A guide for small and medium enterprise of implementing security and firewall system

R.Zhang and P.S.Dowland

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

The aims of project were try to produce training tools to assist network administrators with limited specialist security knowledge in the selection, installation and configuration of firewall systems. The project collected customer's expectation data by questionnaire and real companies' interview methodology, with analysis current arts of firewall technology and available commercial firewall products, the project chose SmoothWall Express 2.0 as firewall system for SME and produced a step by step training guide including installation and configuration parts. The project introduced basic terminology about security and firewall in order to end users getting start of the training guide. Before the training guide producing, the project did firewall functions and security test in order to make sure the SmoothWall can fully satisfy customers' requirement, and the final of the project reviewed real companies expectations and pointed out general weakness of firewall systems and give extra suggestion about firewall and business application. The project compared and discussed similar functions techniques, in order to help SME administrator does not confused between those technologies, and gave some suggestion about how to choose the appropriate techniques for real business environment.

Keyboards

Network, Security, Firewall, Service

1. Introduction

In a recent security survey reported by Penn, Scheon and Berland Associates, around half of small and medium enterprise (SME) respondents said the security of their IT systems been threatened in the past year, another research group Gartner reported SMEs are often with limited budget for in-house IT manpower, they can not afford staff who has sophisticated security knowledge and experience, the report pointed out the security fact, half of SMEs are likely targets for attackers and 60% of them will be unaware of the attacks.

From above information, we learned that the internet for SME is so dangerous, if they just subscribed the internet connection from an ISP (Internet Service Provide) without considering any protection device/method between your LAN (Local Area Network) and the internet, that situation is very horrible dangerous, all of your devices connected to the internet are public for all of the internet users, they only need download a very small program, then they can control the LAN in few minutes. They can do anything as you can, or even they will do something but you do not know how to do. When connect the internal LAN to the internet, you are putting three things at risk:

- Your data: Your computers stored data and outbound and inbound data
- Your resource: the computers themselves and its peripherals
- Your reputation

2. How to protect

Above context, we have introduced firewall can be considered as a guard to check inbound and outbound information to protect your network, however, network firewall can not be prefect unless you stop all of the data transferring, Zwicky et al. (2000) said "a firewall can not fully protect against viruses" and Operating System's bugs can be used by attackers. Virus always pretend like a part of programme or language code, they can cross the firewall with reasonable service requirement, detecting a virus in a random packet of data passing through a firewall is very difficult, it requires:

- Recognizing that the packet is part of a program
- Determining that a change in the program is because of a virus
- Determining what the program should look like (Source: Zwicky et al., 2000)

For example, virus can be compressed into RAR/ZIP file, we can not expect firewall can detect such type files from each transmitted packet, even they can, how about other kind of compression. Also the virus can be from green zone, a piece of infected CD or floppy disk, such as spy virus or Trojan horse virus. We have to install Anti-virus software for each computer/server, and the Anti-virus must have automatic update function. And Windows has a lot of security holes, without hole-fix program, like Windows XP Service Pack 2 (sp2), Firewall + Anti-Virus will become adornments.

Firewall can be a guard, but firewall is not automatic protection. Pohlmann et al. (2002) described "A firewall system does not provide automatic protection; rather, protection is possible only if a firewall system is correctly operated." They suggest that a security policy muse be developed and implemented before a firewall system can be used. To produce the security policy, we need to know who the users are, what should be prohibited, what network protocol will be used, different privileges for different group users, etc.

3. Different types of Firewall

Home PC Firewall Guide divided security defence lines into three layers, first, Choose an Internet Service Provider (ISP) or an email service that offers online (server side) firewall or virus email filters. This will block infections before downloading them. However, this defence line is not very stable and we do not have widely choices, and normally, the ISPs only can offer very limited performance or uniform configuration. Second, to install a wired or wireless hardware router with a built-in firewall between your modem and your computer or network. For this line, we also can use dedicated firewall server, like SmoothWall. Third, Personal firewall software on every computer on your network, commercial products like Microsoft XP built-in Firewall, Norton™ Personal Firewall and ZoneAlarm or BlackICE.

From technologies aspect to approach firewall, Proctor et al. (2002) divided firewalls into three fundamental technologies, Network layer, Application layer and Hybrid. Or other terms describe these technologies include packet filters, application gateways, and stateful packet inspection. Network layer firewall works at three layer of Open Systems Interconnection (OSI) model, it led by Check Point, looking for faster technology and greater flexibility, it operates as a packet filtering, check the packets traffic based on source and destination information, for example rule as figure 1:

Action	Source	Port	Destination	Port
Allow	Any	TCP 80	Web Server	TCP 80

Figure 1 An example of firewall security rule

However, packet-filter firewall does not check detail information, such as the state of communications or application information. Another problem is the “rule” table maybe very huge, without carefully configuration it easy to make mistake. Proctor et al. (2002) concluded “Network layer firewalls are very fast, relatively inexpensive, and the least secure of all firewalls.”

Application layer firewalls are also known as application gateways and proxies. Pohlmann et al. (2002) described application gateway does not just check addresses of inbound deliveries, it opens every packet, examines its contents, and checks the shipping documents prepared by the originator against a clearly defined set of evaluation criteria. The security check at this point is significantly more reliable than packet filtering. However, the check takes longer that packet-filter firewall, for those willing to trade some performance for enhanced security, application firewall may be the good choice.

Hybrid firewalls typically combine characteristics of both network level and application level firewalls to give an improved balance between performance and security. Proctor et al. (2002) described hybrid firewall is a state- or session-aware and performs packet filtering but does not act as proxy. It can provide adequate security and the performance between packet filters and application gateways.

4. Firewall questionnaire and interview

In order to understand SME expectation for firewall, the project did two types of data collection, 1. Sending firewall questionnaire to random people but not the students/staff who from University Technology/Computer department. 2. Interview two real small companies and discuss with their IT administrator to evaluate real company’s requirement.

4.1 questionnaire results

The questionnaire includes 17 questions, and be asked 20 people to fill the questionnaire with face-to-face mode. The questions were designed into three main parts: General part, network and firewall part and firewall training expectation parts.

General part provides information about the fact of average security knowledge level, the average results show people have some computer knowledge, but not network security knowledge, they normally do not understand basic network and firewall terminology. Some people familiar with words: firewall of security. But they normally do not know what type firewall they are using, they also do not know the difference between firewall products. The most of people are using Windows based operating system, only a few people have tried Linux based before.

Network and firewall part shows information about what kind of service are expected, TCP based service more popular than UDP service. The most of them have no idea about services which out though the firewall. The most of people like to spend less than 50 pounds per year for firewall system. They expect a secure, cheap, easy installation and controlled firewall product.

Firewall training part provides information about, the most of people expect the training Guide can provide step-by-step installation and configuration with useful functions guide. They do not mind about presentation media but they expect rich pictures of screen shot, and they hope they can do practice during training.

4.2 Interview

The project interviewed two China's companies, ShanXi DaRen Education and ShenZhen HuaYi digital. They have around 20 staffs for each company, DaRen prepare to use broadband in recently, HuaYi has already connected to the internet. We are going to discuss their situation.

Case 1: DaRen is a company offering foreign language training. The project interviewed DaRen's Manager, he introduced they have around 20 computers want to connect the internet, all computers are Windows based operating system, he expect all of computers can share the internet for HTTP and MAIL Service, and the company needs a firewall to protect their network. However, they do not have in-house IT staff to conduct this task. The company like to invest around 300 pounds to purchase all of networking devices, 150 pounds for each year to maintain those devices. He answered about firewall requirement: fully protection, LAN to internet access, Voice Over IP (VoIP), he also interest for a firewall training program, he hope the training could based on non-computer background people.

Case 2: HuaYi is a company for doing digital video and audio, they are using ADSL as internet connection. Due to ADSL router setting, outside of company can not access company's LAN. Their staffs want to remotely access company's database when they away from company. The company only have an IT staff charging all IT staff, but he is specialist in Web-Design. He likes to join in a firewall training, and expect the training should not too longer, and training should include some basic terminologies could be used in the firewall system. The company would like to spend 200 -300 pounds to improve the networking situation.

Above two interviews reflect the fact of SME requirements and budget ranging for the whole devices. With questionnaire results, we can divide internet application into two main groups: LAN to internet, internet to LAN

5. SmoothWall test and results

The project chose SmoothWall for SME, before the Guide we need to do some test in order to make sure SmoothWall can fully satisfy customer requirements. The project will use WMware software to simulate internet environment to test the firewall. The test bed contains 5 virtual machine based on two real network cards, and each card connect to different switch. The test bed structure likes figure 2 shows:

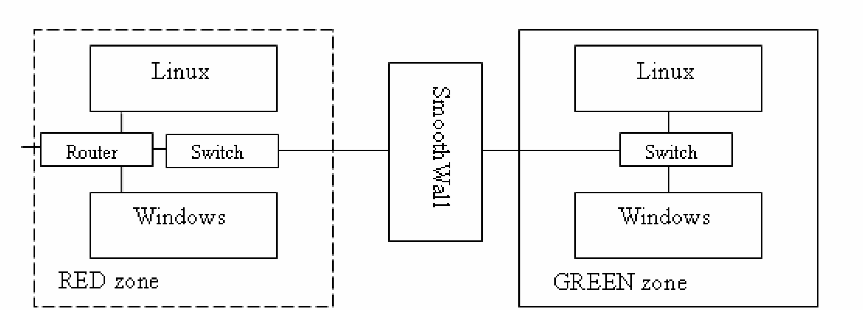

Figure 2 Test bed structure

The network divide into two zones, GREEN and RED. Each zone contains 1 Linux computer and 1 Windows computer, each machine has installed HTTP server and FTP server in order to test firewall functions. All computers setting as below:

GREEN: Subnet mask: 255.255.255.0, default gate way: 192.168.3.1
SmoothWall Interface: 192.168.3.1
Linux: DHCP/192.168.3.199
Windows: DHCP/192.168.3.200

RED: Subnet mask: 255.255.255.0, default gate way: 10.0.0.2
SmoothWall Interface: 10.0.0.10
Linux: DHCP/10.0.0.3
Windows: DHCP/10.0.04

All RED zone can be consider as Internet environment, we need to simulate port forwarding test and attack test from the RED zone. We also need GREEN to Internet service, so we have set all 4 computers as servers.

We are going to give very brief test results report, the purpose of test is used for examination of firewall functions rather than demonstration. =

DHCP Server: Linux and Windows are both assigned IPs information by SmoothWall Server, DHCP => PASS

NAT server: Linux and Windows are both can access internet, NAT server=> PASS

Proxy Server: Linux and Windows setting proxy server address: 192.168.3.1, port: 800, then can access internet, proxy Server => PASS

Port forwarding: add rule in SmoothWall, forwarding 192.168.3.200:80 port to 192.168.3.1. RED zone access 10.0.0.10, and opened 192.168.3.200's web page. Port forwarding => PASS

IP block server: add rule in SmoothWall, block RED Linux IP 10.0.0.3, and using 10.0.0.3 to access 10.0.0.10, access denied, and remove the rule from SmoothWall, 10.0.0.3 can access 10.0.0.10:80 (192.168.3.200) port. IP block server => PASS

Logs service: Access SmoothWall web administrator interface, click logs, you will find comprehensive logs recorded by SmoothWall, it can be used for security and networking analysis. Logs service => Pass

6. Port forwarding Vs DMZ

DMZ exposes all of ports of server, it means DMZ has no firewall protection at all. And only single server available in the ORANGE zone, you need to build all of service into one server, it reduces network structure flexibility. Or you need to set up "dmz pinholes" for forwarding GREEN's ports to ORANGE zone, but similar complex as "port forwarding" setting. Using port forwarding you can only forward wanted services port to the internet, and you do not need to build a ORANGE zone, the services port from GREEN zone.

The choice between DMZ and port forwarding depends on your network requirement and existing network structure. You need to consider your broadband upstream speed, for ADSL connection, downlink and uplink have different data rate, ISPs normally provide 256kbits/s speed for upstream even you may have 8mbits/s download speed, you can not expect using ADSL to build a server for public, but these two techniques help you to easily build a mobile office in your home.

7. Proxy firewall and packet-filter firewall

We have introduced application level proxy and packet-filter firewall: they both have advantage and disadvantage. Norbert etc compared two solutions: Packet-filter can provide higher flexibility, faster process speed, full application supporting. Application proxy can provide higher secure, better management ability, require identification and authentication before transporting. Xinli website described, Proxy server will dramatically increase server usage when high inbound and outbound more than 75MB/s, nowadays, ISPs can provide highest internet connection is 8MB/s, you do not worry about 75MB/s bottle neck, but faster and more RAM is recommend for using proxy service.

8. The weakness of firewall systems

Oppliger (1998) described, “firewall can not protect against insider attack”, firewall only checking when the packet pass through the firewall, for insider communication packets will not need to go through the firewall, no device will stop inside attack. To resolve this problem, we can add extra firewall for higher security department, like financial department. Central firewall + ICF for each computer is a good practice for organisation.

Firewall can hardly detect virus pass through it, especially when the data be compressed, it is impossible to build a scan to check virus signatures, compression with different algorithm can produce any number of a packet format. The efficient way to detect virus is installation of an anti-virus program, the software can check full file rather than packets.

Firewall can not improve the rules by themselves, firewall will do exactly things as you set, a poor setting will results higher vulnerability and firewall can not fix the poor setting. You need to maintain the firewall regularly, you need to view and check firewall logs information, you also need to understand the users expectation, under company policy to improve security policy.

Firewall can be bypassed, in the GREEN zone, the end user may have different internet connection as you provided, a modem connection or a remotely VPN with dual sub-net, other people will have chance bypass you firewall server, firewall can not provide protection that not pass through it, and you whole GREEN may will have a directly link to the internet. You need to pay attention for the security policy again, security policy needs to be discussed with users or you need to force users following the rules.

9. Conclusion

The paper introduced an overview of SME security aspect, briefly discussed SME currently faced problems, and three methods need to be adopted to resolve the problem. Three protection methods must be used at same time. The project did questionnaire and interview for collecting customer data, and the project chose SmoothWall as firewall system for SME, some functions and security test has conducted by the project. The paper discussed some functions may confused SME, and pointed out the weakness of firewall system, also gave the solution to overcome those drawback.

10. Reference

Firewallguide (2006), “Home PC Firewall Guide”, www.firewallguide.com, (accessed 31 July 2006)

Gartner Group (2000), NetworkWorld, “Half of small, midsize enterprises will suffer Internet attack”, www.networkworld.com/news/2000/1011attack50.html, (Accessed 31 July 2006)

Oppliger, R. (1998), Internet and Intranet security, Artech House, Inc.

Penn, Scheon and Berland Associates (2005), SOHOWare Inc., “BroadSscan TM solutions overview”, www.sohoware.com/support/pdf/BroadScan_Solutions_Overview.pdf, (Acessed 31 July 2006)

Pohlmann, N. and Crothers, T. (2002), Firewall Architecture for the Enterprise, Wiley Publishing

Proctor, P.E. and Byrnes, F.C. (2002), The Secured Enterprise Protecting Your Information Assets, Prentice Hall PTR

XinLi (2004), “Firewall five main functions”, www.xinli.com.cn/showPage.phtml?cID=67&oID=322 (accessed 31 July 2006)

Zwicky, E.D., Cooper, S. and Chapman, D.B. (2000), Building Internet Firewalls, 2nd Edition, O’ Reilly & associates