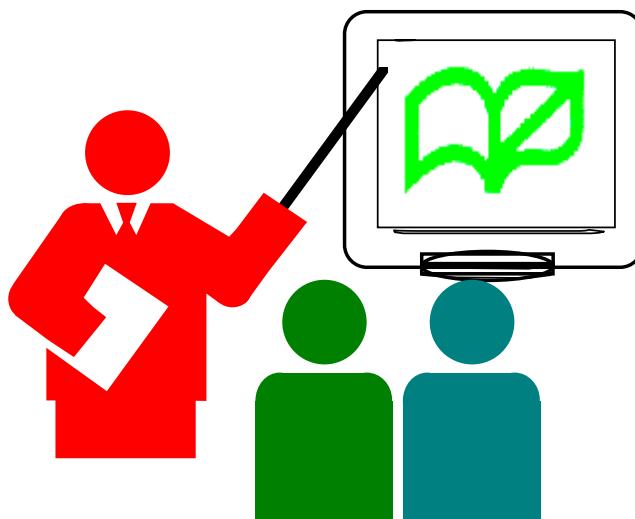


Information Technology in Education Project

Understanding your Internet Gateway

(RM08/2002)



**Quality Education Division
Education and Manpower Bureau
The Government of the HKSAR**

www.emb.gov.hk/ited/

revised in Nov 2005

For enquiry on this document, please direct to the Information Technology in Education Section, Education and Manpower Bureau at (852) 3123 8228 or write to the Principal Inspector, Information Technology in Education Section, Quality Education Division, Shop 28-37, UG/F, Phase I, Waterside Plaza, 38 Wing Shun St., Tsuen Wan, N.T.

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

Understanding your Internet Gateway

Internet is basically a virtual network that allows users to communicate with other connected servers and hosts, as if all of them were part of a local network. However, there is no committed security over the Internet, every site is responsible for its own security.

When schools are connecting their own networks to the Internet, their networks are potentially put under the threats of hacker attack. To protect the interest of schools, it is important to set up a secured Internet Gateway in their school networks.

About this document:

This document discusses some popular Internet Gateway solutions which are composed of router, proxy and firewall systems. It also discusses their security limitations and provides tips to improve such limitations.

There are many different types of Internet Gateway solutions in the market. Schools are advised to consult with their suppliers for those solutions not mentioned in this document.

Internet Gateway

Internet Gateway is a bridge that links up a private network (e.g. school network) and the Internet. All incoming Internet traffic to and outgoing Internet traffic from the private network must pass through the Gateway. Since it is the only outlet of the private network, it is an ideal point where we can impose the security measures. In general, schools may use the following equipment/system to set up an Internet Gateway:

- Router
- Proxy system
- Firewall system



Table 1 summarizes some pros, cons and technical details of using the above equipment/system as an Internet Gateway. For details, reader may read Section 6.1.2 of "IT security in Schools", which is available at:

[http://202.64.213.147/ited/Support_Service/TSS_Ref/IT_Security_in_Schools \[Nov 05\].pdf](http://202.64.213.147/ited/Support_Service/TSS_Ref/IT_Security_in_Schools_Nov_051.pdf)

Table 1: Pros and Cons of different Internet Gateways

| Type | Pros | Cons | Technical Details |
|-----------------|---|--|--|
| Router | Low cost | Sophisticated configuration cannot be easily done. | Router is an electronic device that controls flow of data packets of a network in circuit level. It works like a "middle man" that takes a look at a data packet, forwards it to some destination or drops it. Since it works in circuit level, it cannot perform high-level control, like content filtering. |
| Proxy system | Can also be used for content caching | Technical skills required. | Proxy server is a system that controls data flow in application level; i.e. it is capable of resembling data packets into a message, and looking on its content before letting it go. Thus a proxy server is capable of performing some high-level controls like content filtering or virus scanning. |
| Firewall system | Extensive filtering rule-set can be configured. | Technical skills required. Relatively expensive | Firewall is a system that normally has a combined design with controls in both the circuit level and the application level, thus it is capable of controlling flow of data packets as well as messages. Firewall system may be an electronic box, a server with firewall software running on it or a combined system of routers and proxy servers. |

Since the above equipment/system provides security protection on different communication layers, it is possible to have them to be deployed together. The coming sections will give more examples about the configuration of these items. Limitations and tips in adopting these items will be covered.

However, since this document is not intended to be a cookbook for setting up an Internet Gateway, schools should consult the suppliers to identify a suitable solution with proper security protection for their schools.

Internet Gateway using Router

Router is the simplest implementation of an Internet Gateway. Normally, a router with NAT (Network Address Translation) feature can be configured into an “one-way”

Network Addressing Translation

In order that a machine within a private network can communicate with the outside Internet, one of the simplest ways is to translate the IP address of the internal host (i.e. the machine's IP address in the private network) into a real address of the Internet. Such technology is called NAT (Network Addressing Translation). Almost all Internet Sharing Devices support NAT. However, only NAT alone provides limited security protection to a private network.

Personal Firewall Software

Personal firewall is software that will normally be installed in a personal computer and run locally. While a workstation is connected to the Internet, personal firewall will provide two basic functions. Firstly, it protects the system from unsolicited scans coming from the Internet. Secondly, it offers outbound controls that watch for a Trojan horse or spyware trying to call out from the system. It monitors all Internet data transfer and protects the computer against attack.

Personal firewall normally accompanies with an anti-virus software package or has a built-in anti-virus option. Therefore data coming from the Internet are scanned to ensure that they are safe.

Personal firewall is not solely designed to be used for the above-mentioned scenario; actually, any workstation wishes to gain additional Internet protection against attack should be installed with a personal firewall.

Internet Gateway; that is, only internal workstation in the network can establish links to the Internet, but not vice versa.

However, with such router configuration, an internal workstation is still under the threat of hacker attack when it establishes a link to a hacker site. Hackers may follow the established link to trace and access the workstations and then the whole network resources.



Most Internet Service Provider (ISP) may loan routers to schools for Internet connection purpose. However, schools are not allowed to re-configure them. The function(s) of these routers is/are not equivalent to the function(s) of the above-mentioned router.

There are many inexpensive routers (or Internet sharing devices) available in the market now, such as IP sharer, Internet router, broadband sharer, etc. When selecting such devices, schools should evaluate their performance as well as the number of concurrent users to be supported.



Some Internet sharing devices provide additional features like UPnP¹, DMZ², port redirection, internal hosts access control, etc. Schools are advised to review whether these features are required in schools.

In order to improve the situation, schools may install a personal firewall software package in each workstation connecting to the Internet. However, such software may slow down the performance of the workstation.

Proper use of Proxy server


Instead of installing a personal firewall software package in each workstation, it is wise to set up a central proxy server for all workstations connecting to the Internet. When a proxy server is used to represent all internal workstations for Internet access, it appears as if only this proxy server existed to external hosts. Thus to protect the

¹ UPnP – Universal Plug and Play

² DMZ - demilitarized zone

internal network, we need to strengthen the security of the proxy server.

In addition, proxy server should be installed on a dedicated machine but NOT on the school's main server, or the domain controller. It is because running a proxy server software package on the school's main server or the domain controller will make the server publicly accessible. Hence it becomes more risky to be attacked by hackers as the school's main server or the domain controller may store secured user data.

 Some proxy servers are bundled with proxy client software. Additional proxy services other than web services, such as email, newsgroup, ICQ ...etc, can be provided with this client software.

The following paragraphs describe two common proxy server configurations: **caching server** and **multi-homed proxy server**.

Caching servers

One of the major benefits of using caching server is to improve Internet access performance of the workstation(s) in the internal network. It works by temporarily storing those frequently accessed web pages and delivers them to the requesting workstation without requesting the web pages directly from the Internet again. Diagram 1 below shows a typical configuration of a caching server.

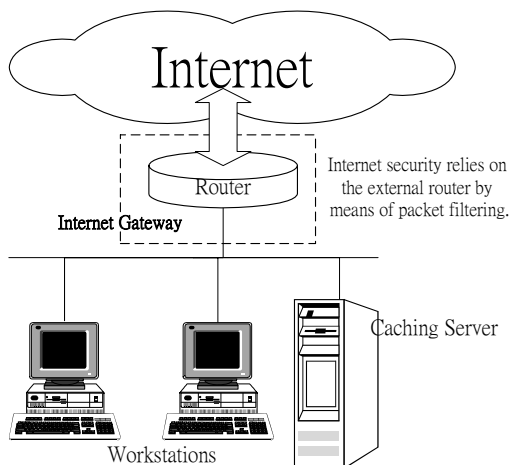


Diagram 1. Caching Server behind a router.

In this configuration, the router should be configured to re-direct all network traffic from the Internet to the caching server only. However, security level of this configuration is more or less similar to the one using a router as Internet gateway mentioned before, because only the router is used to separate the network traffic between the Internet and the internal network. To enhance Internet security, a multi-homed proxy server may be used.

Multi-homed Proxy servers

A multi-homed proxy server is an isolated proxy system with two network interface cards. It connects and sits between school internal network and the Internet. In addition to the caching server capability, it can also filter and control the packets and applications in accordance with user-defined setting or rule-sets.

Schools can further strengthen the protection to the internal network by deploying a multi-homed proxy server behind an external screening router (See Diagram 2 below).

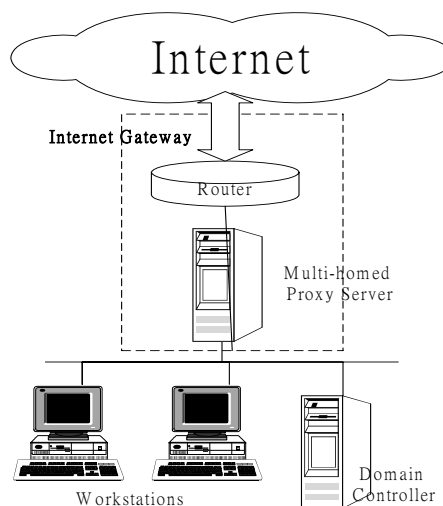


Diagram 2. A screened multi-homed proxy server.

A screened multi-homed proxy server has two network interface cards. One of them connects to the router and will receive traffic from the Internet only; whereas the other will connect to an internal private network and will receive traffic from the internal network only.

Screened sub-network Gateway by multiple routers

When schools are planning to set up public accessible servers such as web server, ftp server or mail server, they are recommended to set up an Internet Gateway with a public accessible zone. A screened sub-network architecture using multiple routers sandwiching a DeMilitarized Zone (DMZ) is usually adopted for such purpose (See Diagram 3).

Both internal and external traffic can enter the DMZ but neither can pass through the DMZ without the assistance of the proxy server and the routers.

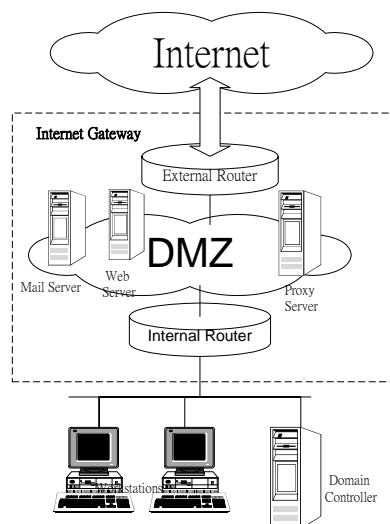


Diagram 3. A subnetwork architecture using multiple routers and proxy server.

Hardware Firewall

A hardware firewall is an electronic box that can manage and analyze data flowing through it. The advantages of hardware firewall are its stability and ease of use. Less administrative effort is normally needed to maintain this kind of device as you can switch it off and on again, then everything will be reset to normal.

There are many hardware firewalls with different features available in the market: (a) some are designed to protect an internal network from the Internet (out-bound only traffic); (b) some have DMZ interface that enables setting up of the public accessible servers; (c) some have Virtual Private Network (VPN) capability that enables a remote user to logon a private network securely via the Internet. Schools should review their individual needs and select the most suitable device.

Software firewall

Software firewall is normally run on a server such as Windows NT server, Sun Solaris server or Linux server. Usually the server may have several NICs (Network Interface Cards), for example: one for Internet, one for LAN (Local Area Network) and one for DMZ.

Software firewall is considered to be more flexible than hardware firewall as memory will be available to keep audit log for further analysis. Upgrading the firewall with a newer version of the software may improve its capability and performance. However, software firewall is usually more complex and difficult to maintain. Internet security expertise may be required to manage and monitor its operation.

Software firewall is considered more sophisticated and complicated, and therefore schools have to evaluate and visualize that schools are by themselves capable of supporting and maintaining such system before deploying it.

Screened sub-network gateway mentioned above is the most popular choice of Internet Gateway for large organizations with their own web servers, ftp server or mail server; heavy traffic; and for those applications that security is critical and redundancy is imperative.

Integrated solution of firewall

Firewalls are specially designed network equipment for keeping unwanted and unauthorized traffic from an unprotected network like the Internet out of a private network. Some firewall manufacturers construct firewall models (consisting of DMZ) that have similar functionalities as screened sub-network architecture discussed above.

In general, there are two types of firewall: **Hardware Firewall** and **Software Firewall**. However, no matter which type of firewall you are deploying in your schools, you should never believe that you are safe and be excluded from hackers' attack after installing it. Only a **well-managed** firewall system can protect the internal network efficiently.

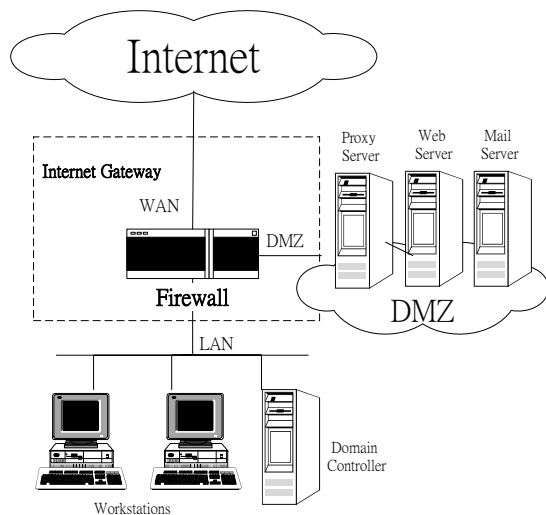


Diagram 4. A typical firewall.

Diagram 4 shows a typical firewall system. Most firewall systems have three network interfaces: one for internal network (e.g. LAN); one for external network (e.g. Internet); and one for DMZ. Public accessible servers and proxy server are placed in the DMZ. Rules should be properly defined in the firewall to prevent data flow between LAN and WAN interfaces directly.

Summary

Internet Gateway is the place where all Internet traffic must pass through. A secured Internet Gateway protects a school internal network from the attacks by Internet hackers, crackers as well as computer virus. This document covers four major types of Internet Gateways commonly used in the market: router, proxy server, sub-network architecture and firewall. (Table 2 below serves as a quick reference to schools to summarize different configurations discussed in this document.)

Schools should note that each configuration can be deployed for other purposes. For example, schools can also use a hardware firewall to set up an outbound only Internet Gateway. Hence, for those scenarios not mentioned in this document, schools are advised to consult with their suppliers.

Finally, schools are reminded that implementation of a secured Internet Gateway is not an one-off exercise. Continuous monitoring and tuning of the system is necessary to achieve the best result.

Table 2: Summary of Different Internet Gateways mentioned.

| Possible Internet Gateway in Schools | Corresponding Section in this document | Application mentioned in this document | Remarks |
|---|--|---|---|
| Internet Router only | Internet Gateway using Router | Outbound only Gateway | Not recommended. Suggested to upgrade with proxy server or personal firewall software. |
| Internet Router with personal firewall software installed in each workstation | Internet Gateway using Router | Outbound only Gateway | Hackers may attack those workstations or servers that are not protected by any firewall software. Too many personal firewall packages within a network may introduce support problems, it is suggested to have a centralized control (e.g. by means of a proxy server). |
| Internet Router with workstations and caching server behind it | Proper use of Proxy Server | Outbound only Gateway | The external router should define rule sets to redirect all messages to the caching server only; the caching servers should be configured to prohibit external hosts from using their proxy service. For better protection, it is suggested to upgrade to a screened multi-homed proxy solution. |
| Multi-homed proxy system with WAN port connecting to the Internet directly | Proper use of Proxy Server | Outbound only Gateway | Both circuit level packet filtering and application level messages controls are provided by the same server. May upgrade to a screened multi-homed proxy solution. |
| Screened multi-homed proxy solution | Proper use of Proxy Server | Outbound only Gateway | The screening router will be responsible for circuit level packet filtering while the proxy server will be responsible for application level message control. The solution provides better Internet security protection to the internal network. |
| A screened sub-network using multiple routers sandwiching a DMZ | Screened Sub-network Gateway by multiple routers | Gateway with Public Services | Good for large organizations with mission critical applications running on it. Complicated and hard to support. Not suitable to schools, hard to support and maintain. |
| Hardware Firewall with proxy server in DMZ | Integrated solution of Firewall | Gateway with Public Services | Suitable for most schools; Easy to maintain. |
| Software Firewall with proxy server in DMZ | Integrated solution of Firewall | Gateway with Public Services | Suitable for schools but require strong technical supporting skill sets. |