Security System Research in the Government Network

Y.Y. Ji
Communication Management Bureau of Zhejiang
Hangzhou, Zhejiang, China

C.L. Yu
HangZhou Dianzi University
Hangzhou, Zhejiang, China

B. Wang
Confidential Bureau of Yuhe
Lishui, Zhejiang, China

***Abstract*—Government network security issues have become increasingly prominent. In this paper, after analyzing the existing government network security system of Yunhe county government network, we pointed out that the threats to the status quo of the government network security. And then we proposed specific rehabilitation programs for the deficiencies of the original network.**

Keywords-government network; network security system; network reform

I. INTRODUCTION

As a special application area of information network, government network demands very high security level for data and information operating in it [1]. It will surely cause serious losses if government network system were hacked. As a consequence, it is very necessary to improve the structure of the security system and enhance the performance of the security system, which is very significant to improve the safety of government network.

II. RELEVANT RESEARCH

A. Internet Security Protection System

Internet security protection system is consist of security operating system, application system, firewall, internet monitoring, security scanning, communication encryption, internet anti-virus, etc. each module is able to cover part of the system function [2].

B. Analysis for Previous Government Network Safety

Take the government network of Yunhe county in Lishui as an example, there are some safety risks in the previous government network.

a. VPN safety risks. As a main way to access government external network from internet, however there is no safety equipment behind the VPN equipment and this makes users, who login government external network via VPN, lack of network protection and safety supervision [3].

b. Server isolation. Server shares the same network with ordinary users without safety separation and access control policy. It would be dangerous if hacking comes from internal network.

c. Different switchers in the backbone network. As the construction of backbone network was not done at one time, there are many different switcher brands and models, which may cause port mismatch.

The previous network topology in Yunhe county is shown as figure1 below,

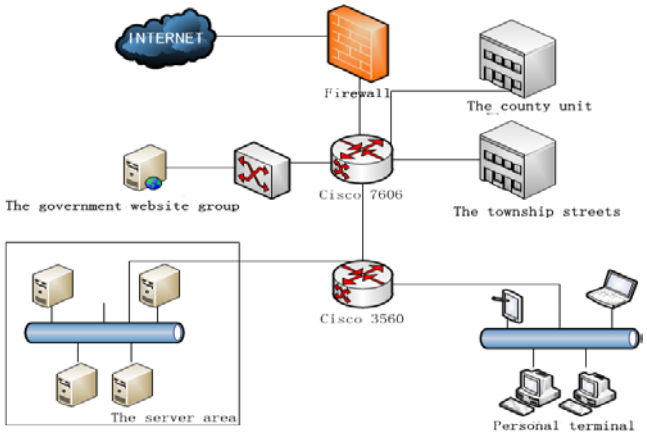

FIGURE I. PREVIOUS NETWORK TOPOLOGY IN YUNHE COUNTY.

III. REFORM PROJECT OF GOVERNMENT NETWORK SAFETY STRUCTURE

A. Firewall

Deploy the firewall between the core switcher in internal network and internet. Considering the necessity of safety redundancy and high performance of network, the firewall shall work at a dual-A status to form redundant double-link structure [4]. Figure 2 shows the reformed firewall deployment plan.

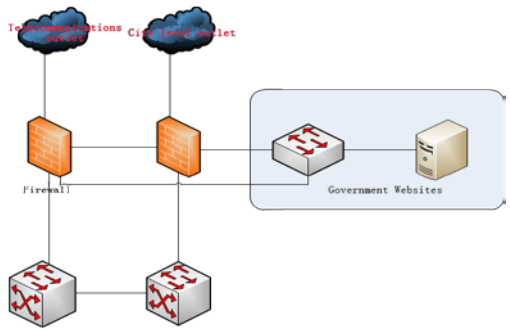

FIGURE II. FIREWALL DEPLOYMENT PLAN.

B. VPN

Government network demands safe transmission when important business data transforming on the internet, and the basic requirements are as follows,

ensure the truth and integrity of data, and the confidentiality of channel. Offer dynamic key exchange, united safety management service, security protection and access control, etc. In order to reduce the impact on present application system and make sure there is no impact on development of some new business applications, VPN network shall be deployed to offer convenience to access internal network via VPN for government workers who are on a business trip [5].

The VPN deployment plan is shown in figure 3.

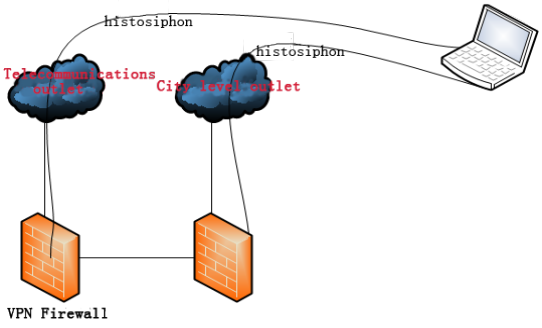

FIGURE III. VPN DEPLOYMENT PLAN.

C. IDS (Intrusion Detection System)

IDS should be deployed on the boundary of government network and information system to detect Trojans and vulnerabilities from external network [6] [7]. The IDS is shown in figure 4.

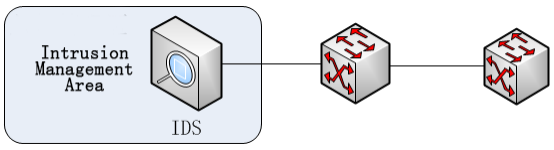

FIGURE IV. IDS DEPLOYMENT PLAN.

This IDS can detect any activity which passes this segment and monitor the dynamic network in real time. It will find intrusion via characteristics of packets, therefore fend against network attack from internal and external environment. In order to improve the intrusion detection capability of the system, continuous update of intrusion characteristics with system version upgrade is necessary.

This IDS applies by-path structure, all data go through the switcher are transmit to IDS via a mirror port on the core switcher. After analyzing the received data, the IDS will give an alarm or call the firewall when finding an attack to stop it.

IV. REFORMED GOVERNMENT NETWORK

This reformation plan divided the government network and information system into separated safety area. Business system area, which is a key protected object, was set up as the core of government network and information system in Yunhe county. So far most safety risks come from the internal internet, an ordinary PC terminal can access servers arbitrarily. Besides, their authority is too high for general PC terminal users, therefore, mishandling, virus infection and malicious attacks may bring high safety risks to servers. So the server area is separated by firewall to realize security isolation between PC terminals area and business area. Reformed government network topology is shown in figure 5.

After the implementation of access control and security isolation between the network in Yunhe county and the Internet, which realized by the firewall between those 2 networks, corresponding intrusion protection and activity management are applied in deep data attack analysis. When attack happens it will directly clean it up or make a warning, which improves the safety of government network system in Yunhe county.

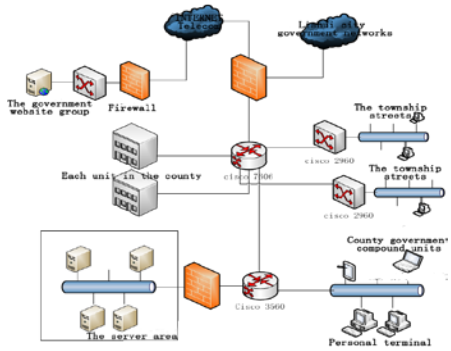

FIGURE V. REFORMED GOVERNMENT NETWORK TOPOLOGY.

V. DATA COMPARISON ANALYSIS BEFORE AND AFTER NETWORK REFORMATION

Because of the specificity of network security devices, it is difficult to define key data when taking test on data. Therefore we can only extract monitoring results on the network repeatedly to test whether the safety data function well. This article take 7 representative and meaningful nodes as test site to measure average delay and packet loss rate during the visit from Yunhe county to each test site. Test data can be reference when comparing and analyzing network situations before and after reformation.

A. Data before Network Reformation

Average delay and packet loss rate before network reformation is shown as table 1 and table 2.

B. *Data after Network Reformation*

Average delay and packet loss rate after network reformation is shown as table 3 and table 4.

C. *Analysis*

As the test results shown, it is obvious that government networks have a lower risk of attacking from professional hacker. As network congestion caused by virus is more common, it is very important for network manager to find reasons for congestion and resource of virus.

VI. CONCLUSION

With the widespread use of government network in government work, security of government network is more and more significant. This article chooses government network of Yunhe county in Lishui city as example, and raises specific network security reforming plan on the base of previous security detection system of government network. After the analysis of test data before and after network reformation, we can draw a conclusion that the probability the government network surfer attacks from professional hacker is reduced obviously. Hence it is significantly meaningful for government network security improvement.

REFERENCES

[1] Feng Ma, Ying-li Zhang, Yu-feng Yang, Commonly security technologies used in E-government network. Industrial Engineering, 7(2), 2004.

[2] Ai-ming Chen, Computer security and confidentiality. Electronic Industry publication, 2004.

[3] Yu-guo Wang, Security technology for computer information systems. Information Systems Engineering, 11, 2013.

[4] Jing-long Cai, Qian Qin, Key technology of firewall research. Science & Technology Information, 27, 2008.

[5] Na Xu, Chao Zhang, Discussion for computer LAN security measures. China Science & Technology Panorama Magazine, 10, 2013.

[6] Jian-chun Jiang, Heng-tai Ma, Dang-en Ren, A Survey of Intrusion Detection Research on Network Security. Journal of Software, 11(11), 2000.

[7] Xiao-jing He, Research for network security intrusion detection technology. Public Communication of Science & Technology, 2, 2012.

TABLE I. AVERAGE DELAY BEFORE NETWORK REFORMATION (MS).

	To City Information Center HUAWEI 8512	To City Information Center East Computer Room cisco7609	To Songyang County cisco7606	To Yunhe County cicso 7606	To Lishui City DNS	To Yunhe County DNS	To Normal PC
The 1st Time	2123	2144	3001	1454	1355	1122	1011
The 2nd Time	13	12	15	2	3	1	11
The 3rd time	time out	time out	time out	time out	time out	time out	time out
The 4th time	13	12	15	2	time out	1	11
The 5th time	1823	1944	2801	1447	1055	922	911

TABLE II. PACKET LOSS RATE BEFORE NETWORK REFORMATION (%).

	To City Information Center HUAWEI 8512	To City Information Center East Computer Room cisco7609	To Songyang County cisco7606	To Yunhe County cicso 7606	To Lishui City DNS	To Yunhe County DNS	To Normal PC
The 1st Time	48	47	65	42	40	34	29
The 2nd Time	0.7	0.7	0.8	0.1	0.2	0.0	0.0
The 3rd time	100	100	100	100	100	100	100
The 4th time	0.7	0.7	0.8	0.1	100	0.0	0.0
The 5th time	40	39	50	37	30	24	18

TABLE III. AVERAGE DELAY AFTER NETWORK REFORMATION (MS).

	To City Information Center HUAWEI 8512	To City Information Center East Computer Room cisco7609	To Songyang County cisco7606	To Yunhe County cicso7606	To Lishui City DNS	To Yunhe County DNS	To Normal PC
The 1st Time	12	9	15	2	3	1	11
The 2nd Time	13	12	15	1	3	1	11
The 3rd time	13	12	15	2	3	1	11
The 4th time	14	13	15	2	3	1	10
The 5th time	13	12	15	2	3	2	1750

TABLE IV. PACKET LOSS RATE AFTER NETWORK REFORMATION (%).

	To City Information Center HUAWEI 8512	To City Information Center East Computer Room cisco7609	To Songyang County cisco7606	To Yunhe County cicso7606	To Lishui City DNS	To Yunhe County DNS	To Normal PC
The 1st Time	0.6	0.7	0.8	0.1	0.2	0.0	0.0
The 2nd Time	0.7	0.8	0.8	0.1	0.2	0.0	0.0
The 3rd time	0.7	0.7	0.8	0.1	0.2	0.0	0.0
The 4th time	0.6	0.7	0.7	0.0	0.2	0.0	0.0
The 5th time	0.7	0.7	0.8	0.1	0.2	0.1	48