4th International Conference on Mechatronics, Materials, Chemistry and Computer Engineering (ICMMCCE 2015)

Enterprise Network Virus Protection Research

Yanjie Zhou 1 , Li Ma 2 ， Min Wen3

1,2College of Mathematical and Computer Science Jiangxi Science & Technology Normal University Nanchang, China
3 Department of Civil and Architectural Engineering Nanchang Institute of Technology Nanchang, China
1zyanjwm@163.com,2 liima@sina.com，3sxwenmin@163.com

Keywords: Network; Safety; VPN. Firewall; Virus protection

Abstract: Enterprise network virus protection system directly affects the interests of the enterprise. A large number of external and internal network security problem data show that enterprises improve the requirements of network security in order to protect network resources of the enterprises. This article analyzes and studies VLAN, firewall, VPN, anti-virus technology of small enterprises' network virus protection system, and put forward enterprise network virus protection measures.

I. INTRODUCTION

Since there is a network, network security problems also arise, and network security problems come in the network too. Network security events such as virus and hacker attacks appear, and such events happen all the time throughout the world. In addition, there are malware intrusions and unauthorized access to user hosts. These behaviors pose a lot of security problems to illegal interception and user's information leak. The harm of network security events has sure been experienced by each computer user more or less, such as: computer system dysfunction leads to the destroy of all the data in the whole computer system, and even affects disks and causes other hardware damage.

In order to prevent network security events, all computer users, especially enterprise network users must take adequate security measures, and even to balance the interests at all costs. But it must be pointed out that the implementation of enterprise network security strategy is a systematic project involving many aspects. So it is necessary to consider the external threats, as it often happens, pay full attention to internal and network management for their own network security has the hidden trouble of security risks. Never own isolated view on any safety measures.

II. THE PRESENT SITUATION OF ENTERPRISE NETWORK VIRUS PROTECTION

A. The present situation of enterprise network virus protection

Generally small businesses depend on networks, including Internet and internal network. The existing network security are no longer able to meet the needs of the development of the company, so, the urgent task now is to set up a comprehensive network security system.

General small business enterprise network security architecture requirements are as follows:

1. The existing network equipment company planning network;
2. The availability of network system protection;
3. The continuity protection of network business;
4. The prevention of unauthorized access to network resources;
5. The protection of enterprise information privacy through network transmission integrity;
6. The prevention of virus violations;
7. The realization of network security management;

According to the demand and status of small businesses, construct network security network system transformation to improve the stability of the enterprise network system and run all sorts of designs in order to ensure the security of enterprise information and avoid leakage of drawings and documents. Computer software is safe by the clients, and can protect user record of key directories and files in client computer operation so that enterprises can have correct use method.

Users are using the client computer to track and prevent the entry of foreign computer and cause harm. Through network switch, all managers have convenient network server, client, user log-in permissions and installation of integrated management and monitoring applications. So you need to:

1. Develop a good business environment to ensure physical security equipment;
2. Divide VLAN control internal network security;
3. Install a firewall system;

4. Set up VPN to ensure data security;
5. Install anti-virus server;
6. Strengthen the management of network resources;

B. Enterprise network structure

Small enterprise's network topological diagram is shown in Figure 1.

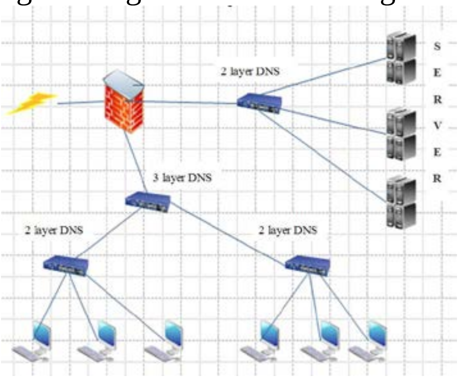


Figure 1 Enterprise network structure

It is used for direct connection to IP network and telecommunication 58.191.65.62, 255.255.255.0 through a firewall to DMZ and common areas. Respectively make NAT firewall client address 10.1.1.0 255.255.255.0. Firewall port address 10.0.1.1 255.255.255.0 accesses the client area. There are various types of servers and address assignments in DMZ 10.1.2.0 255.255.255.0. Firewall interface address is 10.1.2.1 255.255.255.0 in DMZ. Network takes3 layer switch as a core switch, and then accesses switches in two 2 layers.

III. ENTERPRISE NETWORK VIRUS PROTECTION RESEARCH

A. Enterprise network function

1. Resources sharing. Individual users can share the database on the Internet and share printers and the functions of office automation.
2. Communication services. End users through wan connection can send and receive E-mails, Web application implementation, and secure wan access to Internet access.
3. Multimedia capabilities. VPN remote dial-up access. The system supports PPTP remotely access, and field work personnel can access through the network.

B. Enterprise network virus protection design

1. Enterprise physical safety equipment

(1) Physical location choice

Equipment room should meet the requirements as places without certain earthquake, wind, rain and also should avoid near to high-rise building or basement, and host space should avoid high intensity electric field.

(2) Power supply

Computer room should have power, and backup electric power supply to enable public power supply system work to prevent computer fault in a crucial time.

(3) Electromagnetic protection requirements

This should be used to prevent electromagnetic interference and parasitic server; and should avoid communication cable and power cord’s interference with each other.

2. Intranet VLAN settings

A. VLAN division and address allocation

Office manager subnet (VLAN2) : 192.168.1.0 subnet mask: 255.255.255.0 gateway: 192.168.1.1
Production of subnet (VLAN3) : 192.168.2.0 subnet mask: 255.255.255.0 gateway: 192.168.2.1
Market subnet (VLAN4) : 192.168.3.0 subnet mask: 255.255.255.0 gateway: 192.168.3.1
Financial subnet (VLAN5) : 192.168.4.0 subnet mask: 255.255.255.0 gateway: 192.168.4.1
Resource subnet (VLAN6) : 192.168.5.0 subnet mask: 255.255.255.0 gateway: 192.168.5.1

Step one: VLAN divide three switches S1, and add the port VLAN.

```
S1 # configure terminal      S1 (config) # vlan 2       S1 (config - vlan) # name vlan2
S1 (config - vlan) # exit
```

```
# vlan 3 S1 (config)       S1 (config - vlan) # name vlan3     S1 (config - vlan) # exit
4 # 1 (config) vlan
S1 (config - vlan) # name vlan4     S1 (config - vlan) # exit
1 # (config) vlan 5     S1 (config - vlan) # name vlan5
S1 (config - vlan) # exit
S1 (config) 6 # vlan     S1 (config - vlan) # name vlan6
S1 (config - vlan) # exit
S1 (config) # int f0/1     S1 (congig - if) # switchport access vlan 2
S1 (config - vlan) # exit
S1 (config) # int f0/2     S1 (congig - if) # switchport access vlan 3
S1 (config - vlan) # exit
S1 (config) # int f0/3
S1 (congig - if) 4 # switchport access vlan
S1 (config - vlan) # exit
S1 (config) # int f0/4
S1 (congig - if) # switchport access vlan 5
S1 (config - vlan) # exit
S1 (config) # int f0/5
S1 (congig - if) 6 # switchport access vlan
```

Step 2: VLAN IP address assignment and VLAN as "virtual interface processing”.

```
S1 (config) # interface vlan 2
S1 (config - if) # ipaddress 192.168.1.1 255.255.255.0
S1 (config - if) # no shut
# interface vlan 3 S1 (config)
S1 (config - if) # ipaddress 192.168.2.1 255.255.255.0
S1 (config - if) # no shut
S1 (config) # 4 interface vlan
S1 (config - if) # ipaddress 192.168.3.1 255.255.255.0
S1 (config - if) # no shut
S1 (config) # interface vlan 5
S1 (config - if) # ipaddress 192.168.4.1 255.255.255.0
S1 (config - if) # no shut
S1 (config) 6 # interface vlan
S1 (config - if) # ipaddress 192.168.5.1 255.255.255.0
S1 (config - if) # no shut
```

Step 3: Set relay port and 3 layer switches in switches.

For example: Three switch S1 and S2 configuration subnets are in general manager's office

```
S1 (config) # int f0/1       S1 (config - if) # switchport mode trunk
S2 (config) # int f0/1       S2 (config - if) # switchport mode trunk
```

The same configuration relay port configures three switches S1 and other four 2 layer switches.

Step four: Three switches S1 and router R1 routing configuration is complete

```
S1 (config) # IP route 0.0.0.0 0.0.0.0 192.168.10.1     R1 (config) # IP route 0.0.0.0 0.0.0.0 192.168.0.0
```

Step 5: Access control of conversion layer configuration

```
S1 (config) # IP access list 101 permit 192.168.1.0 0.0.0.255 any)
S1 (config) # access - 101 deny IP list any 192.168.1.0 0.0.0.255
S1 (config) # access - 101 deny IP list any 192.168.4.0 0.0.0.255
S1 (config) # access permit any any IP list in 101
```

B. Access control strategy

Office manager VLAN2 can access all the rest VLAN.

Market VLAN4, production VLAN3, resource VLAN6 cannot access manager office VLAN2, and financial VLAN5.

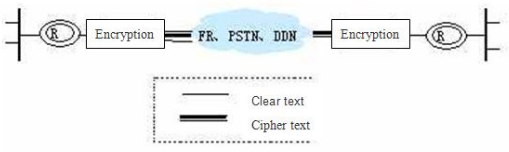
Production VLAN4 and sales VLAN3 visits each other.

3. Communication security

Confidentiality and integrity of data are mainly to protect related confidential business information spread on the Internet through encryption device and equipment, and data encrypted text via the Internet, rather than plain text. You can choose the following ways:

(1) Link layer encryption

Classified nodes wan line uses different level of link encryption equipment for different types of lines for unauthorized users read data, tampering and data transmission to ensure nodes data exchange, which is shown in Figure 2.



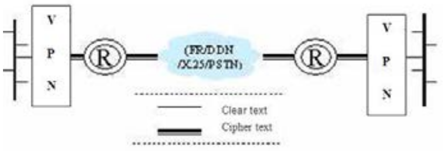


Figure 2 Schematic diagram of cipher machine link equipment Figure 3 VPN configuration diagram

Because the machine is a chain of encryption level, computer rules use point to point encryption and decryption way. Equip each network access encrypted transmission perimeter a link encryption machine of mutual needs and requirements.

(2) Network layer encryption

Considering the wide distribution network and other communications lines, use different encryption equipment which increases design system costs, as well as system expansion, upgrade and maintenance difficulties. Therefore, in this case, we recommend a network encryption machine, which is a kind of encryption method to implement end-to-end, that is to say, in the process, there is an encryption machine. Protect some business secrets and sensitive information and their integrity and authenticity. IP Sec is an important network security service system. A standard IP protocol encryption device is shown in Figure 3.

VPN equipment operation can reduce the investment of network security equipment because there is no specific link; In addition, the most important thing is that it can provide suitable infrastructure and network layer security requirements for all optional virtual private network services platform. Network system can be in such a big government, and VPN equipment upgrade speed can also make network have good scalability. Given the prominent advantages of VPN, according to different needs of enterprises, install VPN equipment import and export in public network at each network node.

4. Anti-virus technology

Today, each network system generally uses WINDOWS operating system; therefore, the used anti-virus technologies include virus prevention, virus detection, and anti-virus:

(1) Prevent virus technology

Anti-virus technology is to detect whether there is a computer virus through system memory, priority access control system, monitoring system to prevent the invasion of computer virus, system damage, and information tampering. This technique can precede read and write encryption protection, control, anti-virus, monitoring system, enforcement procedure.

(2) Detecting virus technology

The feature of virus detection evaluation technique is computer virus technology (such as self-calibration, keywords, file size, etc.) to determine the type of virus.

(3) Anti-virus technology

Through anti-virus technology’s computer virus code analysis, develop new programs to remove viruses and information to restore the original file and set up anti-virus program. Anti-virus technology often happens, and its concrete operation includes a workstation and network file server and email scanning and monitoring and email scanning. Once the virus code base matches the corresponding code, anti-virus program will accept command measures (rename, delete) in order to prevent the virus spread further.

C. Enterprise network virus prevention measures

According to the situation of enterprise network, considering the company's anti-virus system cost and performance of the system, use anti-virus Jiangmin kv online to build internal network anti-virus system. Kv is computer network virus protection system, including some suitable hosts, and a variety of WEB servers, mail servers, application servers, which distribute in different cities and becomes tens of thousands of large network. Kv has the following outstanding characteristics: advanced system structure, strong anti-virus ability, complete remote control, convenient classification, and group management.

Main control center server company kv online edition deploys in three switch before the server in demilitarize zone sub-center. Network topology is shown in Figure 4. Parent-child relationship is between control center and main control center. Control center is the core of kv and kv networks control center is responsible for management. Kv network deployment must be first installed. In addition to daily management and control on computer network, it also records real-time monitoring of virus in kv every computer online protection system, and kill virus and other updated information. According to the control center, divide it into the main control center, sub-center to complete the control center in another child control center, and the main control center is responsible for parent company communication. The "mother" and "children" are a relative concept: each control center field is control center, and control another child with superior network control center, and the control structure can expand the network infinitely.

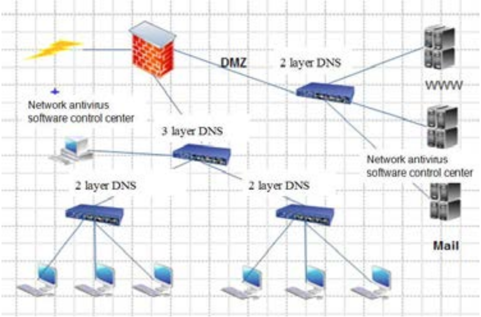


Figure 4 Control center deployment diagram

IV. CONCLUSION

With the popularity of network applications, network security has become particularly important, and the safety system established by government and enterprises is also more demanding. All sorts of network security products present cannot achieve what we want to protect. Through practice, this paper based on risk assessment analysis of network security, carries on the research of network virus protection for enterprises, and puts forward the solution for enterprise security to solve network security problems in general small business. But with the continuous development of computer technology, computer network security technology will be more and more complex, thus enterprise network virus protection should also be constantly updated.

Acknowledgements: This research has been supported by Jiangxi Science & Technology Normal University reform project JGYB-14-24-32.

REFERENCE

[1] Hur J, hoo D, Hwang S O, et al. Removing escrow from ciphertext-policy attribute-based encryption. Computers and Mathematics with Applications[C], 2013, 65(9): 1310-1317

[2] Liang X, Li X, Lu R, et al. An efficient and secure user revocation scheme in mobile social nehvorks. Proceedings of the IEEE Global Communications Conference (GLOBECOM'll) [C], Dec 5-9, 2011

[3] Houston, TX, USA. Piscataway, NJ, USA: IEEE, 2011: Sp Li M, Yu S, Zheng Y. Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption. IEEE Transactions on Parallel and Distributed Systems[C], 2013, 24(1): 131-143

[4] Zhou Z, Huang D. On efficient ciphertext-policy attribute based encryption and broadcast encryption. Proceedings of the 17th ACM Conference on Computer and Communications Security(CCCS'10) [C], Oct4-8, 2010, Chicago, IL, USA. New York, NY,USA:ACM, 2010:753-755

[5] Hur J, Noh D h. Attribute-based access control with efficient revocation in data outsourcing systems. IEEE Transactions on Parallel and Distributed Systems[C], 2011, 22(7): 1214-1221

[6] Hur J. Attribute-based secure data sharing with hidden policies in smart grid. IEEE Transactions on Parallel and Distributed Systems[C], 2013, 24(11):2171-2180

[7] Lubicz D, Sirvent T efficient. Advances Attribute-based broadcast encryption in Cryptology: Proceedings of the 1st
scheme made International Conference on Cryptology in Africa (AFRICACRYPT'08) [C], Jun 11-14 2008

[8] Shallow of alick. The enterprise computer network virus prevention [J]. A heavy technology. 2012(02)

[9] Pan Zehong, Chen chun . The characteristics of network virus and its security strategy [M]. Association for science and technology BBS (second half). Wireless technology. 2011(03)

[10] Stevens R W. Security of personal information in a new health care system.[J]. JAMA : the journal of the American Medical Association,1994,27119.

[11] Anonymous. CA Survey: Adults Worry about Security of Personal Information Online[J]. Wireless News,2008.