

**Information Technology in Education Project**

# **A Closer Look at Internet Firewalls**

**Quality Education Division  
Education and Manpower Bureau  
The Government of the HKSAR**  
[www.emb.gov.hk/ited/](http://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 website at <http://www.emb.gov.hk/ited/>

## A closer look at Internet firewalls

**F**irewall has become an important component in every computer network with Internet access. It is always a myth that after installing a firewall, the internal network will be safe and free from hacker attacks. However, user should bear in mind that firewall provides a certain level of security only if it is properly installed, configured, and ongoing maintained and appropriate tuning to combat new forms of attacks.

A firewall allows the administrator to define/set certain rules to determine what traffic should be allowed in or out of the internal network. Depending on the type of firewall implemented, administrator can restrict user(s) to access to certain IP addresses or domain names, or can block certain types of traffic by blocking the TCP/IP ports to be accessed.

### How do firewalls work?

Firewalls are used to monitor traffic and block any user-defined activity (usually referred to as inappropriate activity). There are two major ways to do this - at the network layer and/or at the application layer.

The network layer firewalls look at packets and check their source and destination IP addresses and TCP ports numbers. The header information in each packet will be used to decide whether the packet is allowed to pass through or not.

Application layer firewalls view information as a data stream and not as a series of packets. In this way, the firewalls scan information passing over them and then decide whether the information is acceptable or not as defined by a set of policies. The application layer firewalls generally are hosts running proxy servers, which do not allow direct traffic between the external and the internal networks. When there is a request from the external network, the firewall "pretends" to be the application server and checks the traffic against its own set of rules. If the information is acceptable, the conversation is then conducted with the real application.

---

#### **About this document:**

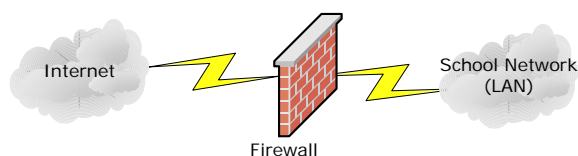
*This document gives you a closer look at the ways firewalls function and how they protect your networks. It also introduces some popular security functions that will be included in the firewalls.*

*After reading this document, readers should be able to distinguish some major features of a firewall and evaluate which features are necessary to their schools.*

---

### What is a firewall?

A firewall is basically the first line of defense for your network. It prevents uninvited guests from browsing your network. A firewall can be a hardware device, a server with firewall software running on it, or a combined system of the above devices. It is usually placed at the perimeter of the network to act as the gatekeeper to monitor all incoming and outgoing traffic.



### Network Layer Firewall - Packet Filtering

#### Static Packet Filtering

One of the simplest and least expensive forms of firewall protection is static packet

filtering. With static packet filtering, each packet entering and leaving the network is checked. The information on the header fields like the source/destination IP addresses and ports, protocol type and TCP flags is checked to determine which packet is allowed or disallowed.

For example, port 25 is the Internet standard for sending SMTP mail which is the channel used for communication between a mail client and a mail server. All e-mail sent via the Internet should be routed through the port 25. In order to allow email to and from an SMTP server, the administrator should set the firewall to allow all network traffic with a TCP source and destination port of 25 (SMTP) and the IP address of the mail server (as either the source or destination IP address). If this is the only rule applied, all non-SMTP network traffic originating from outside the firewall with a destination IP address of the mail server will be blocked by the firewall.

These static packet filtering firewalls do not look into the content for malicious intent and they treat each packet as an individual entity. Border routers are good static packet filters and are the schools the first line of defense. They are convenient, fast, and, in most cases, inexpensive.

However, static packet filtering firewalls are susceptible to IP spoofing, i.e. the intruder tries to gain unauthorized access to computers by sending messages to a computer with an IP address indicating that the message is coming from a trusted host. Another problem of this firewall is that it

rarely provides sufficient logging and reporting capabilities.

### Stateful packet filtering

The stateful packet filtering firewall is a more sophisticated firewall as it has a notion of state. The stateful packet filtering firewall examines the contents of packets rather than just filtering them; i.e. it checks their contents as well as their addresses.

The stateful packet filtering firewall compares certain key parts of the packet to a database of trusted information. Information traveling from the internal network to the external is monitored for specific defining characteristics. The incoming information is being compared with the characteristics. If the comparison yields a reasonable match, the information is allowed through. Otherwise, it is discarded.

For example, a legitimate incoming packet will be allowed if it matches the outbound request for that packet. Conversely, an incoming packet masquerading as a response to a non-existent outbound request will also be blocked.

By using something known as session or intelligent filtering, most stateful packet filtering firewalls can effectively track information about the beginning and end of network sessions to dynamically control filtering decisions. The filter uses smart

#### *Static Packet Filtering*

Static packet filters are widely used by most routers to filter packets based on information contained in every individual packet. Filters can theoretically be configured to determine based on any part of the protocol header, but most common filters are based on the following header information:

**Protocol Type filtering** filters packets based on IP protocol such as UDP, TCP, ICMP and IGMP. Since it can filter only four common protocols available, normally it is leaving them all opened.

**IP Address filtering** is the strongest form of security in static packet filter technique. It limits connections to specific hosts and network based on IP address. However, hackers may still hack the site by using an acceptable forged IP address to pass through the router and hijacked the return packets.

**TCP/UDP Ports filtering** is commonly used for filtering application, such as Daytime, DNS, Echo, HTTP, Quote, Gopher, FTP, POP, Telnet, SNMP, SMTP, NNTP, NetBIOS Session, IMAP, NFS, Whois and RSH.

rules, and thus enhancing the filtering process and controlling the network session rather than controlling the individual packets.

Stateful packet filtering firewall offers improved security and better logging of activities over static packet filters. However, like static packet filtering firewall, this approach also allows a direct connection between endpoints through the firewall. Besides, setting up stateful packet examination rules is a more complicated process.

## Application Layer Firewall - Proxy service

Known as application proxy or gateway firewall, application layer firewall uses software to intercept connections for each Internet protocol and to perform security inspection. It involves what is commonly known as proxy services. The proxy acts as a middleman which re-addresses traffic so that outgoing traffic appears to have originated from the firewall, rather than the internal host.

The primary advantage of application proxy is that no direct connection is allowed through the firewall under any circumstances. All connections from internal clients to the Internet or vice versa must go through the application proxy.

The application proxy has full visibility at the application layer. It can look for more specific pieces of information than a packet filter. For instance, it can tell the differences between a piece of email containing text and a piece of email containing a Microsoft Word document, or the difference between a Web page using Java and a Web page without Java. Rules can be made significantly more specific, as they can be designed based upon anything the application proxy can see at the application level. In addition, the application proxy can offer the best logging and reporting activities.

As can be imagined, the greatest drawback of using this technique is the sacrifice in speed. Since all traffic has to be inspected

at the application level, the performance of the application proxy will have a much more significant drop than using the packet filtering alternatives.

Another drawback is that, to utilize the application proxy, a protocol must have a proxy associated with it. Failure to have a proxy may prevent a protocol from being handled correctly by the firewall that potentially will be discarded.

## Other firewall functions

Since firewall should be the only gateway for Internet access for an organization like school, it is common that some other security functions should be installed, including:

- ◆ Content Filtering;
- ◆ Demilitarized Zone (DMZ);
- ◆ Virtual Private Networking (VPN); and
- ◆ Intrusion Detection System (IDS).

### Content Filtering

Content filtering is the use of a program to screen and forbid access to or the availability of certain Web pages or e-mails that are deemed objectionable. Content filtering usually works by specifying character strings that, if matched, represents undesirable content that is to be screened out. Contents typically to be screened are pornographic content and sometimes violence- or hate-oriented content. Critics of using content filtering programs are that some desirable content may also be unintentionally excluded.

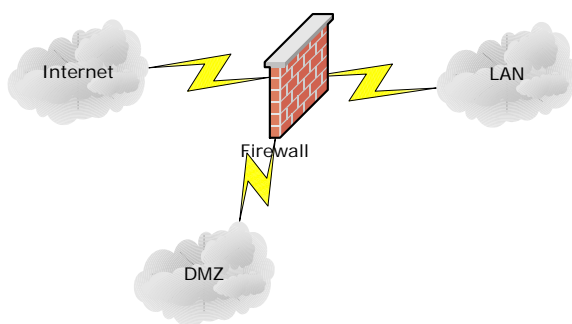
### Demilitarized Zone

There are times that administrator may allow remote or public users to have access to items on the school network. Examples include:

- ◆ Web browsing
- ◆ e-mail

◆ file transfer

In cases like these, administrator may need to create a **Demilitarized Zone (DMZ)**. DMZ is a network added between the internal protected network (LAN) and the external network (Internet), which provides an additional layer of security to the internal network. DMZ separates the external network from directly referencing any hosts in the internal network. It does this by isolating the machine to be directly accessible by all other machines.



If there is no DMZ and the initial frontline perimeter is broken, then the whole school network would be subject to being hacked. Besides, there are often new bugs found in the software. Even if user has hardened the operating system and has installed a firewall to protect the network, there is still

the possibility that the software bug may allow attacker to exploit all the information stored in these systems.

The present of the DMZ gives further protection to the internal network by hiding the important information an extra step away from an attacker. It is easy for the attacker to enter the internal network through the web server. We should separate information so that attackers cannot get to all the systems. This is the type of problem that a DMZ is designed to prevent.

### Virtual Private Network

A virtual private network uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection such as leased line, a VPN uses "virtual" connections route through the Internet to connect the school's private internal network with the remote external users. VPN allows users from the Internet to pass through the firewall and logon to the school network as if they are working inside the campus.

For more details on using VPN for remote access in schools, please refer to "Remote Access – Virtual Private Network" at:

<http://www.emb.gov.hk/index.aspx?langno=1&nodeID=4797>

## Intrusion Detection System (IDS)

Intrusion detection is the process of monitoring events occurring in a computer system or network and analyzing them for signs of intrusions which are attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer or network.

IDS works very much similar to a smoke detector in the office. Smoke detector detects smoke that may lead to a fire. It gives alarms whenever it senses smoke; no matter the smoke comes from a cigarette or a real fire.

In reality, it is extremely difficult to achieve 100% fault-free intrusion detection. Most firewalls with IDS may detect common intrusion activities like port-scan attack, IP half scan attack, Land attack, UDP bomb attack, and Ping of death attack. For other attacks, IDS may either generate a lot of false alarms or miss the real attacks.

But anyway, like smoke detector, it will be completely meaningless if IDS alarms but nobody responds. Thus, monitoring is a very important issue to firewall having IDS.

## Firewall best practices

Firewalls are not the end-all, be-all solution to information security. They are, however, a necessary component of an effective information technology infrastructure. The following are the best practices, in no particular order, that user should consider to ensure that the firewall is configured for optimal performance and effectiveness.

- ◆ Deny all traffic by default, and only enable those services that are needed.
- ◆ Disable or uninstall any unnecessary services and software in the firewall system that are not specifically required.
- ◆ Limit the number of applications that run on the firewall in order to let the firewall do what it is best at doing.

### **Common intrusion detection approaches:**

There are two complementary approaches to detecting intrusions, knowledge-based approaches and behavior-based approaches.

#### **Knowledge-based IDS**

Knowledge-based IDS apply the knowledge accumulated about specific attacks and system vulnerabilities. The IDS contains information about these vulnerabilities and looks for attempts to exploit these vulnerabilities. When such an attempt is detected, an alarm is triggered. In other words, any action that is not explicitly recognized as an attack is considered acceptable. Therefore, the accuracy of knowledge-based IDS is considered good. However, their completeness (i.e. the fact that they detect all possible attacks) depends on the regular update of knowledge about attacks. IDS products available in the market today mostly use knowledge-based detection.

#### **Behavior-based IDS**

Behavior-based IDS assume that an intrusion can be detected by observing a deviation from normal or expected behavior of the system or the users. The model of normal or valid behavior is extracted from reference information collected by various means. The intrusion detection system later compares this model with the current activity. When a deviation is observed, an alarm is generated. In other words, anything that does not correspond to a previously learned behavior is considered intrusive. The advantage of behavior-based detection is that it can detect previously unknown attacks and insider attacks, without the need for knowledge. It is also impossible for the attacker to know what activity generates an alarm and so they cannot assume that any particular action will go undetected. Therefore, the intrusion detection system might be complete (i.e. all attacks should be caught), but its accuracy is a difficult issue (i.e. you get a lot of false alarms). The disadvantage of this approach is in the large number of false positives – alerts that are generated due to legitimate activity.

Consider running anti-virus, content filtering, VPN, DHCP and authentication software on other dedicated systems behind the firewall.

- ◆ If possible, run the firewall service with a unique user ID instead of administrator.

- ◆ Change the default administrator password of the firewall or the underlying operating system.
- ◆ Do not rely on packet filtering alone. Use stateful packet filtering and proxies if possible.
- ◆ If a malicious user can obtain physical access to the firewall, anything can happen. Ensure that physical access to the firewall is controlled.
- ◆ Keep your firewall configuration as simple as possible, and eliminate unneeded or redundant rules to ensure that the firewall is configured to support your specific needs.
- ◆ Make sure that the security rule set on the firewall remains consistent with the school IT security policy.
- ◆ Run the firewall on a hardened and routinely patched operating system. An insecure and non-hardened operating system can render the firewall completely useless.
- ◆ If possible, use a firewall in conjunction with a router when connecting to the Internet to help prevent denial-of-service attacks and successful penetrations.
- ◆ Enable firewall logging and alerting if possible.
- ◆ Regularly monitor the firewall logs.
- ◆ Note any firewall log entries that do not look right, and investigate them immediately.
- ◆ Periodically backup the firewall logs (preferably onto write-once media such as CD-R) and store them for future reference and/or legal protection in the case of an intrusion that must be investigated.
- ◆ Use change-management practices for the firewall to approve changes needed, assess the reason(s) for the changes, document the changes made and describe the necessary

back-out procedures in case the changes fail.

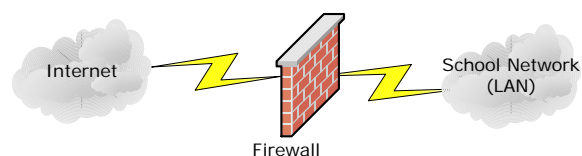
- ◆ Perform ongoing audits, at least yearly, on the firewall to compare what you say you are doing in your security policy with what is actually being done.
- ◆ Constantly monitor (or subscribe to) your firewall vendor's security bulletins.
- ◆ Regularly backup the firewall configuration files, and keep the backups in a safe place.

## Practical firewall topology

The firewall functions described above can be deployed in a wide variety of ways. The followings are some commonly deployed architecture and they are presented in the order of increasing effectiveness:

### Basic border firewall

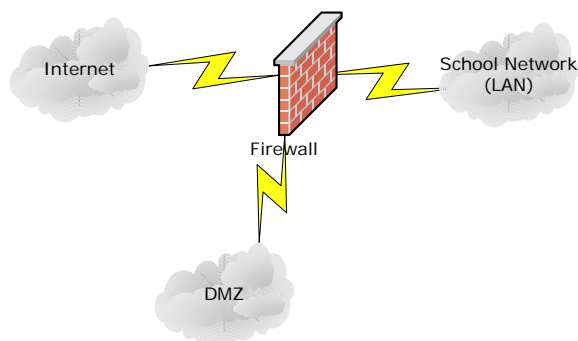
This is the starting point for all firewalls. A basic border firewall is a single host interconnecting a school's internal network and the untrusted external network, typically the Internet. In this configuration, the single host provides all firewall functions.



### DMZ network

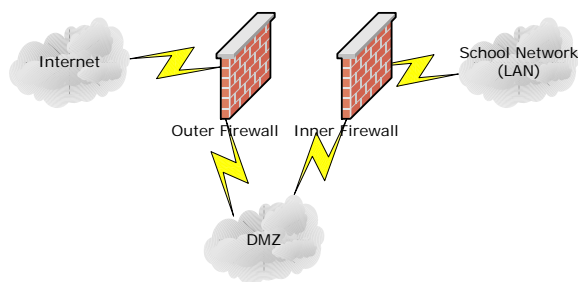
In a DMZ network, the untrusted host is brought "inside" the firewall, but placed on a network by itself (the firewall host interconnects three networks). This increases the security, reliability, and availability of the untrusted host, but it does not increase the level of trust that other "inside" hosts can afford to have. Other untrustworthy hosts for other purposes (for example, a public web site or

ftp server) can be placed on the DMZ network, offering a public services network.



### Dual firewall

The school's internal network is further isolated from the untrustworthy network by adding a second firewall host. By connecting the untrustworthy network to one firewall host, the school's internal network to the others, and the DMZ in between, traffic between the internal network and the Internet must traverse the two firewalls and the DMZ.



## Summary

Firewall is a piece of equipment or a combined system of devices to separate an untrusted network (external network, usually the Internet) from a trusted network (internal network). The level of protection required for a firewall varies among schools. It is very much depends on what assets to be protected and their respective security requirements.

Schools are advised to conduct a thorough risk analysis and formulate their own it security policy before implementing any firewall. In general, for schools with outbound Internet access only, a well-configured basic border firewall should be good enough to fulfill the security requirement.

For schools with public accessible servers, they should deploy firewall with DMZ, or considered to sandwich these public accessible servers between external and internal firewalls.

Finally, schools are reminded that implementation of any IT security project is never a one-off exercise. Continuous monitoring and tuning of the implemented system is necessary to achieve the best result.