THE NETWORK SECURITY PROTECTION SYSTEM AT IHEP-NET

Lanxin Ma, IHEP, Beijing, China

Dehai An, Gang Chen, Baoxu Liu, Ruirong Liu, Chunzhen Wu, Rongsheng Xu, Chuansong Yu, IHEP, Beijing, China

Abstract

Recent years, the network security troubles have often occurred at IHEP. Network security at IHEP has been becoming one of the most important issues of computing environment. To protect its computing and network resources against attacks and viruses from outside of the institute, security measures to combat these are implemented. To enforce security policy the network infrastructure was re-configured to one intranet and two DMZ areas. New rules to control the access among Internet, intranet and DMZ areas are applied. All hosts at IHEP are divided into three types according to their security levels. Hosts of the first type are isolated in the institute and can just access the hosts inside of IHEP. The second type hosts access Internet through NAT. The third type hosts will directly connect to outside. An intrusion detection system works with firewall so that all packets from outside IHEP are checked and filtered. Access from outside will go through firewall or VPN. In order to prevent virus spread at IHEP and reduce the number of spam mail we installed a virus filter and spam filter system. All of these measures make the network at IHEP more secure. Attacks, virus and spam mails decrease dramatically.

INTRODUCTION

This paper describes our experience in practice of the current strategy and management in network security at IHEP-Net.

IHEP was the first institution connecting the computers to Internet in China at the beginning of 90s of the last century. In the past more than 10 years the IHEP-Net developed very quickly. Now the IHEP-Net outlet bandwidth is 10M. The IHEP intranet has a star structure with a main switch connected to each laboratory. Gigabit Ethernet is used as the IHEP-Net backbone. The bandwidth connected to each host is 100M. The main switch supporting Gigabit and Megabit is arranged in the computing center and a lot of switches or switching hubs are installed in each building.

Based on the requirement, big re-construction has been performed in IHEP-Net. The firewall system was reconfigured, and some new network security protection measures were introduced into our network, such as IDS, VPN system, anti-spam system, anti-virus system and the network control and management center etc.

WHY TO IMPROVE IHEP-NET SECURITY PROTECTION SYSTEM

Recent years, especially before 2002, the network security problems have often occurred at IHEP. The IHEP-Net were attacked from outside and inside. There were no anti-virus system and no anti-spam system at that time. The network security had been becoming one of the most important issues of computing environment at IHEP. At the end of 2001, IHEP computing center decided to organize the network security group to strengthen the policy and strategy against the attacks, virus spread and spam mails etc.

THE FIREWALL SYSTEM

Before reconstruction, the IHEP-Net were not secure since there was just a firewall system with some simple rules, which were not fit with the IHEP-Net security requirement. After we re-constructed the network infrastructure, the new IHEP-Net consists of three areas: one intranet, one DMZ and one special hosts area. We also re-configured the firewall system. Access among Internet, intranet, DMZ and special hosts area are controlled by firewall new rules. The current firewall system structure is shown in Fig.1. All hosts at IHEP-Net are divided into three types according to their security levels and are arranged in the intranet, DMZ and special area. The hosts of first type are isolated in IHEP-Net and can only access the hosts inside of IHEP-Net. The second type hosts can access Internet through NAT. The hosts outside of IHEP cannot access these hosts of the first type and the second type. The third type hosts can connect to outside directly. As a rule, the most of hosts that belong to the first type and the second type in IHEP-Net move to intranet, some servers and some special hosts are moved to DMZ and special hosts area. These hosts among DMZ, special host area and those hosts outside of IHEP can access each other according to some rules and protocols via opening some appointed ports at the Firewall. Firewall works well with IDS so that all of packages are checked and deny the attack from outside.

The equipments connecting each subnet consist of the main switch, some sub-switches and a lot of switching hubs. The hosts in intranet are moved to different groups according to their security levels so that the hosts inside each group have their own security protection rules. This function realized by their own capability of main switch

and sub-switches, so the security rules can be set up at each network interface of switches.

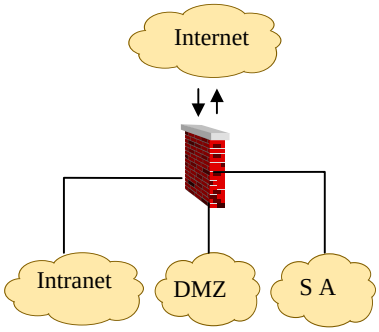

Figure 1: The IHEP-Net Firewall system structure

VPN AT IHEP

In order to access the hosts inside of IHEP-Net from outside the communication must be via FW or VPN, as Fig. 2 shows. Now we just support remote VPN access.

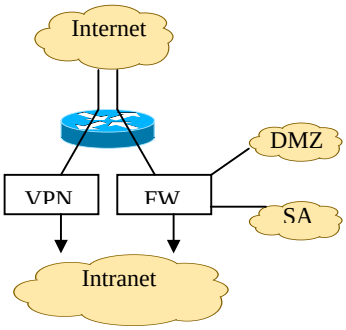

Figure 2: The secure IHEP-Net

The VPN server is located at the middle between router and intranet, and provides a service for hosts needed to access to hosts inside of IHEP-Net from outside. The VPN server handles PPTP as a tunneling protocol. The OS at clients can be Win2000/XP/2003/Linux.

Each VPN user has an VPN account and password. In order to strengthen the security of VPN system and manage strictly the VPN users usbkey hardware authentication is used. The driver for usbkey authentication needs to be installed at client. The interrelated software with usbkey authentication at client is installed at server. That means each VPN user must has a usbkey (the key to access IHEP-Net), and need to plug the usbkey in the USB hardware interface of the client's host so that the communication between the client and the VPN server become successful. The password for the authentication inside usbkey cannot be readable because of its hardware performance. Before the VPN user get the usbkey, the password inside usbkey had been memory at the VPN server.

The process of remote VPN access works as the following: when the VPN connection is started at client, a VPN remote-demand is issued to the VPN server, the authentication is performed. If the authentication is successful, an IP address of IHEP-Net is assigned to a client host and a virtual IP tunnel is established between the VPN server and a client host. But at this time the client host cannot connect to the hosts inside IHEP-Net yet because the second authentication (usbkey authentication) is required. The one-off other passwords are produced respectively at server and client at the same time, if the passwords at server and client are same, then the second authentication is accepted. Client host can access to the hosts inside IHEP-Net. Since the source address of packet is the IP address of IHEP-Net, it is able to receive the services as the IHEP-Net hosts. The VPN server at IHEP also have the capability filtering packet, so the access level for each VPN account can be control through the packet filtering rules for IP address.

THE ANTI-VIRUS SYSTEM

The anti-virus system at IHEP-Net was established since 2002, include the anti-virus system at gateway level and at desktop level.

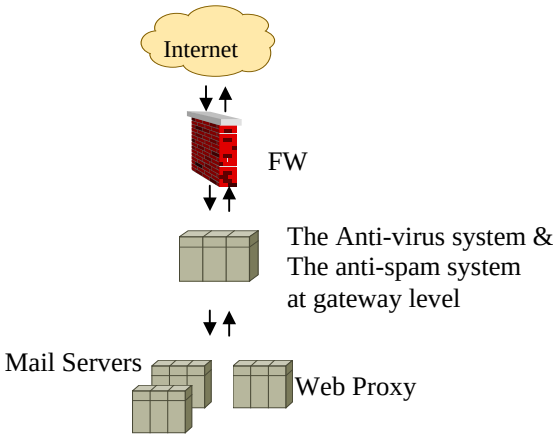

Figure 3: The anti-virus system and the anti-spam system

Fig. 3 shows the structure of the anti-virus system at gateway level. The commercial anti-virus software is used , which real-time detect and clean virus for all SMTP, HTTP and FTP traffic at gateway level. All emails sent and received must be filtered by this anti-virus system first. As long as using a web proxy while viewing webpage, the viruses for HTTP traffic can be detected and cleaned. In the same way, as long as using a file transfer proxy while transferring files, the viruses for FTP traffic can be detected and cleaned. This anti-virus system can act as a file transfer proxy itself.

After filtering virus by gateway anti-virus system, the most of viruses are detected, cleaned or quarantined to special directory. But some viruses also spread into the intranet by other way, for example floppy copy and CD copy etc. In this case, we also established the network version anti-virus system at desktop level, that is server

and clients structure for Window system. The agent needs to be installed at each client. The server downloads the latest scan engine and virus pattern files automatically per several hours from technique support website of anti-virus production enterprise. Then the Clients download the latest scan engine and virus pattern files from the server automatically per several hours. This desktop anti-virus system provides real-time detection and cleanup viruses at clients. The server manages and monitors all of the client hosts, collect and analyze the virus detection and cleanup reports from each client host.

THE MAIL SYSTEM

The spam mail troubles have often occurred at IHEP recent years. The old mail system connected to Internet directly, and it filtered spam just according to keywords and blacklist so that the effect filtering spam were not observable. Thus we have to improve our mail system. The new mail system structure is shown in Fig 3. The firewall provides the first level protection for mail system. The IP addresses that attack IHEP-Net are refused at firewall. We also established the anti-spam system at gateway level using commercial software. All emails sent and received are filtered by the anti-spam system at gateway level. The anti-spam gateway is the only host sending emails to outside and receiving emails from outside. It only opens SMTP port, closes other ports. And other mail servers are not allowed to communicate directly with Internet each other. There are three levels of filtering spam: low, middle, high. Normally we choose low level in order not lose emails.

Recent years, we also have troubles with virus mails at IHEP-Net. To take precaution against spam mail and virus mail at the same time, the anti-spam system works well with anti-virus system together so that all of emails are filtered by anti-spam system and anti-virus system. This makes it possible that the amount of spam email reached to users mail boxes are as low as possible and no virus mails reach to users mail boxes.

After filtering, spam mails received by users decrease greatly, the effect is significantly.

THE SECURITY CONTROL AND MANAGEMENT CENTER

Besides the protection measures mentioned above, we also have our own security control and management center. We use some home-made software to do the following: make statistics and analyze the network flux; real-time monitor and detect the hosts that have huge flux and give alert to the network manager; real-time monitor and find out the hosts that scan other hosts, give alert and analyze the reason; If the host is detected to have huge flux or scan others, it is disconnected to network automatically. For the host sending virus mails, disconnection from the host to mail server is performed automatically via refusing SMTP port so that the host cannot send virus mail any more until the host system works well. In the mean time the owner of the host is informed to install anti-virus software, to kill viruses and to patch the system etc.

SUMMARY

After improving the IHEP-Net security protection system, IHEP-Net becomes much more secure than before, since the communication from the hosts outside of IHEP to inside of IHEP must be through FW or VPN. The VPN becomes the main tool for the communication from outside to inside. Currently we support the remote access VPN and the support of the VPN connection among IHEP-Net has to be considered in the future. The effect in anti-spam and anti-virus is observable. Currently we just support spam filtering at gateway level and it also has to be considered that users can choose their own spam filtering level in the future.