

## The New Exploring for the Key Technology of Distributed Network Security System Design

Honghui GONG<sup>1, a</sup>, Yanwei XU<sup>2</sup>, Ting ZHANG<sup>3</sup>

<sup>1,2,3</sup> Jiangxi Police College, Nanchang 330200, China

<sup>a</sup>gonghonghui@126.com

**Keywords:** Distributed Network; Security System; Security Management

**Abstract.** With the rapid development of Internet, the computer network is gradually becoming a country's economic development foundation and lifeblood of the world dependent on the network is also growing, network security issues attendant becomes increasingly prominent. Network security infrastructure Laboratory, University of Electronic Science and Technology is in this context, to begin related research network security. In this paper, the network information system to conduct a comprehensive monitoring and tracking of online behavior of security auditing technology, developed in line with the audit information security management tools needed to provide technical support for the construction of network security information systems, and on the basis of technical studies on research to develop technical standards and can have independent intellectual property rights and international standards to improve the domestic information network defense capabilities to protect the security of computer information systems.

### Introduction

With the rapid development of computer networks, network security issues are also increasingly attracted attention. Firewall as an effective security measures which are widely used in various types of networks. However, the traditional firewall technology within the network security based on assumptions and assume a single access point, there is a limited scope of defense, rely on the network topology, easy to form a single point of failure and traffic bottlenecks and other issues, a new type of distributed firewall technology is the solution Potential research these issues. Policy distribution in a distributed environment is one of the key technologies of distributed firewall, which mainly involve security protection technology of distributed object technology and strategy. Since traditional distributed object technology for Intranet environments, it is difficult to communicate through a firewall problem extended to the Internet environment [1-3].

This paper describes the definition of network security analysis of network security threats, objectives, introduces the network security architecture and key network security technologies, review the firewall technology and intrusion detection technologies, including off-line structure, internal classification, the main strengths and weaknesses and the future direction of development. On the basis of in-depth study of network security above, we propose a distributed network security architecture,

### Distributed safety critical

Distributed firewall, the firewall best configuration for the different needs of each server and the terminal computer, can fully take into account when configuring the applications running on these hosts, so then under the premise of ensuring network security, greatly improve network operating efficiencies. Due to the distributed firewall distributed across the enterprise network or server, so it has unlimited scalability [4]. With the growth of the network, they are the network processing load further distribution, so they can continue to maintain high performance. Distributed network security technology includes both the traditional firewall technology, also based on this application a number of security technologies.

Bag filter data filter bag can control the site and the site, the site of mutual visits between the network, network and network. Through packet filtering firewall to intercept and inspect all

outbound and inbound data. Firewall packet filtering module first verifies whether the packet filtering rules, regardless of whether filtering rules, the firewall log packets generally the case, the package does not conform to the rules of an alarm or notify the security administrator [5].

**State detection.** State detection technology uses a state detection mechanism is based on the connection, all packets belonging to the same connection as a whole look at the data stream to form the connection state table, rule table through joint cooperation with the state table, on the table individual connection status factors be identified. Dynamic connection status table can be previously recorded communications information, the information may also be other associated applications.

**NAT (Network Address Translation).** NAT technology can be used to create an external private network transparent to the user. NAT can solve the labor problem P address is not enough, while hiding the internal network address labor P. Such external network to the user in terms of the private network is transparent, it does not exist, can prevent internal network structure is stolen, reducing the possibility of being attacked from the internal network to a certain extent, improve the security of a private network.

**IPSec.** IPSec is an open standard protocol for secondary safety developed by the IETF, which is based on IP networks (including Intranet, Extranet and Internet), is a combination of multiple security protocols a more complete security protocol packets together to form. It supports secure transmission of IP information through the public network in the third layer (network layer) OSI model provides encryption, authentication, authorization, and management. IPSec provides for application-transparent encryption services for IP network traffic, define a set of data transfer for authentication, protection of privacy and the integrity of the standard protocols, and through three different forms to protect.

**Authentication.** In a distributed computing environment, users need to access the network at different locations on the service. Usually in order to protect the security of its own resources, service providers need to restrict user access to authorized resources. The user authorization and access restriction policy is based on the identification of customer service requests on. That is, the user's service request or by the users themselves must identify or authenticate, Diao one can access the service provided by the server.

**Agent.** Agent is a proactive entity having an information processing capability, under certain circumstances can perceive the environment, and can run autonomously to represent its designer or user to achieve a series of goals computing entities or programs. It changes with the environment to adjust themselves, with a view to changing environments can still achieve results consistent with the environment.

## **Distributed Network Security Architecture**

UDP, and ICMP packet itself is not connected to the state information, connection state table is stored in a pseudo-connection information. For both of these packages to find the corresponding record as long as the connection table, you can forward the packet without further state inspection guillotine. TCP packet itself presence status information, for a state or BR RST packets will be discarded, other packages will be released. Further TCP connections also need to change the status of the connection state table based on the type of connection that received the packet, so that the connection status table can be maintained (deletion of expired timeout connection). Next, the TCP connection state transitions realization were analyzed. Input parameters of the TCP connection state transitions needed include: direction (active or passive initiator connection responder) package, the package itself, type and status of the current connection is in. According to TCP state transition diagram, distributed network security management workflow shown in Figure 1.

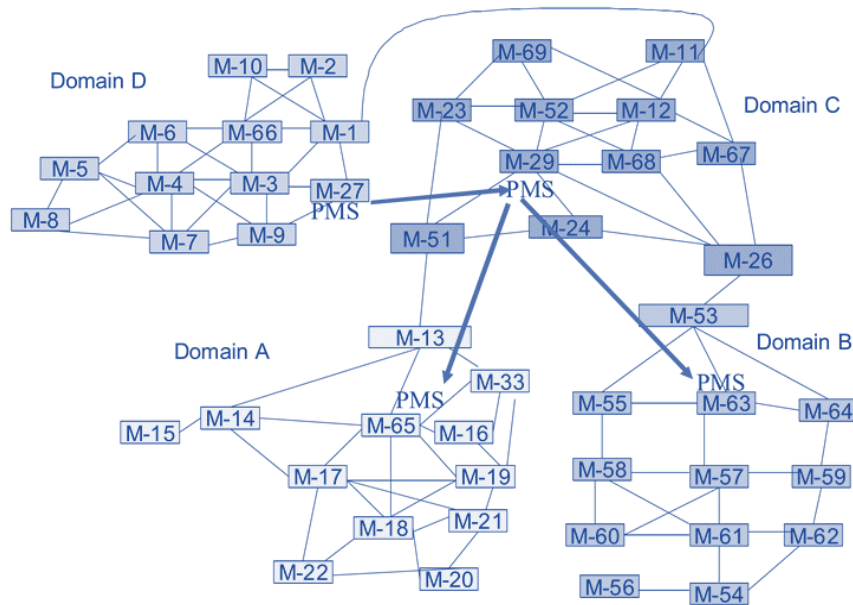


Figure 1. Distributed Security Workflow

Through in-depth research on network security technology, this paper presents a distributed network security architecture, this architecture combines the concept of a firewall and intrusion detection, and joined the distributed concept. This architecture with policy management as the core, the network is deployed at the network edge both central firewall, but also located at the end of the host firewall systems, while also providing intrusion detection system (IDS) and other security means, through various safety components Policy Server unified, collaborative work. To be able to dynamically adapt to changes in the network's security status, contained in the audit server architecture, through the firewall and IDS logs audit events for the development of policies, provide the basis for distribution. An overall view of a distributed security architecture shown in Figure 2.

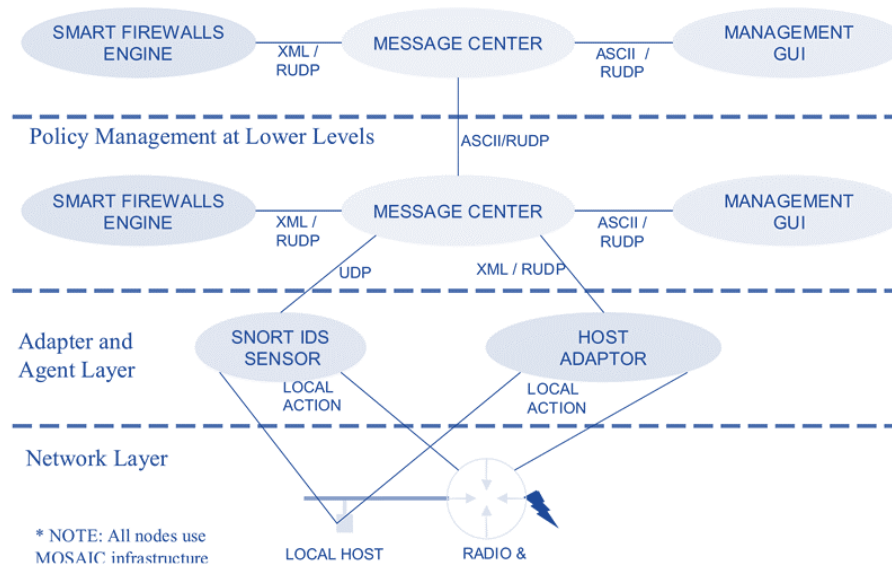


Figure 2. Overall architecture of distributed security

To accommodate large-scale distributed network security needs to be protected, the system uses a hierarchical architecture to implement a security policy management, and in accordance with the coverage of security protection (safety zone) security policy management is divided into three levels: core-level, regional level and subnet level. Core-level managers responsible for formulating policy and regularly distribute security policies (Global Security Policy) the entire security zone to regional-level policy manager; regional-level policy manager combined global security policies and security features of the region to develop regional-level security policy (Regional security policy), regional security policy is sent to the policy server for each subnet within the region (PS), the guide

PS safety components subnet configuration and coordination. Hierarchical architecture makes safety systems to be deployed in large-scale network, suitable for mobile device security management. When the device is in the same area of different subnets move, move back and forth subnet PS through regional-level policy management can interact security policies, mobile devices in the field can also enjoy similar network in the local network security. When the device generating movement across the region, to help complete the interactive security policy through the core level of the Policy Manager.

### Architecture of the distributed security management platform

Distributed network security system, the firewall best configuration for the different needs of each server and the terminal computer, can fully take into account when configuring the applications running on these hosts, so then under the premise of ensuring network security, greatly improve network operation effectiveness. Due to the distributed firewall distributed across the enterprise network or server, so it has unlimited scalability. With the growth of the network, they are the network processing load further distribution, so they can continue to maintain high performance. Hybrid network security management platform must be able to implement remote, multi-user, hierarchical management, and to ensure the security of the entire platform system. For the above demand, the network security management platform designed as a network remote management system, take the server and client mode, shown in Figure 3.

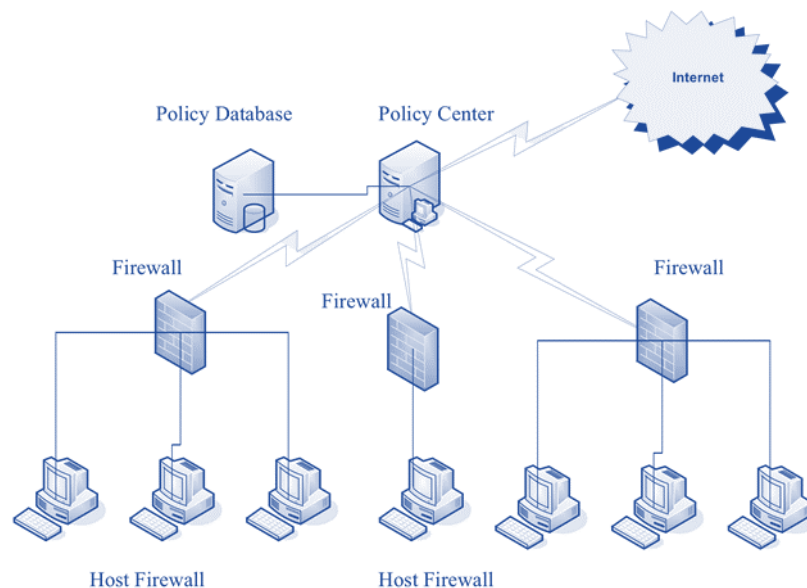


Figure 3. Architecture of the distributed security management platform

Network is not a network device which consists of a static superposition, it is an organic whole. A variety of devices in the network is the skeleton of the entire network, and a variety of information network runtime constitute the pulse of the network. Network security information is generated by the network in a variety of safety equipment, it reflects the current state of a running network administrator to manage network, develop strategies, based primarily on the deployment of equipment, but also an important manifestation of the aspects of the current network security. Therefore, when the network security management, it is necessary to manage a variety of network security hardware devices, but also collect a variety of security information generated by these security devices runtime, and associated management. Network security information relating to the contents of multiple aspects in the management of major risk management function should possess, security policy management and early warning alarm.

## Conclusion

With the development of the Internet economy and the Internet age, the computer network security has attracted common concern around the world, while the booming computer networks, also faces enormous challenges. Faced with the challenges of network security, how to practice some degree of in-depth study of the real problem at the same time, the significance of research for network security is obvious. The research network security connotation and related technologies, and gives a distributed network security architecture, network security this topic in-depth research and development, a number of areas for a more in-depth research, and a targeted practice, laying a good foundation for future research and has some innovative and actionable.

## Reference

- [1] Sridhar S, Hahn A, Govindarasu M. Cyber-physical system security for the electric power grid[J]. Proceedings of the IEEE, 2012, 100(1): 210-224.
- [2] Kahate A. Cryptography and network security[M]. Tata McGraw-Hill Education, 2013.
- [3] Manshaei M H, Zhu Q, Alpcan T, et al. Game theory meets network security and privacy[J]. ACM Computing Surveys (CSUR), 2013, 45(3): 25.
- [4] Mo Y, Kim T H J, Brancik K, et al. Cyber-physical security of a smart grid infrastructure[J]. Proceedings of the IEEE, 2012, 100(1): 195-209.
- [5] Yan Y, Qian Y, Sharif H, et al. A survey on cyber security for smart grid communications[J]. Communications Surveys & Tutorials, IEEE, 2012, 14(4): 998-1010.
- [6] Güngör V C, Sahin D, Kocak T, et al. Smart grid technologies: communication technologies and standards[J]. Industrial informatics, IEEE transactions on, 2011, 7(4): 529-539.