2010 3rd International Conference on Computer and Electrical Engineering (ICCEE 2010)
IPCSIT vol. 53 (2012) © (2012) IACSIT Press, Singapore
DOI: 10.7763/IPCSIT.2012.V53.No.2.30

Network Security and Firewall Technology

Lily Dong[+] and Yuanzhen Peng

Computer Science Department , Yangtze University

Jingzhou, China

Abstract—Along with the Internet rapidly expand, the network security problem is day by day serious, the network security technology is also taken by the people. The solution network security problem's important means are the firewall technology. This article mainly introduced based on predecessor's theoretical knowledge and the method in the firewall technology, then has outlined the firewall technology classification and the major technique characteristic, finally collected some material which the firewall conceived to summarize its trend of development. This article biggest luminescent spot mainly will be the firewall technology future trend of development.

Keywords- Network security; Firewall technology; Network;

Along with the computer application scope's expansion and computer network's swift development, the computer information technology unceasing change people's work, the study and the life, cause people's working efficiency are greatly the enhancement the information resource obtain greatest degree sharing. But must see that follows closely the network security problem which the information technology the development brings to highlight day after day, if not solves this problem well, will certainly to hinder the computer network development the advancement.

1. Outline

The network security is refers to network system's hardware, the software and system's data receives the protection, not is exposed the destruction because of accidental or the malicious reason, the change, divulging, the system moves normally reliably continuously, the network service does not interrupt. The network security says from its essence is in the network information security. From generalized, everything involves to the network in the information secrecy, the integrity, the usability, the authenticity and the controllability correlation technique and the theory is the network security research area. The network security is one involves the computer science, the networking, the communication, the password technology, the information security technology, the applied mathematics, the theory of numbers, the information theory of numbers, the information theory and so on many kinds of discipline comprehensive disciplines.

The network already through many network tools, the equipment and the strategy protects the network which cannot be trusted, the firewall technology is the utilization is widespread and the effect is best. The network firewall technology is one kind uses for to strengthen between the network the access control, prevents the exterior network user to enter the internal network by the unlawful means through the exterior network, visits the internal network resource, protects the internal network operating environment the special network interconnection equipment. It the data packet like link way which transmits to two or the many networks between according to certain security policy implements the inspection, decided that between network correspondence whether to be permitted, and monitors the network running status.

[+] Corresponding author.
E-mail address: dll61092739@tom.com

2. Firewall technology

At present, the existing firewall mainly has: Package of filtration, agent server, multi-skill as well as other types (double host main engine, main engine filtration as well as encryptions router) firewall.

2.1. Package of filtration firewall

The package of filtration firewall is with a software examined flows through data packet's Baotou (Header), decides the entire package's destiny from this. It will possibly decide that discarding (Drop) this package, will possibly accept (Accept) this package (to let this package through), also will possibly carry out other complex movements.

A package of filtration is one kind built-in above the Linux essence routing function firewall type, its firewall work in network level. Under the Linux system, wraps the filtration function is in constructs in the core (takes a nucleus module, or direct in constructs), meanwhile has some may utilize above the data packet the skill, but most commonly used is still examined that Baotou decides a package of destiny. The package of filtration firewall the package which will receive to each will make the permission or the rejection decision. Specifically speaking, it in view of each data newspaper's masthead, carries on the determination according to the package of filtration rule, matches the package with the rule to continue based on the routing information to retransmit, otherwise discards. A package of filtration is realizes in the IP level, includes the filtration according to the data packet source IP address, the goal IP address, the agreement type (the TCP package, the UDP package, the ICMP package), Baotou information and so on source port, goal port information and so on data packet direction of transmission judges whether to allow the data packet to pass. A package of filtration also includes with the service related filtration, this is refers to based on the specific service luggage filtration, because the overwhelming majority service's monitor is resident in the specific TCP/UDP port, therefore, to block all enters the specific service the link, the firewall only need possess contains specific TCP/UDP goal port's package discarding then.

2.2. Agent server firewall

The agent server firewall is the work in the OSI model application layer, it grasps in the application system to be possible to serve as the security decision-making the complete information, therefore, the agent server firewall is called the application layer gateway, this kind of firewall (Proxy) the technology participation through one kind of agent to a TCP connection entire process. The data packet which sends out after the intranet user undergoes such firewall processing, probably is stems from the firewall exterior network card to be the same, thus may achieve the hideaway intranet structure the function. The agent server firewall through moves the proxy service routine on the main engine, carries on the service directly to the specific application layer, therefore is also called the application firewall, its core is the movement on the firewall main engine's agent server advancement.

The so-called agent server, is refers to represent customer processing in the server connection request procedure. When the agent server obtains a customer connection intention, carries on the checking to the customer request, and requested after the specific security's proxy application program processing connection, after will process the request transmits on the true Internet server, then accepts the server reply. The agent server does after the genuine server's reply further processes, will answer that gives sends out the request the final customer, the agent server usual movement between two networks, it regarding the customer is a real server likely, but regarding the exterior net's server, it resembles a client. The agent server user's overall network requested by no means submits for Internet on the genuine server, but first rests on the safety precaution and user's request makes the judgment, whether to act carries out this request, some requests are possibly overruled. After the user has supplied the correct user status and the authentication information, the agent server establishment with the exterior Internet server's connection, is two correspondence spots acts as relaying. The internal network only receives the request which the agent server proposed, rejects the exterior network the direct request. The agent server principle of work schematic drawing like chart shows.

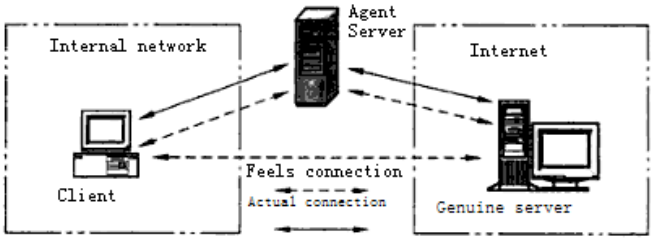

Fig.1. The agent server principle of work schematic drawing

2.3. Multi-skill firewall

In view of a higher secure request, some firewall manufacturer based on data packet filtration technology (Packet Filter) method and based on proxy service technology (Proxy Service) the method unifies, is also unifies the data packet filtration firewall product and the agent server firewall product, forms the new multi-skill firewall product. This kind of multi-skill firewall usually has two kinds of plans: One kind is shields the main engine firewall (Screened Host Firewall, SHF); Other kind is shields the subnet firewall (Screened Sub-Net Firewall, SSNF).

2.4. Other types (double host main engine, main engine filtration as well as encryption router) firewall

Each kind of firewall router and each kind of main engine may compose each type according to its disposition and the function the firewall, including: The double host main engine firewall (Dual-Homed Host Firewall), it is acts as the gateway by the fortress main engine, and moves the firewall software in above, between the inside and outside net's correspondence must pass through the fortress main engine; The main engine filtration firewall (Screened Host Firewall) is refers to a package filtration router to be connected with the exterior net, simultaneously, a fortress main engine installs on the intranet, causes the fortress main engine to become the only node which the exterior net can arrive, thus guarantees the intranet not the exterior non-authorization user's attack; The encryption router (Encryption Router), the encryption router to carries on the encryption and the compression through the router information flow, then transmits the goal end through the exterior network to carry on the solution compression and the decipher.

3. Firewall's trend of development

Along with the new network attack's appearance, the firewall technology also has some recent trend of development. This mainly may from wrap the filtration technology, the firewall architecture and the firewall system administration three aspects manifests.

3.1. Firewall package of filtration technological development tendency

1) Some firewall manufacturer the utilization user authentication and the service expands on the AAA system to the firewall, enables it to have may support based on the user role security policy function. This function is essential in the wireless network application. Has the user identification authentication firewall usually is uses the application level gateway technology, wraps the filtration technology the firewall not to have. The user identification authentication function is stronger, its security rank is higher, but it gives the negative influence which the network service brings to be also bigger, because the user identification authentication requires the time, specially encryption user identification authentication.

2) Multistage filtration technologies. The so-called multistage filtration technology, is refers to the firewall to use the multistage filtration measures, and auxiliary distinguishes the method. In grouping filtration (network level) first-level, filters all source route grouping and the counterfeit IP source address; In transmission level first-level, follows the filtration rule, filters agreement which and harmful data packet like nuke package, Christmas tree package all forbids or/and enters and so on; In using gateway (application layer) first-level, can use FTP, SMTP and so on each kind of gateway, controls and monitors Internet to provide uses to serve general. This was aims at the above each kind to have one kind of synthesis filtration technology which the firewall technology's insufficiency produced, above it might make up each kind to filter technical alone the insufficiency. This kind of filtration technology is clear in the lamination, each kind of filtration technology corresponds to the different network level, embarks from this concept, also

has many contents to be possible to expand, will build the foundation for future firewall technological development.

3) Enable the firewall to have the viral protection function. Was called now usually that it " the viral firewall ", mainly manifests certainly at present in individual firewall, because it is the pure software form, easier to realize. This kind of firewall technology may prevent virus's in network dissemination effectively, is more positive than the waiting attack's occurrence. Has the viral protection function firewall to be possible to reduce company's loss greatly.

3.2. Firewall's architecture trend of development

Along with network application's increase, set a higher request to the network band width. This means the firewall to be able by the very high speed processing data. Moreover, in the later several years, the multimedia applications will be getting more and more widely, it will request the data to pass through the detention which the firewall will bring to be young enough. In order to meet this kind of needs, some firewall manufacturer has developed based on the ASIC firewall and based on the network processor's firewall. From carries out the speed angle to look like, based on the network processor's firewall is also based on software's solution, it needs to rely on to a great extent software's performance, but because in this kind of firewall has some to use in processing the data stratification plane duty specially the engine, thus lightened the CPU burden, this kind of firewall's performance must compared to the traditional firewall's performance good many.

3.3. Firewall's system administration trend of development

Firewall's system administration also has some trend of development, mainly manifests in the following several aspects:

4) First is the central management, distributional and the lamination safety mechanism will be future tendency. The central management may reduce the managed cost, and guarantees in the large-scale network the security policy uniformity. The fast response and the fast defense also request to use the central management system management system. At present this kind of distributional firewall already in Cisco (Cisco), 3Com and so on the big network equipment developer develops successfully, is also "the distributional firewall which" present called and "the embedded firewall".

5) Formidable audit function and automatic diary analysis function. These two spot application may discover early the latent threat and prevents the attack the occurrence. The journal function may also the manager discover effectively in the system saves the security crack, adjusts the security policy and so on various aspects to manage promptly has the very big help. However has this kind of function firewall usually is quite high-level, the early static package of filtration firewall does not have.

6) Network security product systematization

Along with the network security technology's development, has one formulation now, the named "the establishment take the firewall as the core network security system". Because we discovered in the reality, the existing firewall technology meets the current network security need with difficulty. Through establishes one take the firewall as the core security system, may for the interior network system deployment multi-channel security defense line, each kind of safety work perform its own functions, defends the external invasion from various aspects.

4. Concluding remark

Certainly, the firewall itself also has its limitation, namely does not undergo firewall's invasion, the firewall is helpless, if is protected in the network through SLIP and the PPP way directly with the Internet connected internal user, will then create the safe hidden danger. This time, to guarantee the security, the firewall agent server when uses ISP SLIP and the PPP connection, needs to attach some new jurisdiction condition. At the same time, hardware way construction firewall, for example: PIX 520, it insufficiently nimble question also solidifies firewall's common question, therefore in an actual network movement environment, depends upon the firewall to guarantee that merely the network the security is insufficient obviously, this time, should act according to the physical demand to adopt the corresponding security policy.

5. References

[1] Yu Qiu,Internet network security and firewall technology discussion,Mianyang Normal school journal ,2004,23(5),31～35.

[2] Canghong Zhang, Based on nework security firewall technology,Information technology,Chinese new technology new product, 2009,19,29～30.

[3] Yongqiang Gao,Shize Guo,and soon, Network security technology and application grand ceremony, Beijing, people's posts and telecommunications publishing house, 2003

[4] Zhijun Huang.Ai Zhao. Hongxian Xu, Network security and firewall technology, Naval engineering college newspaper, 2002,14（1）,51～53

[5] Guoqin Lin, Brief analysis computer network security and firewall technology, Enshi professional technology institute journal(composite plate), 2007,19(1),69~71.

[6] Wei Huang, Intelligent firewall technology discussion, network security technology and application, 2009,10,29~31

[7] Rui Wang. Haibo Lin, Network security and firewall technology, Tsinghua university publishing house, in 2000

[8] Kuang Chu,network security and firewall technology, Chongqing university publishing house,2005

[9] Lafei(US),Network security, People's posts and telecommunications publishing house, 2008

[10] Fang Zhao . Yulei Ma,network security firewall technology brief analysis, technical information.2010,3.