Bachelor's thesis

Degree Programming in Information Technology

2011

Chen Yiping

FIREWALL DEPLOYMENT AND CONFIGURATION

– A case study

TURUN AMMATTIKORKEAKOULU
TURKU UNIVERSITY OF APPLIED SCIENCES

BACHELOR'S THESIS | ABSTRACT

TURKU UNIVERSITY OF APPLIED SCIENCES

Degree Programme | Information Technology

9.5.2011 | 41

Instructor: Wikström Yngvar

ABSTRACT

Firewall and intrusion detection technology play a crucial role in network security. The objective of this thesis is to apply firewall and intrusion detection technology in a real environment, especially in a commercial area and introduce some basic methods to test a firewall of a network system operation successfully.

This thesis, at first, elaborates on the importance of firewall in network application, then it explains some firewall concepts and the related technology theory. After that, it also covers some applied firewall topologies and configuration instructions. In the end, the author gives an example based on his own work experience in Changsha Xiangtie Network Ltd.

All in all, this thesis is supposed to offer a way to expand the scope of network protection and reduce the probability of network attacks and make a company network much safer than before.

Key Words:

Network security, firewall, intrusion detection, VPN

FOREWORDS

This part makes some introduction about my Changsha Xiangtie Network Ltd. I worked in this company during August 2009.

Changsha Xiangtie Network Ltd is a high-tech located in the Changsha Hunan Province China.

Since company was built in 2006, the CEO has been concerned about the company's management and has established network personnel-management. Not only is network technology applied in the personnel department, but it is also related to the sales, service and financial department.

There are some talented sales managers and technicians working in this company. Some of them receive certificates including TCL, Datwyler, Cisco, Intel and Lenovo. Not only do they have theoretical knowledge in network technology, but they also have passion for work.

Xiangtie Network Ltd has technical cooperation with well-known companies, such as Lenovo, HP, Dell, which allows it to stand in front of high-tech development. It can provide the newest technology and best plans for a large number of customers.

I really appreciate Wang Xiaojun, the CEO of Xiangtie Network Ltd, for offering me this opportunity to study.

22.5.2011

Chen Yiping

Table of contents

FIREWALL DEPLOYMENT AND CONFIGURATION **0**
ABSTRACT **1**
FOREWARD **1**
1.INTRODUCTION **1**
2.BACKGROUND **2**
2.1.Firewall Technology 2
2.2.Intrusion detection technology 3
3.FIREWALL'S THEORY AND STRUCTURE **6**
3.1.The firewall concept 6
3.2.Firewall components 7
3.3.Technical Theory 10
3.4.Firewall structure 13
4. FIREWALL INSTALLATION AND CONFIGURATION INSTRUCTION **15**
4.1.Firewall selection 15
4.2.Firewall deployment 16
4.3.Firewall configuration instruction 18
5. FIREWALL-TESTED TECHNOLOGY **23**
6. INTRUSION DETECTION IN A FIREWALL **25**
7.CONFIGURATION SAMPLE **30**
7.1.Introduction of project 30
7.2.Work process (Web anti-modified system) 31
7.3.Configuration information (firewall) 34
8. DISCUSSION **37**
9. SUMMARY **38**
REFERENCES **39**
APPENDIX ONE **41**

1. INTRODUCTION

With network applications becoming more popular and complex, the number of network security incidents constantly rises. When a local area network connects to the Internet, top-secret data and network equipment would be exposed to Internet. In order to provide different ranks of network protection, network managers have to follow network-configured environment and safety requests to make related strategies in case that unauthorized guests break into the inner network and trace crucial data.

Most of the sources in the Internet instruct people how to configure one simple function on firewall instead of complete guidelines. Published theses are either focused on home users or a specific company’s problems.

Therefore, some theories about firewall and intrusion detection technologies are explained and make a instruction which guides people to construct a firewall and configure some basic functions.

The main goals for this thesis are to introduce principles for firewalls' selection, how to configure and how to detect intrusion.

As a network manager in a network company called Changsha Xiatie Network Ltd. During the work placement period, constructing firewalls for education department of Hunan Province has been witnessed.

The most important part of the thesis is the final chapter including common configuration instructions for firewall which are based on work experience.

2. BACKGROUND

At present, a large number of experts like Marcus Goncalves prefer to introduce network functions mostly based on network structure and hardware configuration. In this thesis, technologies, like firewall technology and intrusion detection technology have been considered in this LAN security strategy for company use. There will be some introductions about these technology development situations as follows.

2.1 Firewall Technology

The term "firewall" that was used for the first time in 1764 to describe walls that separate some parts of a building mostly kitchens from the rest of a structure. These physical barriers slowed down a fire's spread throughout the whole building in order to protect the owners' lives and properties. Although firewall operation on network is not capable of protecting people's lives, it is still essential for protecting network sources from attacks. The first firewall for network security dates as early as in the late 1980s and was used to separate networks from each other. The first-generation firewalls being used were implemented almost at the same time as the routers being introduced. They were capable of packet filtering. In 1989, the second-generation firewalls (also called application layer firewall) and the third-generation firewalls (also called circuit level firewall) were developed by Dave Presotto and Howard Trickey from AT&T Bell laboratories. Those generation firewalls can "understand" some specific protocols, such as DNS (Domain Name System) and web browsing, record information of each connection and determine a data packet's function in transmission. In 1992, Bob Braden developed the fourth-generation firewall based on the new technology of dynamic packet filter. An Israeli company called Check Point Software Technologies built this into new technology called stateful packet inspection. In the meantime, this technology was applied in commercial products. The fifth-generation firewalls were developed in 1998 by NAI global (the world's leading managed network of more than 300 commercial real estate firms), It was a new technology called adaptive proxy and operated in related products like Gauntlet Firewall for NT. [1]

Firewall technology has been widely used in Europe and America. Some representative firewall products are for instance the Nokia IP650 Firewall, the Check Point Firewall-1, the Symantec AXENT VelociRaptor Firewall, the Watch Guard Firewall the II-Plus Firewall and the Cyberguard KnightSTAR Firewall. Those firewalls have quite complete functions and advanced technology. However, configuring firewall technology does not imply that we make a great effort to accomplishing once and the network managers can take rest in the future. Along with high-speed development of hackers' attack technology, firewall technology has to be improved to meet the requirements that defend all kinds of highly technical network attacks. [1]

During recent years, network technology in China has been developed quite fast. However, compared with other countries, firewall technology in China still has a long way to go. There are some representative firewall products in China, like the Beijing Tianrongxing Network Guard, the Shanghai Jiaotong University's firewall system, and the Chinese Academy of Sciences ERCIST firewall system. Those firewall systems have some technologies like packet filtering, agency service and URL-hiding. Although to some extent, firewall products in China could meet customers' security requirement, the firewall technology still has to be developed in research and application.[1]

2.2 Intrusion detection technology

Intrusion detection technology is a new way to improve network security. The purpose of intrusion detection technology is that the systems would automatically take actions to solve problems when detecting computer systems or networks being attacked or finding system vulnerability. Intrusion Detection System (IDS) research dates back to the late 20th century, which has a twenty-year history. It mainly includes a host-based intrusion detection system and a network-based intrusion detection system. There are some milestones in the history of IDS development. In 1980, the report "Computer Security Threat Monitoring and Surveillance" written by Anderson mentioned that the current system audit mechanism has to be improved so that network managers could receive more security system information. This article is considered as the earliest writing related to IDS. Between 1984 and 1986, Dorothy Denning and Peter Nenmann developed an Intrusion Detection Expert System (IDES), which has a combined structure (intrusion detection and expert system). In 1986, it was an accepted fact that Denning's thesis "An Intrusion Detection Model" became another important writing in the IDS area. Under the influence of Anderson and IDES, intrusion detection became highly valued for network security experts. At the beginning, the host-based intrusion detection system has been widely used, which means that every host operates one or more agent programs. This intrusion detection considers the computer host as a target environment and detects the guests' systems in a certain area in order to simplify detection tasks. After an intrusion detection tools analyze and detect host audit information, they report safety and suspicious incidents. Host-based intrusion detection technology development is quite mature. A large number of intrusion detection systems are practical, such as Intrusion Detection Ltd's Kane and Information System Ltd's Stalk. On the other hand, a network-based intrusion detection system operates in a different way. Depending on the known attack mode, it traces packets on the network and analyzes whether they could cause network troubles. At present, a network-based intrusion detection system has been applied on most commercial products and operates on network nodes, like firewalls and routers. Some products are quite widely used, like Axent Ltd's Net Prowler, ISS Ltd's Real Secure and Cisco's Net Ranger. [2]

When a host-based intrusion detection system has been applied, it means that every host to be protected needs an installed detection system, so the configuration fee becomes very high. That is the reason why a network-based intrusion detection system has been more widely used instead of host-based ones. However, the development of high-bandwidth network, switched network, VLAN and encoding transmission imposes limitation on the network-based intrusion detection. Now the most widely applied systems combine host-based intrusion system with network-based intrusion systems. [2]

In total, this thesis regards a company LAN (Local Area Network) as the background. After explaining the firewall concept, technical theory and analyzing firewall configuration instructions, this thesis will explain how to test a firewall and how to research how to operate intrusion detection on VPN (Virtual Private Network). [2]

3. FIREWALL THEORY AND STRUCTURE

3.1 The firewall concept

In general, a firewall is a device or a set of devices that are used to separate protected network from unprotected network. It detects and filters all the packets transmitting from the Internet to the protected network and from protected network to the Internet. There are many methods to operate a firewall. A firewall could be considered as a pair of mechanisms, one is used to block transmission and the other one to allow transmission. Therefore, some firewalls that operate focus on blocking transmission and other focus on permitting transmission. Those two icons in Figure 3-1 which represent a firewall often appear in articles related to network.

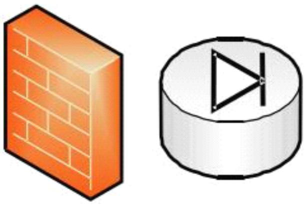

Figure 3-1 Sample of firewall icons

According to Figure 3-1, the left icon is quite visual, like a wall, on the other hand, it means that firewall has capability of filtering; there is a diode in the right icon. As we know, a diode is a device that conducts electric current in only one direction. This symbol could visually explain that a firewall has the characteristic of indirection. Although it violates firewall filtering, the mechanism being applied now illustrates the early thought of the firewall. To some extent, it can illustrate that a firewall has capability of filtering.

At early times, a firewall was designated to trust all the packets from the inner network and not trust all the packets from outer network, therefore, a firewall only filtered all the packets transmitted from outside the network and allowed guests from the inner network to transmit packets outside without any limitation. However, this behavior of firewall is not reasonable and cannot meet customers' requirements. Not only does a firewall filter packets from the outer network, but also needs to reply to the inner network guests' connection request and filter data packets from the inner network. However, it only allows data packets meeting security requirements to transmit, which is considered as owning the capability of "indirection".

3.2. Firewall Components

There are several components included in firewall

The two levels of network-access policy have a great influence on the establishment of a firewall successfully. They are installation and use of the system. During the installation, network managers should define those services and what kinds of data packets are allowed to be transmitted while the other packets are denied. In the process of use of system, those services can be applied on the firewall. Based on the services which were made before, the firewall would restrict or filter the packets in transmission. Some policies are widely spread, including flexibility policy, service-access policy, firewall design policy, information policy and dial-in and dial-out policy.

Policy

Flexibility Policy

In case that the network managers consider establishing a firewall for Internet access, they need to install flexibility policy, because the Internet changes every day and company's firewall requirements are not static. Therefore, flexibility policy is the first choice to solve those problems.[3]

Service-access policy

If user issues and dial-in policies, SLIP (Serial Line Internet Protocol) connections and PPP (Public-Private Partnership) connections are considered in setting up a firewall, the Service-access policy is the right choice to make balance between allowing users to visit network resources and keeping the private network safe.[3]

Information Policy

When the network managers allow information resources from the internal network to be seen by public, information policy can be considered.[3]

Dial-in and dial-out Policy

This policy is to add useful features to those authorized users when they are not on company premises.[3]

Advanced authentication

No matter how hard the network managers write service-access policy and implement firewalls, all the defense systems will be rather useless if there is a weak or unchanged password. There are many methods hackers could break your passwords. For example, some programs like Crack are freely available on the Internet for hackers to crack insecure passwords. Therefore, changing passwords after a certain time is essential. [3]

Some TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) services authentication should be used not only to the level of server addresses but also a specific user or server. Maybe the network managers intend to grant access to a certain user, but they must consider a situation where other people with other purposes would use this computer. This is not controllable. On the other hand, some hackers can change the server's IP (Internet Protocol) address to match those IP addresses which are trusted by a system authentication. IP spoofing is a good example in Figure 3-2, which illustrates the importance of this behavior.[3]

As Figure 3-2 shows, two hosts below are in a private network. The host with IP address 10.1.2.1 is Target one, the other with IP address 10.1.2.2 is a trusted system. Access list is 10.1.2.2. The host with 172.16.42.5 is used by a hacker in the Internet. The hacker would send a client request to the web server with a fake IP address. The web server considers this packet is coming from a trusted system and accepts the client request. Finally it returns a reply to the hacker's host. This process is called IP spoofing.[3]

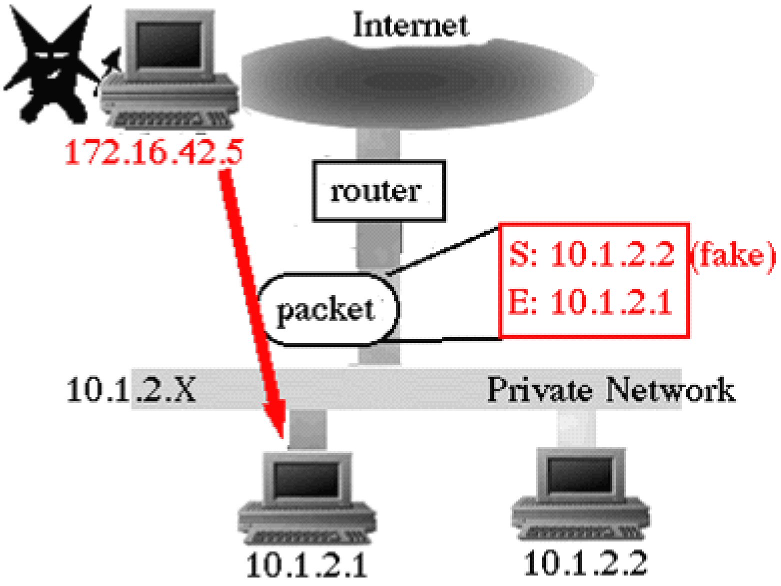

Figure 3-2 IP spoofing

There are three examples of configurations potentially exposed to attacks.

1. Faced to external network, routers support multiple internal interfaces.

2. With two interfaces, routers support subnets on the internal network.

3. In case of proxy firewall, the proxy applications use the source IP address for authentication.

Packet Filtering

In general, after being set up for packet filtering, a router has to be capable of IP packet filtering when they go through the routers' interface. Routers filter IP packets in those fields: which are source IP address, Destination IP address, TCP/UDP (Transmission Control Protocol/user Datagram Protocol) source port and TCP/UDP destination port. [3]

If a firewall is capable of blocking a TCP or an UDP connection to or from specific ports, the network managers could implement several services to guarantee that certain types of connections target specific ports instead of others. A packet-filtering router could separate traffic from the Internet when the packets pass through the router's interface. Sometimes only some specific services are allowed, such as SMTP (Simple Mail Transfer Protocol) for one system and Telnet or FTP (File Transfer Protocol) connection to another system. Filtering on TCP or UDP ports can help us to achieve this purpose.[3]

Application gateways

The application gateway is also a so called application proxy or application-level proxy. It is an application program that runs on the firewall system between two networks. If a client program wants to set up a connection with the destination program in private network, it must firstly connect to the application proxy and the application proxy acts as the client program to negotiation. After the connection is established, the firewall acts as a proxy between the two connections nodes.[4]

3.3. Technical theory

A firewall is a special network device which is used to permit or deny network transmission based on a set of rules and to protect the network from unauthorized access while authorized packets are allowed to pass. The network being protected is called inner network or private network. The one not being protected is called outer network or public network. Firewalls can effectively control network visits and data transmissions in order to protect the inner network information and filter out unauthorized packets.

There are five properties in a well-operating firewall system. The first is that all the packets transmitting between inner network and outer network must go through a firewall. The second is that only authorized packets and data following security strategies in the firewall system are allowed to pass the firewall. Thirdly, the firewall is not under the influence of different kinds of attack. The fourth is, in general, that new information security technologies at present are involved in firewall system, like modern coding technology. The final one is that an operating system is quite nice and convenient for network managers to use. The main technical theory of a firewall system contains data-filtering technology, application gateway technology and address translation technology. This thesis focuses on data packet-filtering technology and state inspection technology. [5]

Data packet-filtering technology

Data packet-filtering technology operates on the OSI (Open System Interconnection model) network layer and the transmission layer. It is also considered as the second defense line of personal firewall technology. Data packet-filtering technology operates on the interfaces of network devices. Based on data packets' source-address, destination-address, port number and protocol type, data packet-filtering technology would decide whether packets may pass or not. Only data packets meeting all the conditions of technologies are allowed to be transmitted to destination while the others are dumped. [5]

The so-called data packet-filtering technology has another name which is "message filtering" technology. It is the most traditional and basic filtering technology in the history of firewall. With the application of this technology, the concept of firewall has been put forward in 1989. Firewall packet-filtering technology is filtering all the packets during transmission and permitting the packets to pass when obeying a set of rules while denying other packets. This security strategy is the fundamental theory of firewall technology. It is made by different kinds of network applications, type of transmission and port use. [5]

Packet-filtering on a firewall is based on packet's head information. The packet's head information includes source IP address, destination IP address, protocol type(TCP packet, UDP packet, ICMP packet), source port, destination port and direction of packet transmission. Packet-filtering judges whether it obeys security rules and permits it transmit. Application of firewall can be simplified as this network topology structure is showed in figure 3-3.

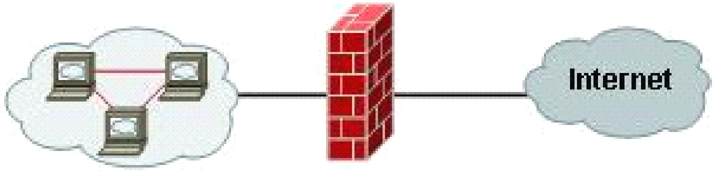

Figure 3-3 A simplified network topology structure

Generally, a firewall is the boundary between the inner and the outer network in the network structure. There are several network devices such as switches, routers in the internal network while the outer network connects to the inner network through firewall instead of other network devices. Because a firewall is regarded as the unique path connecting the inner to the outer network, the whole packets need firewall to transmit. Therefore, it effectively guarantees that all the transmission requests, also those including hacker illegal guests should be filtered out by a firewall.

State inspection technology

State inspection technology is the one which operates the firewall functions on the network layer. It adopts the software engine which operates the network security strategy under network gateway. This is called the inspection module. On the premise of network normally operating, the module selects and detects some state information from the network transmission on different OSI layers. It supports many protocols and application programs. Nevertheless, it is easy to achieve an application and to enlarge a service function. In the meantime, this module can detect the port information, such as RPC (Remote Procedure Call) and UDP. However, packet-filtering technology and agency technology do not support those ports.[5]

When an inspection module detects that a firewall receives an SYN (signal used for establishing network connection) packet, it initiates a TCP connection. This packet should be inspected based on the firewall rules. If being checked under all the rules, this packet is not accepted, then the firewall will deny this connection. However, if this packet is received, this session will be recorded in the state inspection chart and it will calculate a suitable time overflow value. Next time, when receiving a connection-confirmed data packet with symbol of SYN/ACK, the firewall will adjust the time overflow value to the right one. Then the firewall system will compare the data packet without SYN symbol with the state inspection chart. If the source IP address, destination IP address and port number are the same, the system will consider it is in the same session. This behavior of firewall improves system performance, because after a SYN data packet is received, the firewall compares every data packet with the state inspection chart instead of whether it meets all the security strategies.[5]

3.4 Firewall structure

According to the technical theory of a firewall, this thesis designates firewall's structure for education department of Hunan Province. The diagram is as follows.

In Figure 3-4, the external firewall (the left firewall) is considered as the first defense line which will isolate most of an attack action. The strategy of this firewall is to strictly control transmission from the Internet and permit packets outside based on security strategies.

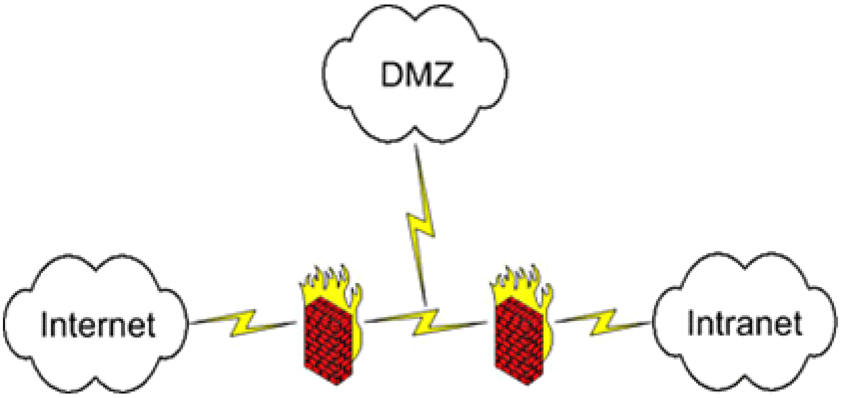

Figure 3-4 Firewall structure's network topology for a company use

On the other hand, the inner firewall operates in a company's local area network and records every behavior of transmission in the record system. The operations of the inner firewall are different from the external firewall. The internal firewall permits transmission without strict limitation in order to collect more information. However, it strictly controls messages to be sent out, because some hackers would use record systems to attack other system. Therefore, the internal firewall should be capable of intrusion detections. For collecting more important data, the internal firewall should include a sniffer to record every packet.

4. FIREWALL INSTALLATION AND CONFIGURATION INSTRUCTION

4.1. Firewall selection

Several brands of firewall products are quite widely used in the world, such as PC Tools Firewall Plus, Outpost Firewall, ZoneAlarm, Cisco Firewall and WatchGuard Firewall. Instead of hurrying to make an agreement with a firewall producer, the network manager should assess the network environment and write out the evaluation of the firewall product performance. Generally, before making an assessment, the network manager asks himself some questions, for example, what functions the firewall is capable of? How does a network manager configure firewall in order to make network well-protection? Generally, there are some factors that should be considered in this assessment.[6]

Multifunctional

A firewall should be able to deny all the services, except for some specific *s*ervices which are:

- The firewall contains advanced authentication measures.
- The firewall is capable of packet filtering.
- The firewall has application proxy.
- The firewall operation system can be updated in time.
- The firewall contains the capability to centralize SMTP access.

Flexible

A firewall should support many security policies instead of concentrating on one policy.

Security policies are able to be adjusted in order to meet some changes happened in the company network.

Convenient

- Installation time is not long.
- Configuration time is not long.
- Especially for IP filtering the language should be easy to understand or modify.

4.2. Firewall deployment

Firewall technology is a network security technology which is widely used in a company's Local Area Network. The function of firewall technology is to prevent undesirable, unauthorized transmission from a protected internal network through boundary control and strengthen the internal network's security strategy. Based on different network situations, there are different firewall structures which meet those requirements. Some common structures are listed: router-shielded structure, dual-homed host structure, host-shielded structure and subnet-shielded structure.

In a company's Local Area Network, there are some application servers (such as WWW server and e-mail server) which can be visited by the internal network and external network. Also, the internal network still needs to be included in company LAN, which is used for permitting transmission from other internal networks in the same company and denying visitors from the external network. Therefore, the network manager should have different security strategies for those servers and internal network. In order to meet education department of Hunan Province's LAN request, the author of this thesis has developed a firewall-designed plan for company use as follows.

Router-shielded deployment

This structure allows application servers and other network guests in the company LAN to operate in the same application layer of OSI. However, if security strategies for shielding routers are configured too much, it protects hosts in the internal network while it affects guests from the external network visiting the application server. On the other hand, if security strategies are not configured enough, it will influence guests' safety of internal network.

Dual-homed host deployment

This structure is quite similar to the router-shielded structure. It uses double network cards instead of shielding router, but it does not achieve the purpose of those application servers and internal network guests can use different network security strategies.

Host-shielded deployment

On the foundation of packet-filtered router, the host-shielded structure (simple host-shielded structure or double host-shielded structure) protects the internal network by adding hosts. It cannot achieve the state where application servers could be visited by guests from the internal network or external network, in the meantime, internal network is not exposed to the external network.

Subnet-shielded deployment

If the subnet-shielded structure is used, application servers will operate in the DMZ region of the subnet-shielded structure. Not only can it be protected by external firewall, but also guests from the internal external network could visit this region. Under the protection of external firewall, the internal network can also be protected by hosts (agent server). Through the router function of core switch, some data packets which would get access in the internal network are delivered to that agent server. Following the packet-filtered rule, it filters some website information which cannot be seen by the internal network guests. On the other hand, the internal network routers would deliver packets which guests from the internal network want to visit Internet by proxy servers. The proxy server will provide some services, like address translation, in order to shield the internal network. This structure makes application servers and internal network operate on different levels of security strategies, which not only meets company LAN request, but also protects the LAN safety.

Therefore, this thesis uses subnet-shielded deployment illustrated in the figure below.

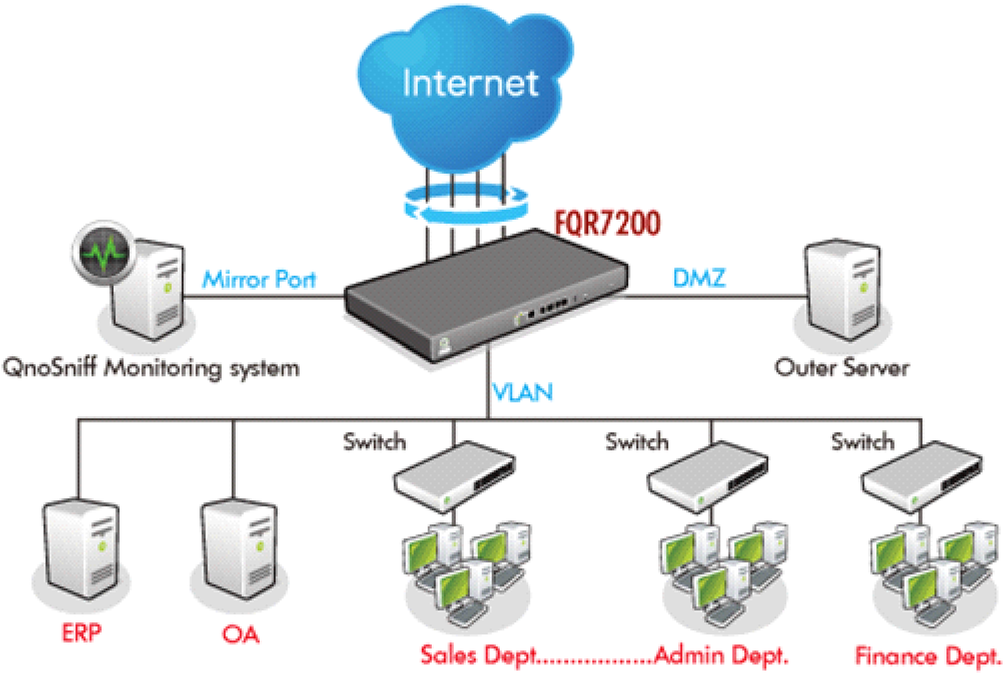

Figure 4-2 Subnet-shielded topology

In total, the company's local area network is designed, according to the core layer, distribution layer and access layer. The core-layer switch provides the network bone connection and the three-layer routing switch function. The distribution layer is responsible for access of network devices, such as servers. Access-layer switches provide guest ports. The firewall is the boundary between the external network and the internal network. The internal network is used for the company's office automatic system, including web service, device development, device agency, operational management, mail service. The distribution layer uses two central switches as backup to charge distribution and flow control.

4.3. Firewall configuration instruction

This thesis arranges a firewall between the external network and the internal network, which is regarded as a safe defense line. In this topology, the server connects to firewall's DMZ distinct and separates the internal network from the external network. On one side, the firewall's network port connects to the internal network port, on the other side; the firewall's network port connects to Internet. Therefore, guests from the Internet can only visit the public services of the company LAN, like WWW, FTP and DNS. Not only does it protect the internal network from external unauthorized visit, but it can also stop company staff using untrusted sources from the Internet. Nevertheless, it can also trace and detect every network security incident in transmission. In a certain time, the source IP-address sends IP-packets with TCP-SYN to 10 different ports of the same IP-address in the internal network and the system will automatically scan the port. The purpose of this behavior is to scan useful services and check whether a port would react in order to identify a target's service. To achieve this behavior, the firewall should be configured as follows:

WebUI

- *Screening > Screen (Zone: selection region name)；input that information，Apply*
- *PortScan Protection: (select)*
- *Threshold :(input value of port scanning)*

CLI

- *Set zone zone screen port – scan threshold number*
- *Set zone zone screen port - scan*

When hackers attack a LAN, in general, they have to scan the ports first. Therefore, the basic function of firewall should contain scanning ports. The LAN that this thesis researches, includes three Ethernet interfaces (DMZ interface, trust interface, untrusted interface). Trust interface is the one that connects to the internal network of the company.

(1) Firewall's relationship to users and servers

The firewall system contains a certificate center, a client agency and a server agency. It uses safety technologies like certificate and code. For clients, safety measures such as authentication and data-encoded are transparent. Figure 4-3-1 below represents the firewall's relationship to users and servers.

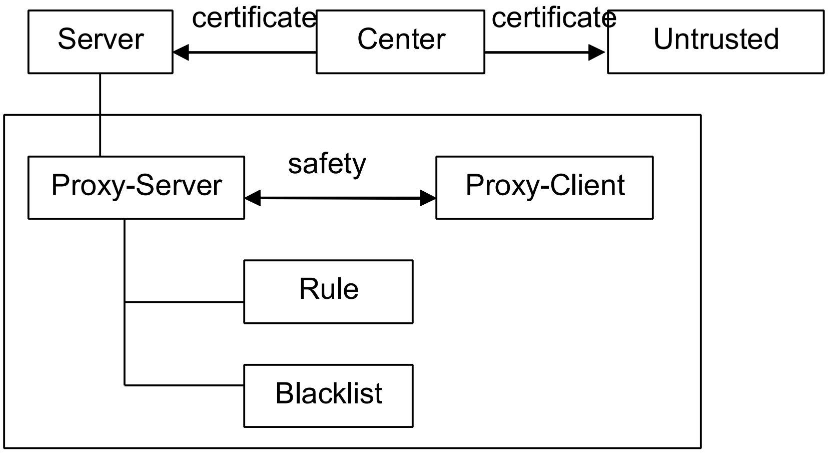

Figure 4-3-1 Firewall's relationship with clients and servers

(2)*Achievement that guards IP address against being deceived*

IP being deceived means that a hacker adds a phony source IP address in the head of a data packet in order to make security systems believe that data packets come from a trusted network. Figure 4-3-2 shows how to achieve the purpose of guarding IP address against being deceived.

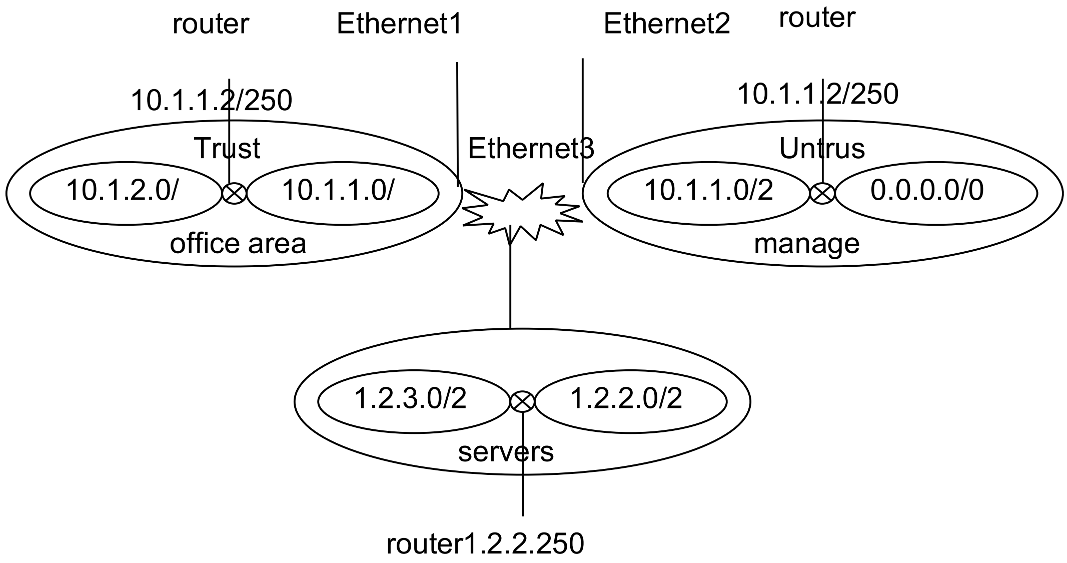

Figure 4-3-2 Internal network's topology in education department of Hunan Province

When network managers operate trust, untrust and DMZ functions in network layer, at the same time, they also enable a protection function of preventing IP addresses from being cheated.

When setting up the firewall the following parameters have to be set:

1. *commands for interface are:*
   - *set interface ethernetl zone trust*
   - *set interface etherntl ip 10.1.1.1/24*

- *set interface etherntl nat*
- *set interface ethernt2 zone dmz*
- *set interface ethernt2 ip 1.2.2.1/24*
- *set interface ethernt3 zone untrust*
- *set interface ethernt3 ip 1.1.1.1/24*

2. *commands for router*

- *set vrouter trust-vr route 10.1.2.0/24 interface ethernetl gateway 10.1.1.250*
- *set vrouter trust-vr route 1.2.3.0/24 interface ethernet2 gateway 1.2.2.250*
- *set vrouter trust-vr route 0.0.0.0/0 interface ethernet3 gateway 1.1.1.250*
- *commands for guarding ip address*
- *set zone trust screen ip-spoofing*
- *set zone dmz screen ip-spoofing*
- *set zone untrust screen ip-spoofmg*
- *Save*

5. FIREWALL-TESTED TECHNOLOGIES

When a firewall is tested, the network managers need to establish a simulative network environment. The test platform is a simulative environment that network managers establish for operating effective tests. The most common test platforms and test tools for firewall will be introduced as follows.

This test environment operates for performance test and function test. In Figure 5-1, the hub could be replaced by a switch or a switched hub. Clients mean many computer hosts. FW means firewalls. Protocol analysis (pro-analysis) could use P network analyzer (IntranetAdviser). The operating P network analyzer could assist network managers to find out source of problem and to investigate network function more quickly and effectively.

This is the diagram of a common test platform for firewall (Figure 5-1).

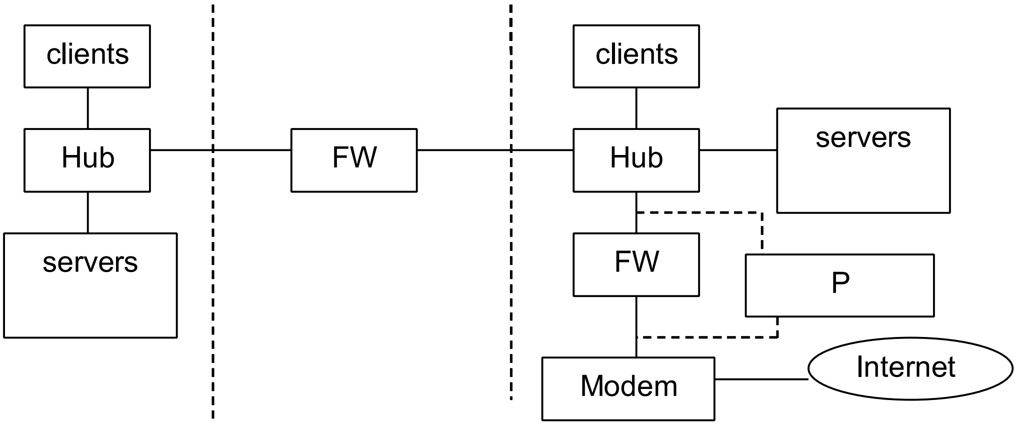

Figure 5-1 A common firewall-testing platform

Firewall-testing tools contain hardware devices and software tools. Some common software tools like IIS, Internet Seanner SAFEsuite, SATAN are security administrator tool used for analyzing the network, CRACK, NSS (Network Security Scanner) respectively. There are some common hardware devices, such as Internet Advisor (HP), SmartBits (NetCom), ATM switches, routers, switches, hubs and so on.

6. INTRUSION DETECTION IN A FIREWALL

Intrusion detection is a series of defensive methods. After the analysis of system data and finding out unauthorized network visits and attack action, the system will automatically take actions like alarming and cutting intrusion lines. There are three types of information that would be used in intrusion detection: long-term information related to intrusion detection technology, configuration information related to system current work status and auditing information related to describing system incidents respectively. An intrusion detection process can be seen in Figure 6-1.[7]

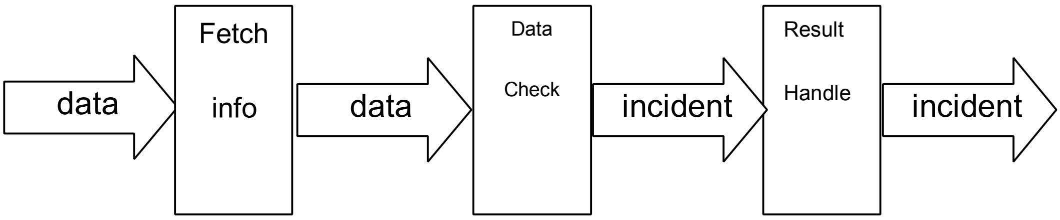

Figure 6-1 Common intrusion detection system diagram

In Figure 6-1, data include record information, dynamic information, network data information, flow change. All of those can be called data source. The function of the fetch info module is to provide data for the system. After fetch info module receives data, system simply analyzes data, for example, it simply filters data and standardizes data format. Then, those data having been handled would be delivered to the data analysis module. The function of the data analysis module is to deeply analyze the data and find out attack information. The system automatically changes the incident to a record result and delivers it to the result-handling module. The result-handling module's function is alarm and reaction. Intrusion detection is considered as an active security defensive technology, which not only provides protection against internal attacks, external attacks and incorrect manipulation, but also intercepts intrusion before the network system is damaged.

(1) Intrusion detection arrangement

Firewall intrusion detection operates intrusion detection on each step of the process in the network system in order to find out and identify attack attempts in time and protect the system sources against being incorrectly used or illegally widely used. When firewall intrusion detection detects exceptional incidents happening, the network system will take proper reaction in time, for example. It will automatically inform the network administrators. [8]

Some company network managers establish a firewall with the function of intrusion detection between the internal LAN and the Internet. The firewall can detect attack actions from the Internet or an internal network. When some exceptional incidents happen, it will actively inform the firewall to cut off the attack source. Arranging a firewall with intrusion detection is described in Figure 6-2.[8]

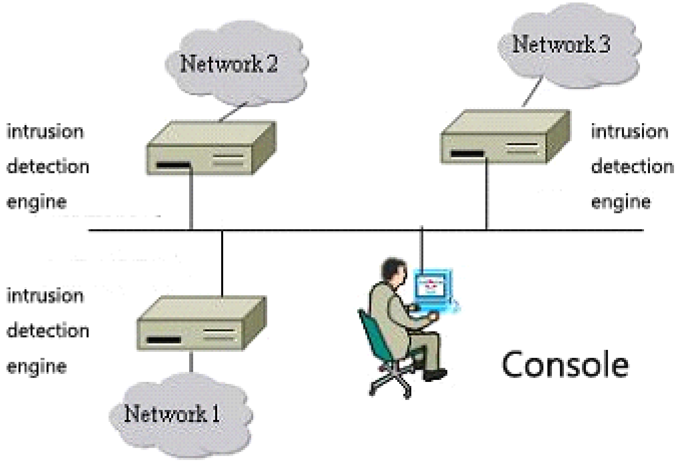
Network 2
Network 3
intrusion detection engine
intrusion detection engine
intrusion detection engine
Console
Network 1

Figure 6-2 Firewall with intrusion detection

A firewall with function of intrusion detection is capable of intrusion detection, network management and network detection. It can track all the data packets transmitted between the internal network and the external network. Based on the built-in attack character library, the firewall uses methods like mode-matching and automatic analysis to detect intrusion actions and irregular situations. After that, it records the related incidents in the database. Those incidents could be considered as administrator analysis materials, which can entirely guarantee network security in the company LAN and make up an overall network security solution plan.[8]

(2) arrangement for remote guests visiting VPN

If network managers establish a VPN server in a company LAN, remote or mobile guests are able to use the VPN software application program's encapsulation and encryption to create a safe virtual connection between the company LAN and the open unsafe public Internet, which is so-called access VPN. In other words, when using a local ISP to connect to the Internet, guests could visit the remote company LAN. In this situation, guests need to pay only same fee for connecting to the local ISP instead of a large fee. Therefore, not only do guests save a lot of money, but also this plan improves the security of data transmission.[8]

Based on the Local Area Network strategy, sources in some company LANs are only allowed to be visited by guests from the internal network. Under this strategy, in order to break this network area limitation, this thesis takes VPN technology. Because the IP addresses of those remote guests or mobile guests who would like to visit company LAN are not permanent, the author of this thesis decides to establish and setup a VPN server so as to allow remote guests and mobile guests to visit the company LAN through the VPN. Remote guests would visit the company LAN after using software to configure the VPN. According to this situation, a tunnel is established between the client and the VPN server and this is transparent to ISP.[8]

Because the operation systems that most guests in the company LAN use are Windows series, Windows 2003 Server's RRAS (Routing and Remote Access Service) can be used to establish VPN connections with PPTP and LZTP. VPN connections include router-to-router and guests with remote access server. Therefore, the author makes decision to establish VPN server with the Windows 2003 server in the company LAN. In this situation, guests only configure the VPN software on the operation platform like Windows series, then they can visit company LAN via the remote VPN server. VPN connections use a dial-up connection of RAS (Remote Access Server) to establish. RRAS dealing with the query from the VPN connection which is similar to the deal dial-up connection with a remote server.[8]

If a VPN server in company LAN could operate properly, at first, this server must be connected to the Internet, guests from the Internet would visit it. Secondly, it should be possible to connect to other machines in Education Department of Hunan Province network. Remote guests can use it to visit the LAN, because network managers establish a remote access on the VPN server. It mainly overcomes the problem of the LAN regional limitation and is convenient for remote guests and mobile guests to visit the LAN. Security requests are not too high and for wide network guests, operation on VPN is not difficult. Because the Windows series which support VPN protocol are PPTP, this thesis chooses VPN connection with PPTP. This thesis chooses VPN server in company network can be seen in Figure 6-3.[8]

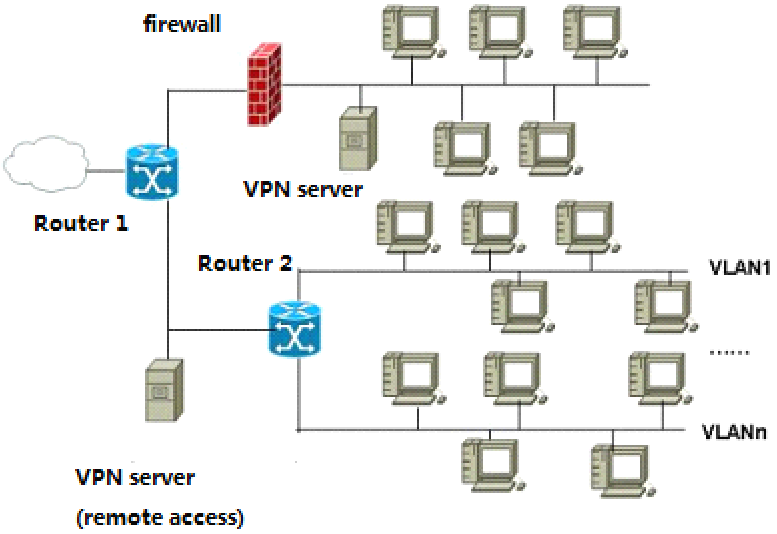

Figure 6-3 A network deployment with VPN server

If network managers would like to configure the VPN server with RPAS, at first, they should make sure that the IP address is used by the VPN server and works as a public address that can be visited on the Internet. Secondly, network managers should choose guest authentication, which occurs between the Windows authentication and the RASIUS authentication. If RASIUS (Remote Authentication Dial In User Service) authentication has been chosen, the network managers had better arrange another server for RADIUS authentication. There are two authentication protocols that could be selected, MS-CHAP v2 and MS-CHAP. At last, network managers should configure the interface filtering and visiting strategy, which is the most important part, because not only does it relate with the VPN server's operation successfully, but it also influences security problems. When designing a strategy, network managers could arrange different visiting restriction for users based on the user group, accounting name, request service type and sending-request physical interface. For example, normal guests can be given rights to visit the "office automation system" server while people who work in the science department have the right to visit the science server.[8]

7. CONFIGURATION SAMPLE

7.1. Introduction of project

During the work placement, Changsha Xiangtie Network Ltd provided the author with the opportunity to establish a management system for the clients of the education information network. The objective of this system is to establish a management platform that the city board of education was able to cooperate with each district of education department and schools in order to improve work effort and complete work flow.

Basic principles

There are several basic principles that must be followed. They are security and reliability, quick reaction, advanced technology, commonality, practicability and expandability.

Security and reliability

According to security of students and teachers' work management and professional data, when setting up the system, network managers not only should consider stable operation, but also apply strict security measures.

System structure

Network managers decide to separate the management system for education information network users and the outsiders. Because some electrical application platform should operate on external network, this platform is designated to the internal network and the external network in order to achieve different levels of data and materials' security.

Hardware private key

In order to meet the requirement that clients want to secure data and the key work process, network managers use a smart card chip to store the private key of users as well as the digital certificate and check user identity and permission.

Permission control

Based on organization, roles, work types, network managers arrange groups of people with different permission according to three modes including students' work, teachers' work, and entrance examination.

Data encryption:

In the management system for the education information network users, the storage and transmission of data should be encrypted, which avoids information leakage. The design for system update, function expandability, interface connecting with upper information system should be considered, based on data encryption and permission control.

System backup：

When network managers establish electronic application platform, data backup plan and technical safeguard measures should be considered in order to guarantee the system's security. Sometimes the system fails but the system data can be promptly restored.

The main work for our technical department is to achieve security and reliability of management system.

The network topology of management system is illustrated in Figure 7-1.

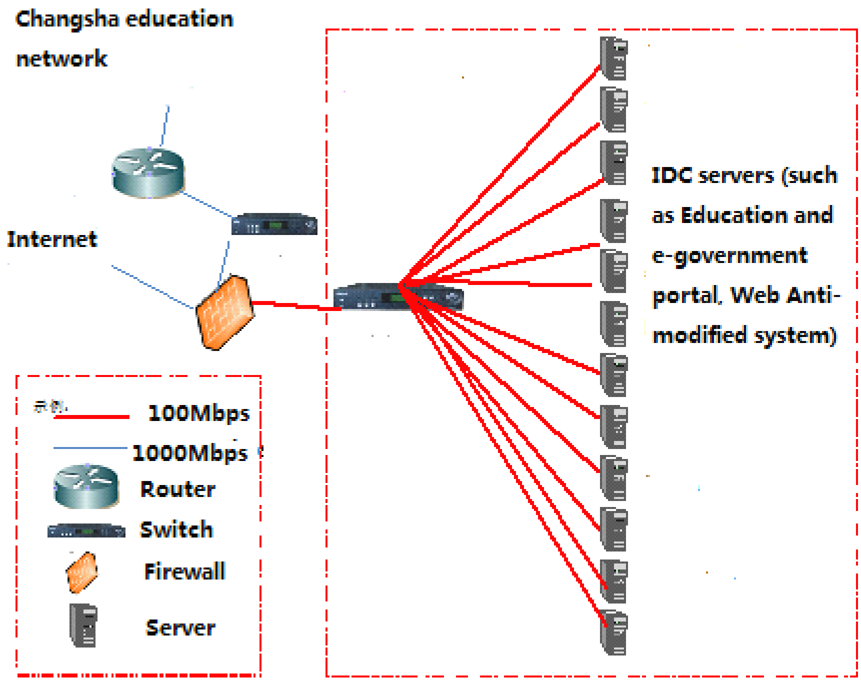
Changsha education network
Internet
IDC servers (such as Education and e-government portal, Web Anti-modified system)
100Mbps
1000Mbps
Router
Switch
Firewall
Server

Figure 7-1 Network topology of management system

7.2 Work process (Web anti-modified system)

Our team's job was to help the education department to establish and implement a Web anti-modified system.

System introduction

A web anti-modified system takes advantage of the most advanced technologies including file-filtering drive technology, event-triggered technology and security transmission technology. It obeys an Internet-related standard protocol. The web anti-modified system mainly provides functions like file-detected protection and file synchronization transmission in order to ensure that file system's documents and permission are not modified.

The system is divided into two parts, detection center and detection proxy. (Figure 7-2)

The detection center provides the web page with file synchronization and real-time file protection in order to recovery web files on the detection proxy in time.

The detection proxy stores the web files protected by the detection center, which makes it convenient for users to visit. When hackers break into detection proxy servers and modify web page, the detection proxy can replace it with the original files.

Function introduction

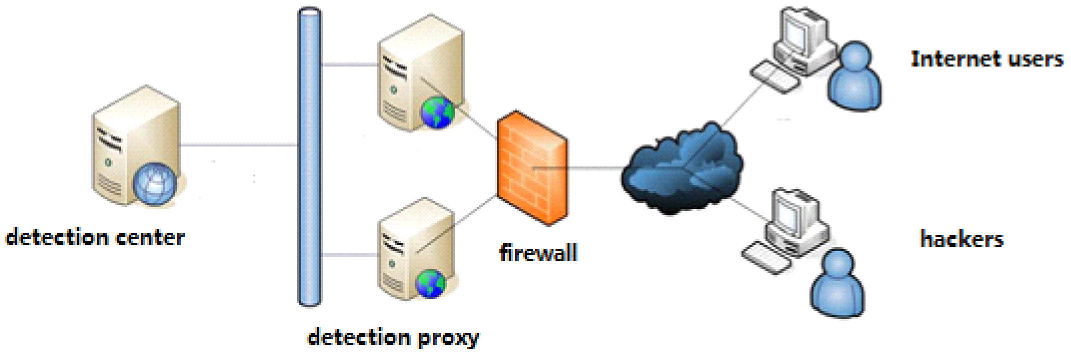

Figure 7-2 Function introduction of a firewall

File protection

The web anti-modified system takes advantage of real-time detection technology and is capable of providing detection files with real-time protection.

Automatic distribution

The portal platform generally uses the content management system and automatically produces a large number of web page files. At the same time, the system must ensure that the web content is the same as the backup data. A web anti-falsified system provides hot deployment functions and guarantees that the users only need to do simple configuration to achieve complete protection of the web pages. The web anti-modified system, combined with content management system, is able to manage the content of the web pages and keep the web safe.

Incremental backup and update

The content of the portal platform updates regularly. If network managers do some special operation, which causes the content not to be the same as in the backup, the backup needs to be updated. For efficiency and accuracy, the system provides the incremental backup and synchronization (incremental update) function. Before doing the backup or update, the system will compare the files to the backup by monitoring and then passes the incremental changes in the file.

Support of static web pages

The system supports monitoring and protections of the static pages and the file templates.

Access to audit

The system works on site maintenance support for the inquiry and audit functions. In order to allow the administrator and operator to do daily maintenance well, the system provides a log audit tool, user queries and statistics.

7.3 Firewall for configuration information

To achieve the purpose that was mentioned above, we decided to use a Huawei firewall. The Huawei firewall is widely used in China. The author has personally taken part in the firewall-establishment process. To protect the configuration information of the education department, this thesis only introduces some theory we used during the process.

1. Access list

The access list is used to make rules for the firewall interface. Several packets from some selected IP addresses are allowed to pass through the interface while the others are forbidden. On the other hand, several packets to some IP address are blocked when passing through the interface while the some others are allowed.[10]

Here follows the parameters for creating a standard access list:

- *access-list [normal | special] listnumber1 { permit | deny } source-addr [source-mask]*
- *access-list [normal | special] listnumber2 { permit | deny } protocol source-addr source-mask [operator port1 [port2]] dest-addr dest-mask [operator port1 [port2] | icmp-type [icmp-code]] [log]*
- delete access list
- *no access-list { normal | special } { all | listnumber [subitem] }*
- clear access-list counters
- *clear access-list counters [listnumber]*

- enable/disable firewall
- *firewall { enable | disable }*

2. NAT configuration

The main function of NAT is to achieve that hosts from the private network are capable of visiting the public network. The way that NAT uses fewer public ip addresses instead of private IP address could be helpful for reducing the speed of the public IP address's shortage. The other function of NAT is to provide public addresses for interior servers, which allows hosts from the Internet to visit.

3. Partly P2P bandwidth-limited configurations

This method is used to limit bandwidth for a certain network.

Configure number x(such 200M, 400M)for class0 P2P bandwidth-limited

[firewall] firewall p2p-car class 0 cir x

Configure P2P bandwidth-limited strategy

[firewall] acl number 3000(or 3001,3002, this number will be used below)

[firewall-acl-3000] rule permit source 192.168.0.0 .0.255.255.255(This ip address means a specific network's bandwidth is limited)

[firewall-acl-3000] rule permit destination 192.168.0.0 0.255.255.255

[firewall-acl-3000] rule deny ip

Apply P2P bandwidth-limited strategy for interzone

[firewall] firewall interzone trust untrust

[firewall-interzone-trust-untrust] p2p-car 3000 class 0 inbound (or outbound)(inbournd means bandwidth that hosts from a specific network could download, outbound means bandwidth that hosts from a specific network could upload).

More details are found in appendix 1.

8. DISCUSSION

Nowadays, firewalls play a crucial role in network security. Firewall components like policy, advanced authentication, packets filtering and application gateway are capable of protecting a firewall completely. However, only depending on installing and configuring firewall cannot achieve the purpose of completely protecting the network.

Network managers consider adding other equipment and software to keep the protected network safe. For instance, intrusion detection and anti-virus packages can be the best choices for network managers to install. Intrusion detection systems enable network managers to detect and analyse each packet in order to make sure it does not damage the network. Anti-virus packages can be installed on each host to protect them. Nevertheless, with the rapid development of hacker technologies, network managers need to update the firewall system regularly to counteract this threat.

The old generation of firewalls concerned on network layer and transmission layer. It filters packets based on packets' host network address, ports and protocols. In the mean time, the most important security equipments are in offices. With the development of threats from internal network and application layer attack, old generation of firewalls is not capable of completing all the defense mission. Therefore, a growing number of security functions should be included in firewall technology.

9. SUMMARY

This thesis introduces the basic background of the firewall concept, such as history of firewall, history of intrusion detection. Then it also explains what a firewall is, firewall deployment and components. To improve the security of network, intrusion detection system has been mentioned. In the end, the thesis introduces the author's work practice to illustrate how to configure a firewall for commercial use.

This thesis is a case study for administrators or network managers who want to install and configure firewall for a company.

Due to time limitation of work practice, the author was not able to take part in the whole process of establishing management systems. Therefore, every detail of the process cannot be explained in the thesis. In the future, the author will take more time to continue his study in firewall configuration and take part in work practices. Because more advanced security technology would be applied in firewall, those can be introduced later.

What is done by now is to find some commands to assist network managers to filter packets from Internet based on host IP addresses, protocols and ports. However, there are more threats from internal network. How to effectively protect them from internal threats becomes another crucial problem for future thesis to investigate. The new generations of firewalls already work on this. Nevertheless, more functions will be included in firewall technologies, such as intrusion detection. How to make those functions operate is also considered.

REFERENCES

[1] Ingham Kenneth, Stephanie Forrest *A History and Survey of Network Firewalls.* The University of New Mexico Computer Science Department Technical Report 2002-37 available at

http://www.cs.unm.edu/~moore/tr/02-12/firewall.pdf referred on 2.4.2011.

[2] Zhou Wen *Brief introduction of intrusion detection technology and Development.*Enterprise Technology Development,2008(04),76-79.

[3] Goncalves Marcus . *Firewalls complete*, McGraw-Hill Companies:US, 1998 235-245.

[4] *Application gateway* [www-document] available at http://www.webopedia.com/TERM/A/application_gateway.html referred on 2.4.2011.

[5] Kang Li *Network security and firewall technology*, Inner Mongolia Science and Economy Publisher: Hohhot, 2009.

[6]*How to select a network firewall* [www-document] available at

https://www.icsalabs.com/sites/default/files/How%20to%20select%20a%20Network%20Firewall.pdf referred on 3.4.2011.

[7] Zhao Sasa *Intrusion detection system*. China Sciences and Technical Information: Silicon Valley,2008.

[8] Feiertag Richard, Sue Rho, Benzinger Lee, etal. *Instrusion Detection Inter-component adaptive negotiation*. Computer Networks: London, 2009.

[9]*Gigabit QoS Firewall Router* [www-document] available at

http://www.michaelsoft.com.my/fqr7200-dual-core-gigabit-multi-wan-router

referred on 3.4.2011.

[10] Maiwald Eric, *Network Security: a beginner's guide,* Osborne/McGraw-Hill: US, 2001 261-179.

APPENDIX 1

The IP addresses for the interface are configured as follows:

```
[firewall-E0/0/0] ip address 192.168.1.1 24

[firewall-E0/0/1] ip address 176.168.0.1 24

[firewall-E1/0/0] ip address 192.168.2.1 24
```

Add interface to related network

```
[firewall-zone-trust] add interface Ethernet 0/0/0

[firewall-zone-untrust] add interface Ethernet 0/0/1

[firewall-zone-dmz] add interface Ethernet 1/0/0
```

Configure packet-filtering ACL rules

```
[firewall] acl 2000

[firewall] rule permit
```

Configure Nat address pool

```
[firewall] nat address-group 1 176.168.0.10 176.168.0.20
```

Configure ACL rules for address pool NAT

```
[firewall] Acl 3000

[firewall] rule permit ip source-address 192.168.1.0 0.0.0.255
```

Configure packet-filtering rules between trust network and untrust network

```
[firewall] firewall interzone trust untrust

[firewall-interzone-trust-untrust] packet-filter 2000 outbound
```

Configure Nat rules for interzone

```
[firewall=interzone-trust-untrust] nat outbound 3000 address-group 1
```

Configure Nat server

```
[firewall] nat server global 176.168.0.10 inside 192.168.1.100
[firewall] nat server protocol tcp global 176.168.0.10 80 inside 192.168.2.101 8080
[firewall] nat server protocol tcp global 176.168.0.12 1021 inside 192.168.2.102 ftp
```

Configure ACL rule for visiting Nat server

```
[firewall] Acl 3000
[firewall] rule permit ip destination-address 192.168.2.0 0.0.0.255
```

Configure interzone packet-filtering rules

```
[firewall] firewall interzone DMZ untrust
[firewall-interzone-DMZ-untrust] packet-filter 3000 inbound
```