configuration required.

Generic Routing Encapsulation protocol (GRE)

This protocol was developed by Cisco and is used to encapsulate a wide variety of protocol packet types inside tunnels resulting in the creation of virtual point to point links. GRE does not support encryption and can be monitored by a protocol analyser.

Point to Point Tunnelling protocol (PPTP)

This protocol was developed by Microsoft, US Robotics and other vendors to securely transmit data over the internet. This protocol is no longer considered secure and some vendors recommend that it should not be used at all. It works in conjunction with GRE. Problems are encountered if a firewall is used because of the way PPTP is designed to work. However this protocol is easy to use.

Layer 2 Tunnelling protocol (L2TP)

L2TP combines the best features of two tunnelling protocols. Layer 2 Forwarding (L2F) protocol, which was developed by Cisco, and PPTP from Microsoft. L2TP is an extension of point-to-point protocol (PPP) and PPP is a layer 2[2] protocol used to transport internet protocol (IP) traffic over point-to-point links such as ISDN. L2TP does not support encryption.

IP Security protocol (IPSec)

IPSec was developed by the Internet Engineering Task Force (IETF) to support the secure exchange of packets at the internet protocol (IP) layer [2]. IETF is an organisation which develops and promotes standards called Requests for Comments (RFC) that deal with architecture and operation of the internet. IPSec operates at the network layer [2]. IPSec is a combination of protocols. IPSec supports encryption and it is the protocol of choice for large organisations wanting their data secure. IPSec is a multi vendor protocol and is used on routers, firewalls, personal computers and servers. IPSec is scalable and has built-in key management. IPSec can be used in two modes which are tunnel mode and transport mode.

Internet Key Exchange protocol (IKE)

IKE is used in conjunction with IPSec. IKE allows IPSec users to agree on security services such as authentication and encryption. IKE operates in two

phases. The first phase establishes host authentication, encryption algorithm and keys to be used. The second phase establishes the actual IPSec algorithms, and keys used for the VPN.

Secure Sockets Layer (SSL)

This protocol was developed by Netscape to move data securely over the internet. Browsers such as Internet Explorer and Netscape support this protocol. Secure sockets layer protocol is used in what has come to be known as clientless SSL VPN. This type of VPN only requires a browser and does not need any special equipment or software to establish the VPN.

Transport Layer Security (TLS)

The Transport Layer Security is a successor to SSL. It is an IETF standard protocol. This protocol is used for authentication and establishing a secure encrypted connection between client and server. TLS can use the RSA algorithm for encryption and is application independent. The revised version 1.1 is now published.

VPN encryption

The use of VPN in a PACS environment requires consideration of other issues such as the confidentiality of patient data. Encryption is a way of translating plain text into secret code. Encrypted data going through a VPN tunnel cannot be easily viewed by unauthorised users.

Symmetric encryption

Also known as secret-key encryption, symmetric encryption algorithms use the same key to perform encryption and decryption. This type of encryption is suitable for encrypting large volumes of data. Examples of symmetric encryption are DES (data encryption standard) and triple DES.

Asymmetric encryption

Also known as public key encryption, asymmetric encryption uses two keys; one key is used for encryption and the other key for decryption. Asymmetric encryption is processor hungry. This type of encryption is suitable for encrypting authentication information. RSA and Diffie-Hellman are examples of asymmetric encryption.

Common Encryption Standards

Data Encryption Standard (DES)

DES was developed by IBM in 1974. DES is a symmetrical encryption algorithm and uses an encryption key which is effectively only 56 bits long. This encryption key is now small considering that computers have so much processing power. With DES the main algorithm is applied sixteen times during encryption.

Triple Data Encryption Standard (3DES)

This encryption standard was developed to reinforce DES which can be broken by trying a large number of all possible keys (referred to as brute force attack). 3DES was developed by Walter Tuchman and is an application of DES and uses different keys to encrypt data blocks. Each data block is encrypted three times. The maximum effective key length of Triple DES is 112 bits.

Advanced Encryption Standard (AES)

AES was formed to replace 3DES is symmetric encryption. AES uses any of the 128, 192 and 256 bit encryption keys and is strong and fast. Each key makes the algorithm behave differently. DES is mainly for hardware encryption but AES can run over a wide range of platforms such as smart cards, computer software on desktops or laptops, hardware such as routers and firewalls, web browsers etc.

RSA encryption

RSA encryption algorithm was developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman. They developed it at Massachusetts Institute of Technology (MIT). RSA encryption is commonly used with web browsers such as Netscape. This type of encryption is mostly used in SSL type of VPNs and is based on the public key system. RSA encryption is asymmetric and uses two digital keys, one for encryption and the other one for decryption.

RSA encryption takes more processing time than most encryption methods. It is not suitable for encrypting very large volumes of data. RSA encryption is suitable for use in authentication.

East and North Hertfordshire NHS Trust

Brief overview of the hospitals

East and North Hertfordshire NHS Trust consists of three major hospitals: Hertford County Hospital in Hertford; the Lister Hospital in Stevenage; and the Queen Elizabeth II Hospital in Welwyn Garden City. The trust provides services to a population of 500,000 people and has a workforce of over 4,200 staff. The diagnostic imaging departments in East and North Hertfordshire NHS Trust carry out approximately 217,500 examinations annually and they use a Kodak PACS.

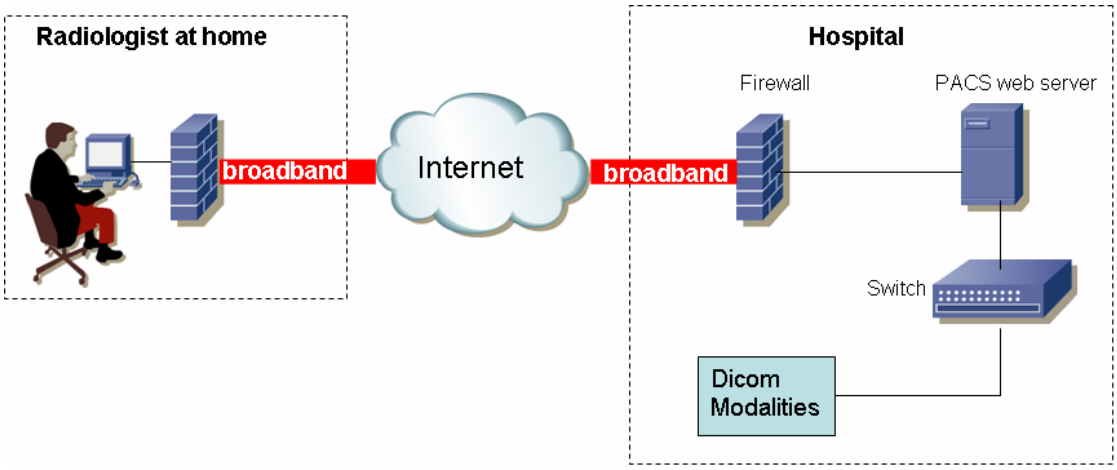
Old solution

Before implementing the VPN solution the radiologists were using ISDN to link to RadWorks, a teleradiology solution. With this system radiologists and clinicians could only view images of the most recent scans. They were not able to view other images, or reports on previous images. Although this setup worked they found that it was slow and limited.

VPN solution

The trust decided to implement a broadband VPN solution, which was installed and managed by Hicks Associates. The radiologists and clinicians use the VPN for reporting and commenting when they are on call. Figure 8 illustrates a simplified schematic overview of the VPN solution. The PACS web server is

Figure 8. VPN solution



located at the Lister Hospital. On the hospital network a firewall terminates the VPN connections. The firewall can terminate up to100 VPN tunnels and is connected to the internet using British Telecom ADSL broadband link with an upload speed limited to 270 Kbps. Network address translation (NAT) is done by the firewall. 3DES is used for encryption and IPSec as the tunnelling protocol.

Radiologists have ADSL connections in their homes that connect to the internet using a broadband router with a built-in firewall. The router also does network address translation to give more added security.

The radiologists use different ISPs and the trust pays for the broadband monthly subscriptions. Each radiologist is supplied with a computer by the radiology department.

User experience

According to the PACS manager, the radiologists think that the VPN solution is faster. A radiologist can now download a CT study in approximately three minutes. They also believe that it is more reliable.

With Radworks the radiologists were not able to access previous scans and reports and this is now possible with the VPN solution. In the past on-call radiologists had to come to the hospital to view plain radiographs if the clinicians were unable to diagnose. Now using the VPN the radiologists can view the images from home. The ability to access previous scans and reports have made the radiologists more confident and accurate in their comments on scans.

Next steps

According to the PACS manager of East and North Hertfordshire NHS Trust, users have complained that the VPN is slow at certain times. The PACS manager investigated and found that this happened when all the users are accessing the VPN simultaneously.

David Hicks of Hicks Associates commented that the system is reasonably reliable and some of the problems which occur are due to the fact that:

- Some of the consultants use their own broadband and in some cases the contention and user load slows the data transfer dramatically.
- Some internet service providers have problems with IPSec VPN data and others block it completely.

To improve the service the upload speed from the web server to the internet needs to be increased. At the moment the maximum achievable upload speed is approximately 270Kbps. This has a considerable impact when all users are downloading images at the same time.

When symmetric digital subscriber line (SDSL) is available the current Trust ADSL can be upgraded. With SDSL the upstream and downstream speed are identical and if the link is upgraded to 2 Mbps users would see a significant improvement when downloading studies.

The future of VPNs in PACS

By 2007 the majority of hospitals in England will have a PACS system in place. Some of the hospitals will have implemented a VPN or trialled one. Like all new technologies, once a critical mass of early adopters have used VPNs and appreciate the benefits, others will follow in adopting the technology.

Some ISPs can now provide the next generation of broadband with download speeds up to 24 megabits per second. It is expected that in a few years time the price of broadband connections will have gone down and the speed of the connections gone up. With a number of hospitals now acquiring 64 slice CT scanners the number of images stored on PACS is expected to increase. The next generation of broadband should be able to cope with downloading of a large number of images when using a VPN.

N3 is the new national network which is going to be used to connect NHS IT systems. Once N3 has been fully implemented it will be possible to use this network for implementing VPNs.

Voice recognition is a tool which is becoming increasingly popular with radiologists for reporting on PACS workstations. As more and more radiologists use VPNs to access PACS they will no doubt want to use voice recognition/digital dictation over VPNs.

Bibliography

Morgan B. CCNP Building Scalable Remote Access Networks, Indianapolis. Cisco Press. Nov 2003

Benjamin H, Heffner C, Paquet C, Building Scalable Remote Access Networks, Cisco press. Jan 2004

European e-trade to overtake US, ITWeek 11 April 2005

BT broadband goes to 5 million, ITWeek, 11 April 2005

http://findvpn.com Articles and Guides About Virtual Private Networks

http://www.windowsecurity.com/articles/VPN-Options.html Comparing VPN Options

http://www.vpnc.org/vpn-technologies.html VPN Technologies: Definitions and Requirements

http://vpn.shmoo.com VPN Information on the World Wide Web

http://www.cisco.com

http://www.webopedia.com

References

[1] http://www.healthvpn.co.uk/ Cable and Wireless

[2] MHRA Educational Report MHRA 03053 PACS Education: Beginners guide to networks: part I & II. Medicines and Healthcare products Regulatory Agency; 2003.

Glossary

Please refer to the PACSnet online glossary on the PACSnet website http://www.pacsnet.org.uk

Asymmetric digital subscriber line (ADSL) This is a method of delivering data at high rates over ordinary phones lines. With ADSL the downstream data rate is higher than the upstream rate.

Contention ratio Contention is when the bandwidth available is shared by a number of broadband subscribers. A contention ratio of 1:50 means a broadband subscriber will be sharing the bandwidth with forty nine other subscribers.

ISDN2 This is an international standard for transmitting voice, data and video over digital telephone lines. ISDN uses bearer channels to carry voice, data and video. ISDN2 consists of two bearer channels and each channel has a bandwidth of 64 Kbps.

Gateway A network device that links two or more networks.

Internet Service Provider (ISP) Any company that allows subscribers gain access to the Internet, usually via a telephone line, cable, ADSL line, ISDN or a leased line.

Local Area Network (LAN) A computer network that spans a small area.

Network Address Translation (NAT) A method of connecting computers to internet which use unregistered IP addresses. The unregistered (private) IP addresses are translated to a registered IP address which can be used to connect to the internet.

Packet Data sent over a LAN is separated into blocks known as packets to create optimum transfer over a packet-switching network. One of the key features of a packet is that it contains the destination address in addition to the data.

Sniffer Computer software or a device that monitors data travelling over a network.

Symmetric digital subscriber line (SDSL) This is a version of DSL where the upload and download data rates are the same.

Wide Area Network (WAN) A computer network that spans a relatively large geographical area and typically consist of more than one LAN.

Acknowledgements

PACSnet would like to thank Dave Harvey of Medical Connections (www.medicalconnections.co.uk), David Hicks of Hicks Associates (www.hicksassociates.co.uk) and Ruth Gilbert, the PACS Manager at East and North Hertfordshire NHS Trust for their assistance in the production of this report.