Secure communication in the computer network

Ing. Boris MATEJ[1]

[1] Department of Informatics
Armed Forces Academy of gen. M. R. Štefánik
Liptovský Mikuláš, Slovakia
boris.matej@aos.sk

Abstract: Network security plays important role in today's digital world. The most services and applications require online access and operate on multi-user and multi-device network. This makes intensive demands on security to prevent possibly dangerous issues in shared network environment. Mobile networking and web services make this situation even more complicated. There are many different solutions out there used in comprehensive combinations to pursue the same objective - safe and secure communication over the network. Firewall technology is one of the technologies used in today's networks to ensure significant level of network security. Basic firewall principles are implemented in many different ways to achieve the best results. This paper deals with basic classification of firewalls and outline main characteristic of selected classes of firewalls. It presents software and hardware solutions with different approaches to the subject. It also suggests appropriate fields for applications in selected classes of firewalls. All presented facts render firewalls as definitely not obsolete concept.

Keywords: firewall, packet filter, application gateway, proxy firewall, IDS, IPS, security policy

1. Introduction

Security has always been one of the most important aspects of the network. As security deployments become more complicated with addition of mobile connectivity and web services, enterprises are looking for comprehensive answers.

Firewalls are used to examine network traffic and enforce policies based on instructions contained within the firewall's rule set. Firewalls represent one component of strategy to combat malicious activities and assaults on computing resources and network-accessible information. Other components include, but are not limited to, antivirus software, intrusion detection software, patch management, strong passwords passphrases, and spyware detection utilities.

2. Firewall Classification

The way a firewall provides greater protection relies on the firewall itself, and on the policies that are configured on it. Basic classification divides firewalls into hardware and software firewalls. Detailed classification of firewalls is possible on the basis of their activities into packet filters, application gateways, stateful or dynamic packet filters, stateful packet filters with protocols control, IDS (Intrusion Detection Systems) and IPS (Intrusion Prevention Systems).

2.1 Hardware Firewall

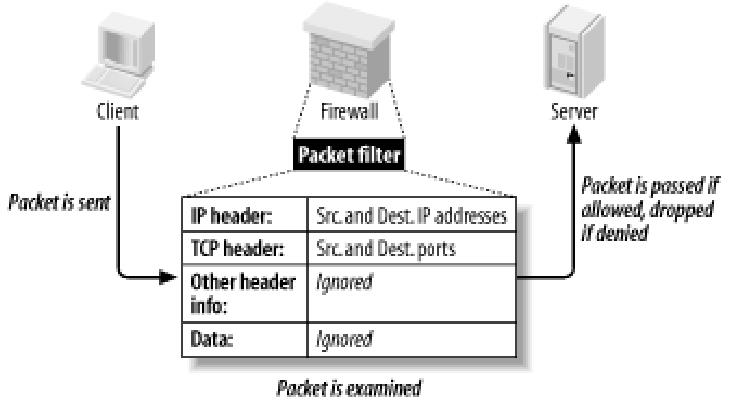
A hardware firewall is preferred when a firewall is required on more than one machine. Hardware firewall provides an additional layer of security to the physical network. The disadvantage of this approach is that if one firewall is compromised, all the machines that it serves are vulnerable.

2.2 Software Firewall

A software firewall is a second layer of security and secures the network from malware, worms and viruses, and email attachments. It looks like any other program and can be customized based on network requirements. Software firewall can be customized to include antivirus programs and to block sites and images.

2.3 Packet filters

Packet filters are the oldest and simplest form of firewalls. Their activity, an exact definition of the rules, in which what is defined by the address and port of the packet can be forwarded in which the address and port. Packet filter monitors each incoming and outgoing packet, decodes the packet header and then stops it or released it.[1] Packet filter inspection is performed on the third (network) and fourth (transport) layer of the OSI model.[4]



IP header:	Src.and Dest. IP addresses
TCP header:	Src.and Dest. ports
Other header info:	Ignored
Data:	Ignored

Fig. 1. Example of the Packet filter

The advantage of this solution is the high speed communication analysis, so even today are still used in networks that do not require high accuracy or in-depth analysis of ongoing communication, but it is a high-speed communications with large data volumes. Disadvantage of this solution is the low level of control ongoing communication that especially in more complex protocols (FTP - File Transfer Protocol, audio / video streaming, RPC - Remote Procedure Call, etc.) require to open and use the ports and the direction of the link, which can be used by other protocols that may pose a security risk.

Typical packet filters include, for example ACL (Access Control List) in older versions of IOS operating system used in Cisco firewalls or „ipchains“ firewall used in the older versions of Linux kernel.[3]

2.4 Application gateway

Application gateway or proxy firewalls also in contrast to the packet filter completely separated from each other communicating network between which they are located. All communication passes through the gateway application as two. The first is the connection between the client that initiates communication and proxy firewall. Proxy firewall client request process and opens a new connection to the server that the client be served by request. The data, which in turn receives from the proxy firewall server before the client. Checking application gateway takes place on the seventh (application) layer of the OSI model. [4]

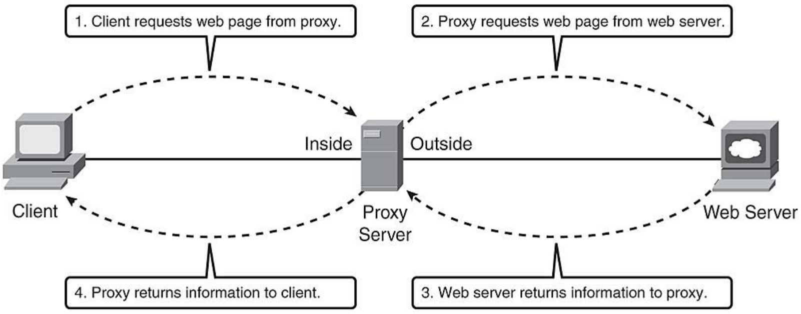

1. Client requests web page from proxy.
2. Proxy requests web page from web server.
Inside
Outside
Client
Proxy Server
Web Server
4. Proxy returns information to client.
3. Web server returns information to proxy.

Fig. 2. Example of Proxy firewall

The advantage of this solution is the relatively high security. Disadvantage of this solution is the high demands on the hardware. Application gateways are capable of processing only a small amount of ongoing communications over packet filters with greater latency. Each protocol requires write their own proxy or use a generic proxy, which are not safer compared to using packet filter. Most of the original application gateways were therefore able to control several protocols, usually ten. Additionally failed quite well to protect your operating system and client knowledge required to communicate with the application gateway. These deficiencies have been phased out, but after the introduction of state packet filter, the development of most application gateway gradually stopped and today is no longer only used in very specific cases.

Typical applications include, for example, The Gateway Firewall Toolkit (fwtk) and it inspires TIS Gauntlet company, later purchased by NAI.

2.5 Stateful or Dynamic packet filters

Stateful packet filter acts like a simple packet filter, however, additionally store information on approval of concentration that can be used when deciding whether outgoing packets belong to permitted connections and will be released through the filter or have to go through the decision process. It accelerates packet processing. Allows you to create rules indicating the direction of the link and the firewall will be able to independently authorize the transmission of packets for known protocols and connection with others that the protocol used. Major improvements is the possibility to create a virtual connection status without status for protocols such as UDP (User Datagram Protocol) or ICMP (Internet Control Message Protocol).

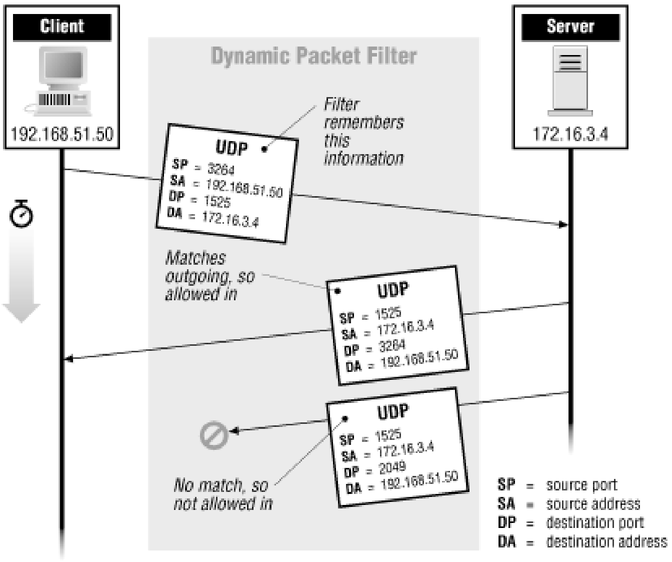


Fig. 3. Example of Dynamic packet filtering at the UDP layer [2]

The biggest advantage of stateful packet filters is the high speed analysis of ongoing communication, relatively high level of security in comparison with the application gateway and many times simpler configuration. Reduction of the risk of misalignment of the rules. The disadvantage of this solution is generally a lower level of security, that provide a gateway application.

2.6 Stateful packet filters with protocols control and IDS

Modern stateful packet filter in addition to information about status and the ability to dynamically open ports for control and data connections more complex protocols implement mechanisms due diligence. The firewall allows you to control the communications passing through the level crossing correctness of data protocols and applications. Often in that it integrates IDS to the firewalls. These systems work similarly to anti-virus programs. Using a signature database and heuristic analysis reveals the formula of possible attacks. Their main feature is the sensor that through mechanisms for detecting harmful and dangerous codes identify potential hazards. The system should be able to generate a warning alert after detecting unusual activity, writes the incident in the log file and alert system administrator in this unusual activity. It should also be able to recognize the attack from external or internal network.[5]

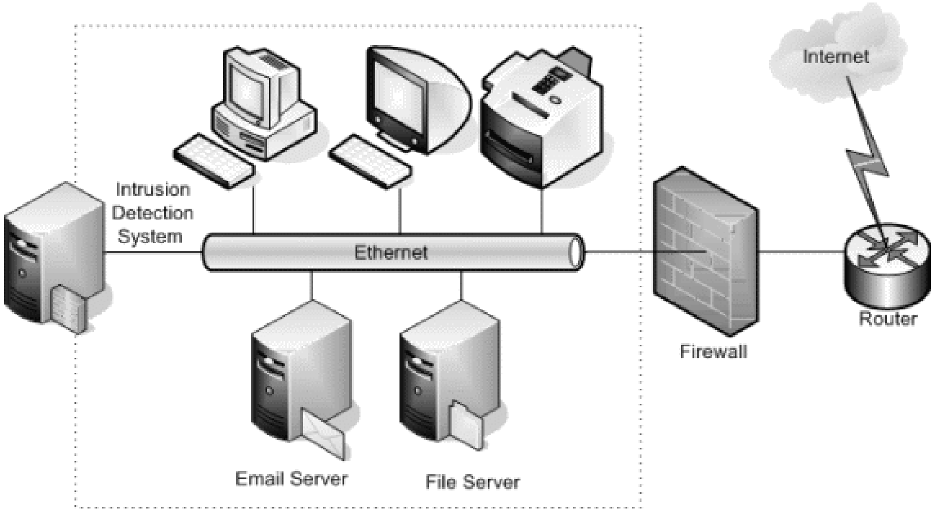


Fig. 4. Intrusion Detection System diagram [4]

The advantage of these systems is the high level of safety ensured by passing control protocols while maintaining a relatively simple configuration, relatively high scanning speed compared to the application gateway, the status packet filter is a noticeable slowing down (about a third to half).The disadvantage is the safety design of the basic safety rules to maintain safety systems as simple and small as possible. This type of firewall integrates a huge number of functionalities which increases the probability of errors in the code that can lead to a compromise of the whole system.

Typical of this category of firewalls are Check Point Firewall-1 (from version 4.1, at present NGX), products of Juniperas NetScreen, ISG and SSG. Similar functionality is available in the form of experimental modules also for "iptables" in the Linux kernel. [3]

2.7 IPS

IPS systems are generally considered an extension of IDS systems because they monitor the network operations, which could lead to disruption of network security. The major difference to the IDS is that the IPS is included directly into the network path (in-line) and thereby active preventing or blocking the detected undesirable and dangerous activities in the network. The system can perform actions after detect by unwanted activity, such as generate the warning alert, filtering harmful packet, violent reset connection or to block potentially dangerous operation of IP addresses. IPS is also able to fix faulty CRC (Cyclic redundancy check), defragment packets and streams to prevent shifting difficulties of TCP packets.[5]

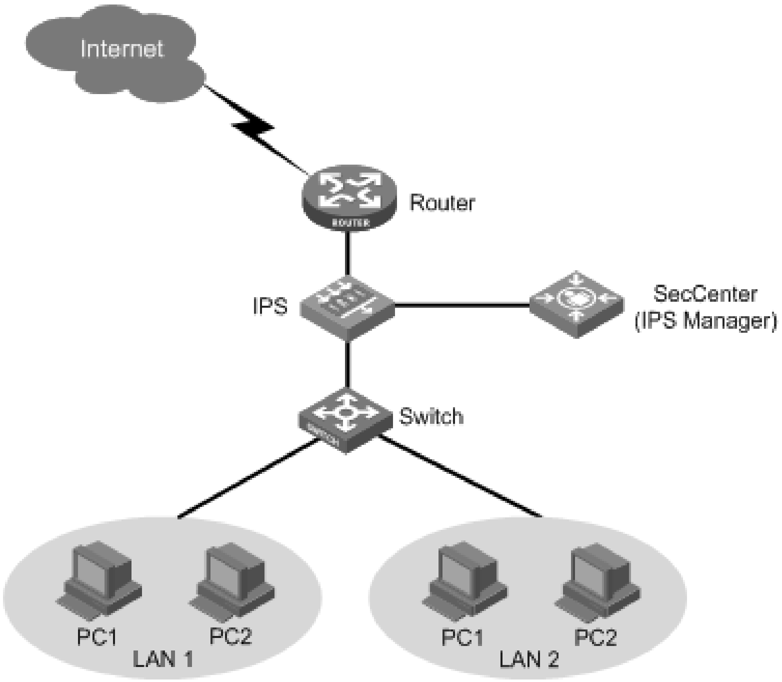


Fig. 5. Intrusion Prevention System diagram [5]

IPS has many advantages over their legacy counterparts IDS. One advantage is they are designed to sit in line with traffic flows and prevent attacks in real-time. In addition, most IPS solutions have the ability to look at layer 7 protocols like HTTP, FTP, and SMTP which provides greater awareness.

3 Firewall security policy

Setting rules for communication through firewalls commonly termed “firewall security policy”, abbreviated “firewall policy”. The Firewall security policy includes not only the actual rules of communication between networks, but in most of today's products also various global settings as address translation (NAT -Network Address Translation), instructions for creating encrypted connection between encryption gateway (VPN - Virtual Private Networks), searching for possible attacks and protocol anomalies (IDS), authentication and sometimes the authentication of users and bandwidth management.

4 Conclusions

This paper provides an overview of firewalls and their roles in protecting the network. Though some have predicted the end of the firewalls, its strategic location in the network makes it an indispensable tool for protecting assets. Good security practices dictate that firewalls should be deployed between any two networks of differing security requirements.

References

[1] KOVÁČ, M.: Analysis of network communication, Armed forces academy of general Milan Rastislav Štefánik in Liptovský Mikuláš: Thesis, 2015.

[2] ZWICKY, E. D., COOPER, S., CHAPMAN, D. B.: Building Internet Firewalls (Second edition), O'Reilly & Associates, 2000, ISBN 978-1-56592-871-7, [cit. 2015]. Available on the website:http://docstore.mik.ua/

[3] RASH, M.: Linux Firewalls: Attack Detection and Response with iptables, psad, and fwsnort, No Strach Press, 2007, ISBN 978-1-59327-141-1, [cit. 2015]. Available on the website: http://www.cipherdyne.org/LinuxFirewalls/

[4] SCHNEIDER, T.: The Best Damn Firewall Book Period (2nd Edition), Syngress, 2007, ISBN 978-1-59749-218-8

[5] NEWMAN, R. C.: Computer Security: Protecting Digital Resources, Jones & Bartlett Learning, 2009, ISBN 978-0-76375-994-0