Research on a New Type of Network Active Defense System Scheme

Xia Qing
Library
Huaihai Institute of Technology
Lianyungang, China
Email:xiaqing1@163.com

***Abstract*—At present, the focus of network security research mainly centers on the increase of detection ability of a single detection tool. For example, improve the accuracy and detection efficiency of firewall and intrusion detection system but despise the defense ability of the whole network system. This paper puts forward the concept of network active defense system and emphatically analyzes its architecture, working principle, software platform, hardware platform, and development platform and data packet acquisition mode.**

***Index Terms*—active defense; intrusion detection; data packet acquisition; software and hardware design**

I. INTRODUCTION

Along with the propulsion of information process in the world, computer network technology has been developed and popularized rapidly, followed by generalization, complication and frequency of hacker activities. The core of active defense is intrusion detection system and its auxiliary key system is trap network. This paper will put forward a new kind of network active defense system for solving hacker attacks and viruses and make a detailed analysis of its architecture and working principle.

II. ARCHITECTURE OF NETWORK ACTIVE DEFENSE SYSTEM

Network active defense system is a kind of active and positive system for guarding against and preventing network abnormal behaviors and it is deployed at the mirror port of network switch to monitor all data packets in the network, after it detects an abnormal behavior, it will actively link with the network switch based on a particular control interface and stop the network abnormal behavior and obstruct the attack source by closing physical ports, thereby preventing the network security threat spreading.

The architecture diagram of network active defense system (NAD system) is shown as Fig 1:

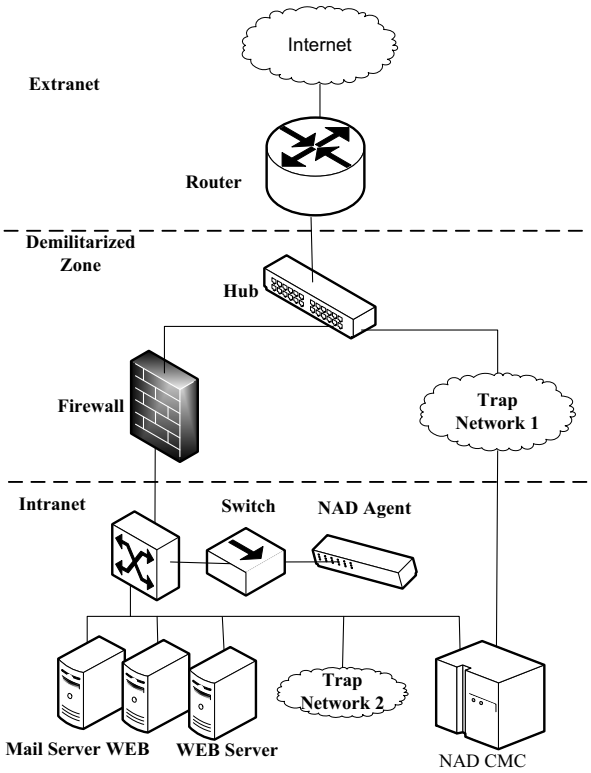

Fig. 1 Architecture Diagram of Network Active Defense System

NAD system is mainly composed of three parts, namely NAD CMC (Network Active Defense Control and Monitor Center), NAD agent and anti-virus agent, among which:

1. Monitor and control center (NAD CMC): It is deployed on the center switch, required to communicate with all monitor and control agents in the network, responsible for providing security administrators with a system control platform, making detection rules with broad-spectrum effect, receiving the rule updating from trap networks, updating monitor and control agent detection rules, managing and configuring monitor and control agents and system management functions, real-timely collecting the logs and alarms uploaded by monitor and control agents and finishing data statistics and analysis and report generation, print and output functions.

2. Monitor and control agent (NAD Agent): It is directly connected to and runs on the monitored network and can occur simultaneously and real-timely monitor multiple sub-

978-1-4244-4520-2/09/$25.00 ©2009 IEEE

networks, receive the commands from the monitor and control center and return the running results. Monitor and control agent itself is installation and maintenance free except for the most basic system configuration parameters and all operations are completed by the monitor and control center in the distance.

III. WORKING PRINCIPLE

This system is divided into two parts logically, namely acquisition of intrusion knowledge and use of intrusion knowledge. Trap networks are responsible for obtaining intrusion knowledge and NAD CMC and NAD agents are responsible for using intrusion to implement the defense of internal network.

Shown as Fig 2, set up trap network 1 in the extranet region and connect it with the hub, it is parallel with the firewall and can detect all data packets entering the intranet, excluding those data packets which can not enter the intranet and round the firewall. Trap network 1 is responsible for trapping the hacker viruses and attacks from external network, analyzing their properties and extracting detection features to update the rule database on NAD CMC. Set up trap network 2 in the intranet region and connect it with the backbone network and it is responsible for trapping the hacker viruses and attacks from internal network, analyzing their properties and extracting detection features to update the rule database on NAD CMC.

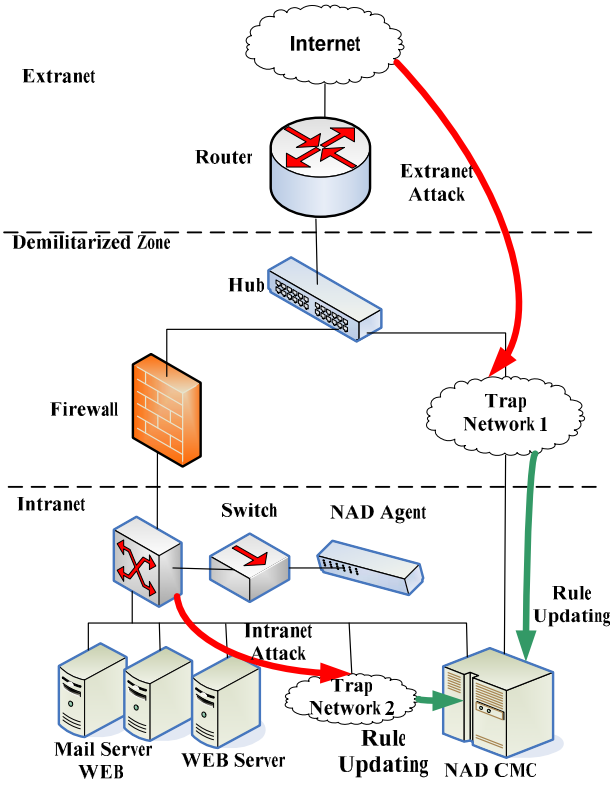

Fig. 2 Intrusion Knowledge Acquisition Diagram of Network Active Defense System

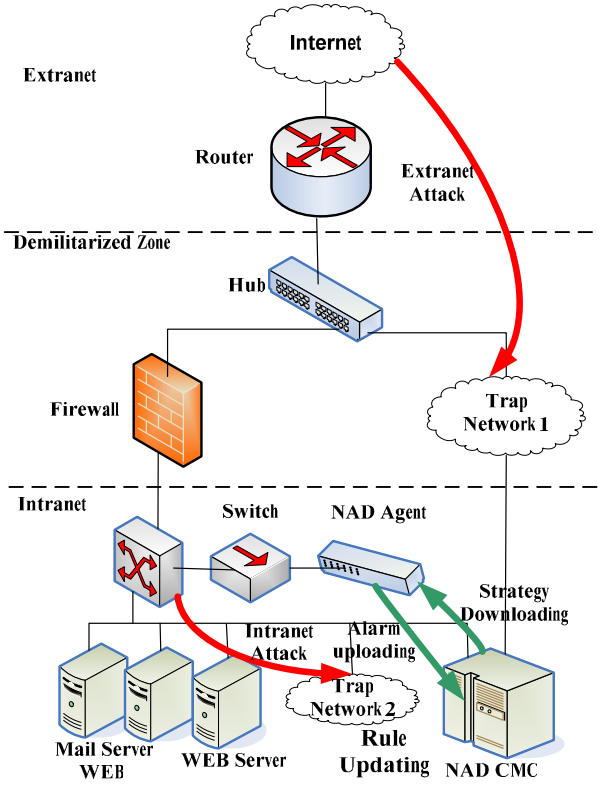

Fig. 3 Intrusion Knowledge Application Diagram of Network Active Defense System

Shown as Fig 3, NAD CMC is deployed on the center switch, after it finds that a new rule is generated, it will automatically download the new strategy in the rule database to NAD agents deployed in different sub-networks. NAD agents use the strategy received from NAD CMC to make a real-time detection of network flow and send alarm information to NAD CMC when an abnormality occurs. For the known alarm, NAD CMC directly intercepts the attack according to the predefined method; for the unknown alarm, NAD CMC submits a request for manual intervention and makes a final judgment to realize the detection of double-layer granularity.

In addition, network administrators can log in to NAD CMC in any place within the local area network (of course, security can also be improved by restricting the login hosts of administrators) and perform these operations on CMC management platform, such as other configurations of agent, real-time and historical network state check, suspicious host tracing, network fault removal and defective host isolation, etc.

The software structure diagram of NAD system is shown as Fig 4. NAD Agent receives and executes the strategy made by CMC, finishes the trapping and analysis of network data packets, records network state generation logs in detail, finds network abnormalities and produces alarms and completes log and alarm uploading through communication module. NAD CMC receives logs and alarms, writes them into the database and informs the administrator. If the

strategy blocks illegal hosts automatically, it is located to the physical port of access layer equipment automatically and closes the port, and meanwhile produces an operation log, which will be convenient for administrators to examine in the future.

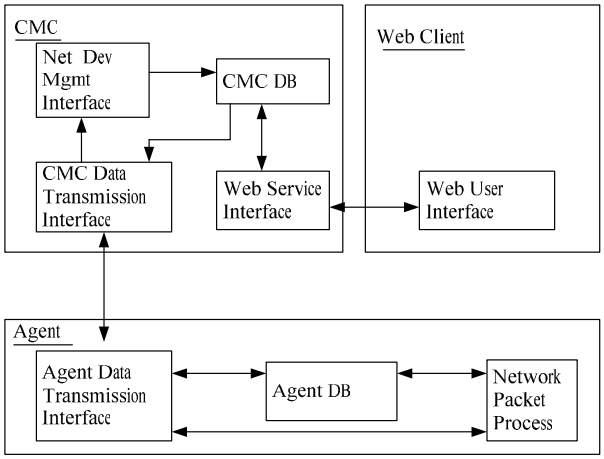

Fig. 4 Software Architecture Diagram of Network Active Defense System

IV. DESIGN OF SYSTEM SOFTWARE AND HARDWARE DEVELOPMENT PLATFORMS

A. Hardware design

The hardware of NAD system is composed of two parts, namely control and monitor agent and control and monitor center CMC; control and monitor agent selects a customized high reliability industrial computer and widely used NIC chips with mature technology and it can provide 2 to 4 monitoring ports according to the needs of application environment (number of concurrent monitoring sub-networks).

The handling and storage capacity of Agent machine is far lower than that of CMC machine, it is because that:

1. Agent machine monitors sub-networks and it is directly connected on the access layer switch, but at present, the transmission rates of most LAN access layer switches are 10/100Mbps and the maximum network utilization is about 80%. In such a case, the configuration of Agent machine is generally not very high.

2. CMC server needs to undertake multiple services simultaneously in NAD system, such as database service, Web service and data transmission service, etc, especially database service. NAD system needs to not only show users the real-time network state information but also store the historical data of network, convenient for examining in the future, so it requires that the handling and storage capacity of server should be strong enough.

B. Software design

1. Selection of running platform. We adopt Red Hat Linux Professional 9.0 (Kernel 2.4.0-18) on NAD Agent and Red Hat Enterprise Linux AS 4.0 (Kernel 2.6.9-5.EL) on NAD CMC.

2. Selection of database. We adopt MySQL5.0 on NAD Agent, it is open-source and stable and the data quantity on Agent is less, so using MySQL can be fully competent; adopt Oracle 9.2 on CMC, it has been accepted by vast users for its outstanding performance in handling mass data and using Oracle9.2 can construct database clusters conveniently, thereby ensuring that all working loads have maximum outputs. When it runs on a cluster, it balances working loads on available machines automatically to ensure the full use of hardware and using RAC (Real Application Clusters) can prevent application stopping. When a machine goes wrong or needs maintaining, application can continue the access to the data on another machine in the cluster and doesn't need to stop. Automatic data mirror, backup and recovery abilities can prevent data loss caused by general reasons and don't need expensive storage solutions. Powerful flashback query can check and restore the data of earlier editions easily and doesn't need to perform complex and time-consuming recovery operation.

C. System development platform

1. ACE (Adaptive Communication Environment). ACE is a free-usable, open-source and object-oriented framework which realizes many core modes used for concurrent communication software. ACE provides a group of rich reusable wrapper facades and frame components and it can cross many kinds of platforms to finish universal communication software tasks, including event demultiplexing, event processor assignment, signal processing, service initialization, interprocess communication, shared memory management, message routing, distributed service dynamic configuration (reconfiguration) and concurrent execution and synchronization, etc.

2. Libpcap. It is a function library trapped by the network data packets under Unix/Linux platform and a lot of network monitoring software is based on it, such as famous TCPDUMP and SNORT.

3. Libnet. It provides a series of interface functions and realizes and encapsulates the constructing and sending process of data packets. We can use it to construct the data packet heads of protocols of various layers from application layer to link layer in person and combine these packet heads with valid data together in an orderly manner to send.

D. Network data packet acquisition mode

Network data packet acquisition mode includes network equipment (switch, etc) mirror, TAP (Test Access Port) and NetFlow, etc.

TABLE 1 COMPARISON TABLE OF NETWORK DATA PACKET ACQUISITION MODES

	Network equipment mirror	TAP	NetFlow
Content of data packet	Original network data packet	Original network	(iflndex) It provides source address,

		data packet	destination address, source port, destination port, protocol type, service type and network equipment input interface (iflndex) of data packet
Scope of application	All network equipment supporting mirror image	Apply to all networks	Cisco、Enterasys、Extreme、Foundry、Juniper At present, it supports these manufacturers: Cisco, Enterasys, Extreme, Foundry and Juniper
Monitoring range	All data packets of network equipment	Can only monitor the in and out data packets on the equipment connecting with TAP	All data packet information of network equipment
Influence on the network	Little	Great influence when deploying and little influence after deployment	Little
Deployment difficulty	Small	Small	Small
Deployment expense	Small. It only needs to be configured on the original network equipment	Relatively large, it is mainly because that the newly-added TAP equipment is expensive	Small

NAD system adopts network equipment mirror mode to carry out network data packet acquisition, it is mainly because NAD system needs to trap all types of data packets of network equipment in the local area network (monitor intranet host scan, intranet video on demand and BT download service, etc), all types of data packets of local area network and extranet (monitor the utilization of the whole network, etc) and NetFlow, etc, other acquisition modes can not meet system requirements, and in order to get the minimum monitoring granularity, NAD system needs to monitor the data of access layer switch at the bottom; TAP can not be competent.

V. CONCLUSION

Aimed at unknown attacks, such as hacker virus, etc, this paper puts forward a network active defense system and establishes a whole network active defense system taking trap network as intrusion knowledge acquisition platform and network active defense CMC and agent as intrusion knowledge use. The emergence of this system makes up for the deficiencies of passive defense system in the field of safety protection and effectively resists the intrusion of unknown viruses and attacks.

REFERENCES

[1] John D Howard, An analysis of security incident on the internet, Camege Mellon University, West Lafayette.USA, 1997

[2] Edward G Amoroso, Fundamentals of Computer Security Technology Prentice-Hall PTR, 1994, p67-97

[3] Oracle Corporation.Oracle9i Real Application Clusters [EB/OL] 2002-08). [2006-04]

[4] Steven Mcanne, Van Jacobson, The BSD Packet Filter: A New Architecture for User-level Packet Capture [A].In proceeding of the 1993 Winter USENIX Technical Conference[C], January 1993,San Diego, CA, 259-269.

[5] S. Forrest, A Perelson, L Allen, and R Cherukuri, "Self-nonself discrimination in a computer" in Proc IEEE Symp Research in Security and Privacy, May 1994, 202-212

[6] Yiming Gong, Detecting Worms and Abnormal Activities with Netflow, Part12004-08-16, 132-145