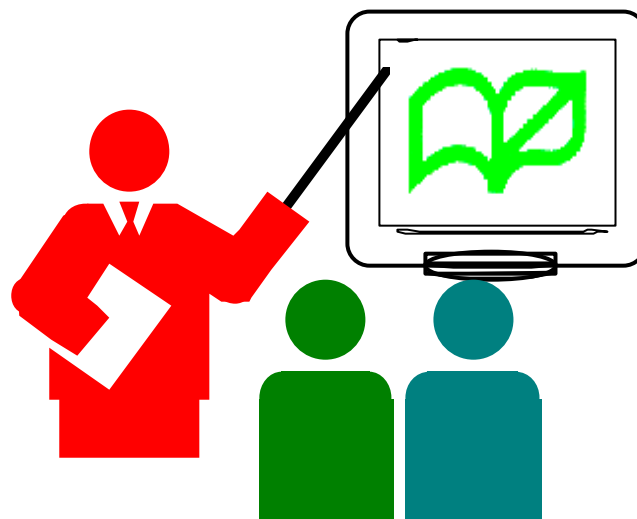


Information Technology in Education Project

Remote Access- Virtual Private Network

(RM09/2002)



**Infrastructure Division
Education Department
The Government of HKSAR**
www.ited.ed.gov.hk

November 2002

For enquiry on this document, please direct to inspector of Regional Support Section, Infrastructure Division, Education Department at (852) 3123 8103 or write to Principal Inspector, Regional Support Section, Infrastructure Division, 5th Floor, Kai Tak Government Building, 5 Arrivals Road, Kowloon City, Hong Kong.

The full text of this publication is available at the Information Technology Education Resource Centre home page at <http://www.ited.ed.gov.hk>.

Remote Access-Virtual Private Network

Virtual Private Network (VPN) has recently become a very common method of remote access application in this ever-changing world. It enables users to use the existing Internet infrastructure to establish a remote connection to enhance the resource availability and productivity.

About this document:

This document is designed to help readers to understand the nuts and bolts of VPN as well as the choices available to enhance the security of a VPN.

After reading this document, readers should be able to distinguish different VPN devices available in the market and be aware of the necessary considerations to set up a secure VPN.

Modem pool

In the past, "dial-up connection" is the only way for providing remote access service. In this case, user is required to set up a modem pool consisting of a number of modems and telephone lines on the server side. However, remote access using a modem pool is unsafe. It is because modem connection is always considered as the backdoor for hackers. In addition, there is no encryption of the data transferring between the remote clients and the servers. Also, such arrangement is not suitable for LAN-to-LAN connection due to its uncertainty in availability.

Moreover, remote access service using one or two dial-up lines is easily setup with less cost. But, user should be aware that such arrangement will become expensive when the number of modems and telephone lines have to be increased to meet the demands from more remote clients.

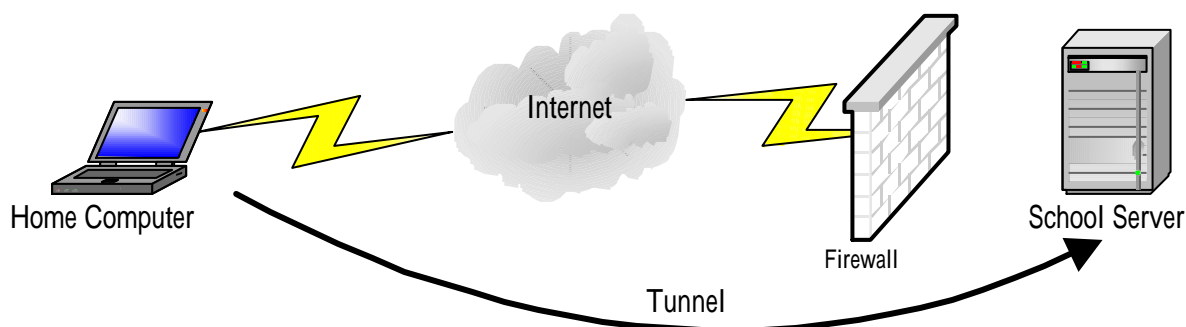
Remote access in schools

Schools may have a need to set up a remote access service to enable users to access the school servers after school hours. For example,

- To allow teachers to use their home computers to retrieve or update those teaching materials stored in their school servers;
- To enable teachers to run certain school applications remotely; and
- To enable system administrators to monitor and maintain the school network outside school premises.

What is VPN?

VPN is a private data network that makes use of the public network (mostly the Internet) to provide private connections. VPN maintains its privacy by using tunneling technologies and security procedures. Essentially, tunneling is the process which involves encapsulation, encryption and routing. Tunneling wraps (or encapsulates) the original packet inside a new packet which travels through the Internet. Encryption may also be applied to enhance the data integrity and privacy of the packets.



Note: Internet is a connectionless packet switching network. Messages are divided into many small packets that flow through a cloud of servers or routers until they reach their final destination. The technology is not secure because data packets can be trapped by hackers during the flow.

Data communication using VPN is safer than ordinary Internet traffic. It is because the encapsulated data packets can prevent hackers from reassembling them into the original message even if they are trapped.

Notes: VPN can be used over the Internet or within an Intranet. In addition to remote access service, it can be used for other purposes such as LAN-to-LAN Bridge and Extranet VPN. However, these applications will not be covered in this document.

Tunneling protocols

Among various tunneling protocols, the following three commonly used tunneling protocols will be discussed:

- IP Secure (IPSec);
- Point-to-Point Tunneling Protocol (PPTP); and
- Layer 2 Forward Protocol (L2FP).

IPSec is the de facto standard for VPN. It is originally designed to provide LAN-to-LAN tunneling. It is more complicated to be set up but it provides more comprehensive features, especially in security.

PPTP and **L2TP** are much easier to be set up and they are supported in Windows operating system. By setting up a PPTP server, users can use the built-in VPN features in Windows for VPN connection, without loading extra client software.

In contrast with IPSec which handles only IP packets, PPTP and L2TP support different protocols and they are more suitable in multi-protocol environments, such as a LAN running NetBEUI, IPX and AppleTalk.

The low cost, easy setup and integration with Windows operating systems make

IP Security (IPSec) is a collection of authentication and encryption protocols, that are developed by the Internet Engineering Task Force (IETF). It can be used either as a complete VPN protocol solution, or simply as the encryption scheme within L2TP or PPTP.

IPSec extends standard Internet Protocol for the purpose of supporting more secure Internet-based services (including, but not limited to, VPNs). It is designed to address data confidentiality, integrity, authentication and key management, in addition to tunneling.

Point-to-Point Tunneling Protocol (PPTP) is a tunneling protocol developed by Microsoft. It was developed originally as an extension to PPP (Point-to-Point Protocol) which is used for TCP/IP of serial lines (dial-up modem connections). PPTP is relatively easy to be set up.

Layer Two Tunneling Protocol (L2TP) is the hybrid of the Cisco's Layer 2 Forwarding (L2F) Tunnel Protocol and Microsoft's PPTP. It is commonly used for node-to-node applications where the tunnel terminates at the edge of the user's network. However, L2TP does not include schemes to secure the packet level information. It relies on the use of other security schemes such as IPSec for data confidentiality.

PPTP a viable remote access solution that does not require heavy-duty encryption and authentication.

Proprietary VPN products

Other than the three mentioned industrial standards of VPN, some manufacturers are deploying VPN solution based on their own developed protocols, such as the Layer two Forwarding protocol (L2F) from Cisco.

The major advantage of using such proprietary VPN protocol is that commonly known hacking tools are not applicable to these devices/solutions. However, it has a disadvantage that only the manufacturer can provide security refinement, especially when some vulnerabilities are found on these devices.

Implementation

Schools may either set up VPN facilities inside their school premises or acquire VPN service from service providers. Basically, there are three typical approaches to set up VPN facilities in schools. They are:

- Hardware-based VPN;
- Software-based VPN; and
- Outsourcing.

Hardware-based VPN

Most schools already have Internet access devices, such as routers or firewalls, to protect their Internet connections. Some of this hardware can be upgraded to provide additional features.

VPN Router

Some router manufacturers have added VPN features to their products by means of software upgrade.

For the router with VPN support, schools may simply upgrade the router software for VPN enhancement without buying additional hardware. The deployment is easier.

However, intensive CPU processing is required for data encryption during the building of the virtual tunnel, which may lead to a degradation of the router's performance and limit the throughput. Schools should consider this issue if there will be a large number of potential concurrent users for the service.

Hardware Firewall VPN

Most users like to group all Internet related security activities onto the firewalls. As a result, many firewall packages now support VPN services within their firewall systems. This can be done by either software or hardware upgrading.

This approach is similar to the router-based approach. Thus their benefit and consideration are very much similar.

However, normally it is much more expensive to upgrade a firewall.

Software-Based VPNs

Schools may have many servers in the school network such as domain controllers, file server, proxy server, mail servers and firewall system. Additional features such as VPN can be added to these servers.

Operating system VPN option

For network operating systems, Microsoft and Novell had developed the VPN service modules for their server operating systems.

One of the main advantages of this option is that it allows us to share the user account data and to control the access by applying defined user-access privileges. Similar to router-based VPNs, performance degradation issue may be happened when the number of concurrent users increases. However, this problem can be solved by deploying a higher performance server or a cluster of servers.

Software Firewall VPN module

Some software firewalls also have VPN modules too. These modules are usually more powerful but more expensive when comparing with the server VPN options. Schools that are using software firewall can check whether a VPN module is available or not.

Outsourcing

School may simply outsource the VPN service to an Internet Service Provider. The provider will set up the necessary hardware or software in respect of the required services to school. Hardware equipment may be set up either inside or outside the school premises.

The advantage of outsourcing is that school needs not to consider the hardware maintenance cost, system performance or technical support issues. As a result, school may increase or decrease the requirement of the number of VPN connections based on the school IT

development or the number of new users. Of course, the provider may have different charging schemes for different number of VPN connections.

Deployment Considerations

Before deploying VPN to let your mobile users to access the school servers, the following issues should be reviewed:

Security

Allowing external users to enter the school network via the Internet may affect the security of the whole network. Schools should consider deploying strong security measure to prevent hackers, such as:

- Limit the number of users who are authorized to use the services;
- Protect/limit the amount of sensitive data to be accessed from outside;
- Schedule the availability of service or offer the remote login service on a need-to-do basis;
- Always enable security logging and perform regular security auditing; and
- Change user password or digital certification periodically.

Interoperability

One of the key benefits of VPN is its capability to enable applications of different network protocols to work under a TCP/IP network. Nevertheless, it is not guaranteed that all applications can be successfully run under VPN. Schools are advised to have a trial run before deploying the service.

Performance

Setting up VPN tunnels involve encryption and decryption of data packets. A stronger security requirement may request a longer encryption key and thus a longer processing time. Schools should note that the required encryption and decryption processing time would be multiplied by the number of concurrent connections.

Thus school is advised to conduct a capacity planning to see whether additional dedicated server is required to support the VPN connection.

Cost

Schools should justify the cost in relation to the benefits gained. Schools may consider (a) purchasing a dedicated device; (b) purchasing add-on software; (c) upgrading the existing hardware; or (d) enabling the bundled service in their school servers.

While selecting among these options, schools are advised to make good use of the existing hardware until the resulting performance is not acceptable.

Summary

VPN is a technology that helps data packets transmit over the Internet, with an additional security protection, which even hackers found difficulties to reassemble the data into the original content after being captured.

There are various types of VPN standards and implementation methods available in the market. Each of them has its own strengths and weaknesses. School is advised to review its requirements on remote access seriously and to discuss with the market practitioners to identify the most suitable remote access solution for school.