Firewall

A newsletter for IT Professionals

Issue 7

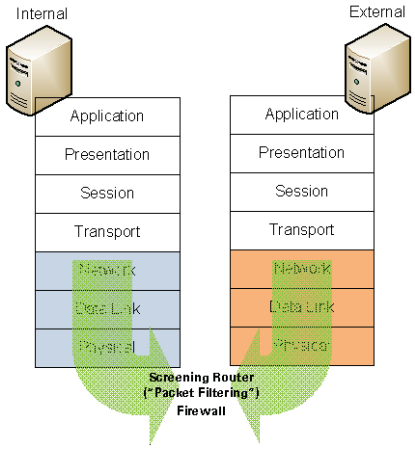
I. Background of Firewall

Any device that controls network traffic for security reasons can be called a firewall. It puts up a barrier that controls the flow of traffic between networks and is able to protect the boundary of a university's internal network whilst it is connected to other networks (e.g. the Internet, third-parties' private networks).

The safest firewall would block all traffic, but that defeats the purpose of making the connection. Therefore, the key function of a firewall is to strictly control selected traffic in a secured manner.

There are three major types of firewalls that use different strategies for protecting internal networks from external or internal threats.

Screening Router



Also known as "Packet Filters", the Screening Router is the first generation of firewall devices built on network routers and operate in first three levels of OSI reference model. The device checks for matches to any of the packet filtering rules pre-configured, and drops or rejects the packet accordingly.

Network administrators are required to define a set of rules to instruct the Screening Routers to filter out packets. As most of the applications communicate over the Internet today uses well know ports for particular type of traffic, such as 80 for HTTP and 20 for FTP, the Screening Routers can easily distinguish between, and thus control, those types of traffics unless non-standard ports are used.

The major weakness of Screening Routers is its "stateless" nature – no information on the connection state is examined. Instead, only the low-level information contained in the packet itself will be filtered, such as source/destination address, protocol types, port numbers, etc.

Reference:
http://www.windowsecurity.com/whitepapers/General_Firewall_White_Paper.html
http://www.windowsecurity.com/articles/A_firewall_in_an_IT_system.html

I. Background of Firewall (cont'd)

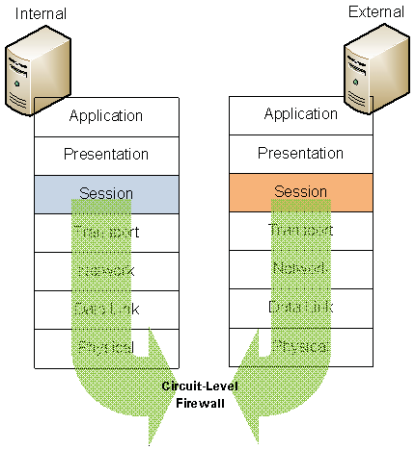
Proxy Server Firewall

A Proxy Server Firewall operates at the upper levels of the OSI protocol stack (i.e. all the way up to the application layer) and provides internal terminals with proxy services to external networks. Messages from internal terminals are relayed by the Proxy Server Firewall to external destinations. A major benefit of deploying Proxy Server Firewalls is that they are able to hide the internal network information or structure through changing the IP addresses of outgoing packets.

Furthermore, Proxy Server Firewalls is able to look at more detailed information inside the packets, which enables more sophisticated monitoring and control of traffic fows at the network boundary. However, degradation of performance and reduction in the transparency of access to other networks are the possible by-products of using Proxy Server Firewalls.

There are two types of Proxy Server Firewalls:

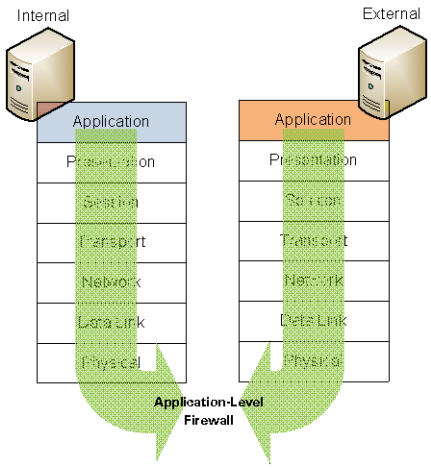
- **Circuit-Level Firewall**



A Circuit-Level Firewall works at the session layer of the OSI model. They monitor TCP handshaking between the packets to determine if a requested session is legitimate.

A virtual "circuit" is established between the internal terminals and the proxy server. "Network Address Translation" technique is used, where requests from the external networks go through this "circuit" to the proxy server, and the proxy server relays those requests to the external networks after changing the IP addresses of the packets. All packets delivered by the Circuit-Level Firewall are tagged with public IP addresses and the internal private IP addresses are not exposed to potential intruders. There is no way for a remote terminal to determine the internal private IP addresses of the universities.

- **Application-Level Firewall**



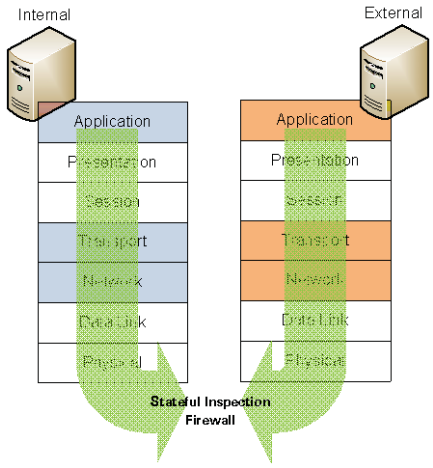
An Application-Level firewall provides all the Circuit-Level firewall features and also provides extensive packet analysis.

Not only does the firewall evaluate IP addresses, it decides whether to drop a packet or send them through based on the application information available in the packet, which stops hackers from hiding information in the packets. Such function is achieved via setting up multiple proxies on a single firewall for difference applications, and examines the data or connection at Application Layer based on tailor-made rule(s) for each application. Because they are application aware, more complex protocols like H.323, SIP and SQL can be handled.

Reference:
http://www.windowsecurity.com/whitepapers/General_Firewall_White_Paper.html
http://www.windowsecurity.com/articles/A_firewall_in_an_IT_system.html

I. Background of Firewall (cont'd)

Stateful Inspection Firewall



Being the third generation of firewall architecture, Stateful Inspection Firewalls work at multiple layers of OSI reference model, including Network Layer, Transport Layers and Application Layers, and is also known as "Dynamic Packet Filtering" firewalls.

A Stateful Inspection Firewalls monitor the state of active connections, analyses the traffic patterns down to the Application Layer and detects abnormalities based on the analysis results. For illustration, incoming and outgoing packets are monitored over a period of time by the Stateful Inspection Firewall. Outgoing packets that request specific types of incoming packets are tracked and only those incoming packets constituting a proper response are allowed to pass through the firewall.

The dynamic feature of Stateful Inspection Firewall enables more accurate filtering of packets by considering the context of the traffic. However, some Stateful Inspection Firewalls are implemented to allow direct connection between internal and external terminals as they rely on algorithms to recognise and process application layer data instead of relying on proxies, thus exposing internal IP addresses to potential hackers. Some firewall vendor incorporate stateful inspection and server proxy techniques together for added security

Key Benefits Achieved through Firewall

- **Inbound and Outbound Filtering** – Traffic filtering is the primary and most important function of a firewall. Inbound filtering processes inbound data towards the internal IT environment of the university and rejects any unsecured / malicious content. Outbound filtering can prevent the spread of malware originated from internal hosts and terminates certain types of communication prohibited by the university's information security policy. E.g. Peer-to-Peer, Streaming, etc. This function can also be modified to allow certain external terminals to reach the internal network or for certain data to be released to the external networks.
- **Stealth Mode** – Firewalls not only block unauthorised requests to the information systems or personal computers within the university, but also avoid sending responses to probing activities committed by hackers, making them in "Stealth Mode" and reducing the exposure to further malicious attacks.
- **Privacy and Sensitive Data Protection** – Many firewalls now have the ability to block spyware, hijackers, and adware from reaching the university's internal terminals. It prevents authorised leakage of private data or sensitive information of the university and its members
- **Intrusion Detection** – Firewalls can detect various intrusion activities via scanning incoming data for signatures of known method, record any suspicious events and notify users when such attacks are recognised. Firewall notifications and logs allow users or IT security staff of the university to timely detect any possible penetration attempts on the university's information systems and resources and prepare corresponding mitigating measures.

Reference:
http://windowsupdate.microsoft.com/
http://www.windowsecurity.com/articles/A_firewall_in_an_IT_system.html
http://www.bleepingcomputer.com/tutorials/tutorial60.html

II. Risk of Firewall in Universities

Firewalls are one of the most critical devices or applications that protect universities' information systems and resources from unauthorised access or malicious attacks. To effectively utilise the security features of firewalls, accurate configuration and maintenance of rules shall be made by universities' network administrators and IT security staff in accordance with the Information Security Policy and any other applicable security standards (e.g. Acceptable Usage Standard). Inappropriate management of firewall systems may result in security flaws and risks that are unaware by the universities. Some examples are illustrated below.

- **Default or Improper Configurations**

  Most off-the-shelf firewall products are pre-set with default administrator login names and passwords. If they are not changed before being deployed into universities' networks, hackers may easily gain privileged access to firewalls by trying the default passwords used by popular vendors. If succeeded, hackers can modify the rule configuration and allow attacks to pass through the firewalls without notice.

  Rely on default or improper firewall configuration would impose vulnerabilities on the access security as well as the effectiveness of traffic filtering function within the firewalls. As each university has its unique design of information systems and network infrastructure, firewalls may not be able to detect malicious packets or prohibited communication if the configuration is not tailor-made based on the IT security policy, procedures or standards.

- **Hardware or Software Failure**

  Firewall software or hardware is subject to accidental malfunction, deliberate sabotage or compromise. Without proper monitoring of firewall operation status by the IT operations team, such failures may go undetected for a prolonged period of time and create great exposures to both external and internal threats that harm universities' information security.

- **Insecure Communication with Firewalls**

  In general, management of firewall configurations is performed remotely. If weak and insecure protocols are used in communication, firewall servers and applications are then vulnerable to various known exploitations that aim to compromise the communication channels and subsequently launch malicious attacks against the universities.

Reference:
http://www.ogf.org/documents/GFD.83.pdf

III. Risk of Firewall in Universities (cont'd)

- **Conflict with Other Applications**

  Almost all applications with communication capabilities are created with the thought that there is no firewall in place. Moreover, the information on protocols and port numbers used by some applications are not available until they are executed. As a result, using a firewall may sometimes make certain features of the applications no longer work properly. In worse cases, the incompatibilities could result in service interruption or even loss of data.

- **Improper Change Management**

  When universities update their information security policy, procedures or standards, corresponding changes (if any) shall be made to the firewalls. Without undergoing the change process in a controlled manner, incorrect updates could be implemented, which prevents firewalls from complying with the information security requirement. Moreover, unexpected security and performance issues may arise if obsolete firewall rules are not timely removed.

Related Article

Keep Your Firewall Rulebase in Shape

Firewall rule which if unmanaged can leave gaping security holes, performance degradation and management issues. Firewall rules are born and modified as a result of access requests from users or IT projects. And over time, they become irrelevant – because applications, services and networks change, and users leave.

These unused or "stale" rules are a hidden menace to your firewall policy rulebase. First of all, they slow down performance – since the firewall has to scan all of the rules from the top for every traffic request. Second, they are a threat to security – they may leave access open to an unwanted visitor. And finally, they are a blow to manageability. Just like the firewall, you too need to go through the whole list of rules each time you handle a change request.

See the article: (http://www.securitypark.co.uk/security_article265832.html)

Reference:
http://www.ogf.org/documents/GFD.83.pdf

III. Exploitations on Firewall

Like universities' other information systems, desktops or networks, firewalls are computing devices/applications and also have vulnerabilities exposed to certain type of exploitations. Some major firewall exploitations are described here:

1 Information Gathering

Port Scanning is one of the most popular techniques attackers use to discover services they can break into. All terminals connected to a Local Area Network (LAN) or the Internet run many services that listen at well-known and not so well-known ports. A port scan helps the attacker find which ports are accessible through the firewall. Common port scanning techniques include:

- **SYN Scan** – Initiate a half TCP connection by sending SYN packets and waiting for SYN + ACK packets to indicate active hosts.
- **Fragmented packet Port Scan** – Splitting the TCP header into several IP fragments in order to bypasses some packet filter firewalls because they cannot see a complete TCP header that can match their filter rules.
- **Fingerprinting** – Sending unusual combination of data and interpreting the responses of a system in order to figure out what it is.

2 Denial of Service ("DoS") Attack

DoS attacks are based on packet flooding, which uses up bandwidth, CPU, and memory resources on not just the victim device, but also intervening devices, such as routers, switches, and firewalls. One of the most common DoS attacks is the Smurf attack. In a Smurf attack, the attacker sends a flood of ICMP messages to a reflector or sets of reflectors, with the source IP address in the ICMP echo messages spoofed. The hacker changes these addresses to the address of the target firewall devices and causes flood attack on them, which overwhelm the firewalls so that they cannot function properly.

3 Buffer Overflow Attack

Buffer overflow is an abnormal behaviour where a program, while writing data to a buffer, overruns the buffer's boundary and overwrites adjacent memory. Successful exploitations using buffer overflow are resulted from vulnerabilities inside application programs. Certain types of firewalls are known to have such vulnerabilities that may be exploited by hackers. For example, the java services running on port 3858 on a SunOS machine used by SunScreen Firewall as remote administration protocol were found to contain numerous buffer overflows. If hackers managed to exploit these vulnerabilities, it is possible to execute arbitrary code on that machine.

Reference:
http://www.auditmypc.com/port-scanning.asp
http://nmap.org/book/man-bypass-firewalls-ids.html
http://www.informit.com/articles/article.aspx?p=345618#
http://www.exploit-db.com/exploits/16041/

IV. Hardening Steps for Firewall

Firewalls are part of the IT environment of universities and shall be secured in accordance with the universities' Information Security Policies and relevant industrial standards. Hardening steps for the firewall systems are recommended to focus on "Access Security" and "System Security".

Access Security

- **User authentication**

  The use of a centralised authentication, authorisation and account mechanism is recommended for the user authentication on firewalls. User specific accounts are implemented and maintained in a general directory. Only one local account should be configured on the firewall as a backup account when the central authentication mechanism is not available.

  RADIUS or TACACS(+) are the examples of a common centralised authentication, authorisation and accounting mechanism. For instance, in the configuration of a Cisco PIX firewall, the firewall can be configured to define remote AAA servers by a configuration similar to:

  aaa-server TACACS+ protocol tacacs+
  aaa-server TACACS+ host 10.0.0.2 secret123
  aaa-server TACACS+ host 10.0.0.3 321terces
  aaa-server TACACS+ max-failed-attempts 3
  aaa-server TACACS+ deadtime 5
  aaa-server TACACS+ timeout 5
  aaa-server RADIUS protocol radius
  aaa-server RADIUS host 10.0.1.2 secret123
  aaa-server RADIUS max-failed-attempts 3
  aaa-server RADIUS deadtime 5
  aaa-server RADIUS timeout 5
  aaa-server LOCAL protocol local

  The administrator user accounts on the firewall can be authenticated by using either an internal user database or an external user database.

- **Management Traffic**

  A secure connection should be established for the management of firewalls. This can be configured in several ways.

  For Checkpoint firewalls, each administrator can be created a certificate to enforce symmetric authentication. IP restriction on management traffic can also be set up by enforcing a firewall rule in the management console.

  For Cisco PIX firewalls or NetScreen firewalls, Telnet access can be disabled and SSH can be selected for in-band management connections.

Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_installation_and_configuration_guides_list.html
http://www.juniper.net/techpubs/software/screenos/screenos6.0.0/
http://www.checkpoint.com/support/technical/documents/

IV. Hardening Steps for Firewall (cont'd)

System Security

- **Generic Device Security**

  The same level of attention to the management traffic should be paid to the general traffic of the firewall.

  Unless the ports explicitly needed for connection to other devices, the console and auxiliary ports should be disabled. Otherwise, these ports can be used by unauthorised users for managing the device through a direct connection to the console or modem port.

- **Traffic Filtering**

  The actual traffic filtering that a firewall should perform is configured through use of policies. The appropriate rules should be configured matching the traffic filtering policy. A policy is a set of rules that determines how traffic passes between security zones (inter-zone policy), between interfaces bound to the same zone (intra-zone policy), and between addresses in the Global zone (global policy). When a security device attempts to pass a packet from one zone to another, between two interfaces bound to the same zone, or between two addresses in the Global zone, the security device checks its policy lists for a policy to permit or reject such traffic.

- **Logging**

  Firewalls should send its logs to a central server and have detailed logging options.

  For example, on a Cisco PIX firewall, logging is recommended to be sent through use of AAA by applying a configuration as follows:

  "*aaa accounting authentication enable console*"

  This command causes syslog messages to be sent (at syslog level 4) each time the configuration is changed from the serial console.

  To log firewall rules in a Checkpoint firewall, this can be configured by entering a configuration in the SmartCenter management console as follows:

  - For each of the Security Policy rules you wish to track, right click in the Track column and choose Log from the menu. All events matching these rules are now logged.
  - Launch SmartView Tracker through the SmartDashboard's Window menu. The Log mode is displayed, showing the records of all events you have logged.

  Which rules are logged depends on the firewall policy. However, one rule that most likely should always be logged is the "*deny any any*".

Reference:
http://www.cisco.com/en/US/products/sw/secursw/ps2120/products_installation_and_configuration_guides_list.html
http://www.juniper.net/techpubs/software/screenos/screenos6.0.0/
http://www.checkpoint.com/support/technical/documents/

V. Summary

Implementing firewalls within the universities' networks is a necessary means to protect their information systems and resources from malicious activities initiated by hackers, malware or viruses.

While enjoying the security benefit brought by the firewalls, universities should also pay close attention to their weakness and associated risks, which, if exploited, would leave the entire IT environment vulnerable to external threats.

To effectively block unauthorised attempts from external networks using firewalls, it is important to maintain proper configuration of the rule sets in the firewalls based on universities' information security policy and industry best practices, as well as enforce strict protection on the firewall systems.