Analysis of Identity Based Firewall Systems

Nenad Stojanovski[1] and Marjan Gušev[2]

Abstract – **The advances in today's computer technology bring the user's experience to such level where one of the most important things is the user mobility. The rise of user mobility within enterprise networks has brought the needs to allow mobile users to use mobility with full capacity in all aspects of collaboration. This problematic issue inspired many IT vendors to develop their own security solutions that extend user mobility. The general security solution to extend user mobility was introduced with identity based firewall systems, which extend the evaluation level of TCP/IP packets by inserting user identity to the whole inspection process. In this paper we will give a detailed analysis of the current identity based firewall solutions. During the analysis we will compare in lot of details how these solutions work and what they need in order to allow user mobility. As part of our research we develop and apply methodology with indicators to evaluate how these solutions affect computer network complexity and how they affect complexity in enterprise network.**

Keywords – **Identity based firewalls, user identity, firewalls, network security, computer networks, firewall analysis.**

I. Introduction

The advances in today's computer technology bring the user's experience to such level where one of the most important things is the user mobility. The rise of user mobility within enterprise networks has brought the needs to allow mobile users to use mobility with full capacity in all aspects of collaboration. This problematic issue inspired many IT vendors to develop their own security solutions that extend user mobility.

The main purpose of this paper is to analyze identity based firewall solutions that can be found on today's IT market. In the first chapter we give a general review on how firewall systems work and what intelligence is present behind the filtering mechanisms. The second chapter gives an analysis of the major players in the identity based firewall market. The analysis consists of information from technical character, where we present the findings of what is needed for these solutions to properly function. The last chapter gives a summary about the analysis of the firewall systems.

II. Firewall Technologies

A. Today's firewall technology

Times During the past two decades, Information Technology has evolved at such level that the complexities of the applications that are used by the users introduce the needs of extra security layers, aside from those present by the applications. Because of these needs, the firewall technology was introduces to help protect the assets that are sensitive and that shouldn't be accessed by everyone. It can be easily said that the firewall is a security gateway which is made up of the following components:

- Security policy – is a special type of policy that resides on the gateway, which contains all the rules that allow/deny access to certain resources. The rules are designed using IP addresses, TCP/UDP ports or applications
- The firewall is a software or a hardware device – it comes in the form of an appliance or in the form of an software add-on to the operating system
- Extra security features - as an addition to the firewall security policy, the firewall implements extra features that help protect the assets behind the firewall
- Demilitarized Zone or DMZ - a network segment that exists between the trusted and untrusted networks. DMZs offer some level of protection to the hosts that exist within that segment of the network.

Although, firewalls are introduced as a security mechanics it must be pointed out that there are advantages and disadvantages in using firewalls. The main advantage is the extra centralized security then bring, as well as the total cost of ownership of having a centralized firewall. The disadvantages are that they pose a bottleneck to the network, as well as false sense of total security when we speak about the insider attack.

In the beginning, the firewall at first had the task to protect the network at the IP level, layer 3 of the TCP/IP model. As time passed and applications evolved there were new challenges that had to be fulfilled by the firewall. In order to fulfill the needs, firewall systems had to evolve to a level where they could actively support the needs of modern IT technology. Today's firewall systems support all layers starting from the IP layer and ending to the Application layer.

Firewall systems are usually placed at layer 3, 4 or 5, depending on the control and protection they have to offer to the assets. The firewall systems that operate at layer 3 and 4 are called packet filtering firewalls. Their purpose is to filter IP and ICMP traffic, as well as TCP/UDP ports. A firewall

[1]Nenad Stojanovski is with Makedonski Telekom AD, Orce Nikolov BB, 1000 Skopje, Macedonia, E-mail: nenad.stojanovski@telekom.mk

[2]Marjan Gušev is with the Faculty of Natural Sciences and Mathematics, Ss. Cyril and Methodius University,Arhimedova b.b., PO Box 162, 1000 Skopje, Macedonia E-mail: marjan@ii.edu.mk

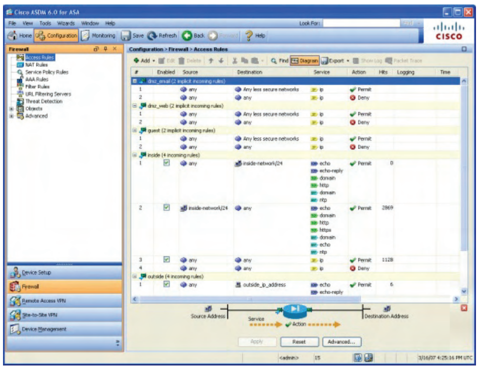
system at layer 5 is also known as application gateway and has the purpose to filter the traffic based on the application that generates the traffic.

B. Packet filtering firewalls

Packet filtering firewalls were the first firewall system that were invented. To be more precise, the first packet filtering devices were routers which had the ability to filter traffic based on layer 3 and 4 information. Packet filtering firewalls should be able to do the filtering based on the following fields: source IP address, destination IP address, TCP/UDP source port, TCP/UDP destination port.
Example firewall rules are shown on Figure 1. Some packet filtering firewalls allow additional layer 4 options to be added to the rules, like TCP flags that sometimes are very vital for enhancement of the TCP/IP communication between hosts. Packet filtering firewalls also support stateful packet inspection. The state oriented connection tracking add a state table to the firewall in which the firewall keeps information about the incoming or outgoing connections that go through the firewall system. In this way, the firewall system adds the flavor of inspecting if the incoming or outgoing packet correlates with an entry in the state table of the firewall. In this way, the firewall adds an extra mechanism to the network which protects against certain types of network attacks.

C. Application Level Firewalls

Application layer firewall is a computer networking firewall operating at the application layer of the TCP/IP protocol stack. These types of firewall systems can be implemented as a piece of software running on a single computer, or a stand-alone piece of hardware. Often, it is a host using various forms of proxy servers to proxy traffic before passing it to a gateway router. Because it acts on the application layer, it may inspect the contents of the traffic, blocking specified content, such as certain websites, viruses, and attempts to exploit known logical flaws in client software.



Configuration > Firewall > Access Rules

#	Enabled	Source	Destination	Service	Action	Hits	Logging	Time
dmz_email (2 implicit incoming rules)								
1		any	Any less secure networks	ip	Permit			
2		any	any	ip	Deny			
dmz_web (2 implicit incoming rules)								
1		any	Any less secure networks	ip	Permit			
2		any	any	ip	Deny			
guest (2 implicit incoming rules)								
1		any	Any less secure networks	ip	Permit			
2		any	any	ip	Deny			
inside (4 incoming rules)								
1	☑	any	inside-network/24	echo echo-reply domain http domain ntp	Permit	0		
2	☑	inside-network/24	any	echo domain http https domain echo ntp	Permit	2869		
3	☑	any	any	ip	Permit	1128		
4		any	any	ip	Deny			
outside (4 incoming rules)								
1	☑	any	outside_ip_address	echo echo-reply	Permit	6		

Fig. 1. Firewall policy example

Application layer firewalls may intercept all packets traveling to or from an application. They block other packets, if configured, dropping them without acknowledgment to the sender. In principle, application firewalls can prevent all unwanted outside traffic from reaching protected machines. One of the newest additions to the host based application level firewalls is the possibility to add rules that would allow or deny access to certain applications. It is also possible to allow different types of privileges to the application. Another branch of application firewalls is the web application firewall. It can be an appliance, server plug-in, or filter that applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as Cross-site Scripting (XSS) and SQL Injection. By customizing the rules to your application, many attacks can be identified and blocked. The effort to perform this customization can be significant and needs to be maintained as the application is modified.

Issues regarding the use of application level firewalls might be administrative tasks where they can be very complex for configuration, since they bring extra levels of complexity. This means that the total cost of ownership is much bigger because most of these firewalls need individual maintenance and support. Figure 2 shows the performance comparison between firewalls that filter layer 3, 4 and layer 5 traffic.

B. Identity based firewall systems

In the last few years the windows domain infrastructure has spread rapidly among companies. This has brought the ability to uniquely identify users in this domain, since every user has been given a unique domain user name. Moreover, with the rapid development of new devices, like smart phones, laptops and the lowering of the prices for them, the need of user mobility within these companies has rises. The whole concept of mobility asks that the users are mobile within their work environment, which forces them to use different IP addresses. By using different IP addresses, they are limited in the access to their resources. In order to solve the issues with the mobility, security companies have started to design and develop new concepts that could be implemented into the current firewall technology. These concepts should allow users to extend their mobility and let them be mobile in such ways that they would be able to access resources from where ever they are.

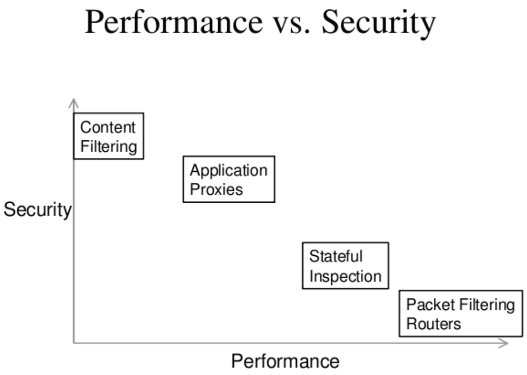


Fig. 2. Performance comparison between different types of firewalls

The whole idea behind the identity based firewall concept is to use the domain user name to build firewall rules. This can be done by embedding it with the standard firewall rules, but instead of using a source or destination IP, the rule will use the user name.

III. Analysis of Identity Based Firewalls

A. Analysis of Microsoft Internet Security and Acceleration server

One of the youngest firewall systems around is the Microsoft Internet Security and Acceleration server, or Microsoft ISA. Microsoft Internet Security and Acceleration Server (ISA Server) is described by Microsoft as an "integrated edge security gateway". Originating as Microsoft Proxy Server, ISA is a Firewalling & Security product based on Microsoft Windows primarily designed to securely publish web servers and other server systems, provide stateful, Application-Layer Firewalling, act as a VPN endpoint, and provide Internet Access for client systems in a Business Networking environment.

ISA Server 2006 is a multi-featured and multi-purpose security product that can be deployed in a variety of ways to meet the unique requirements of virtually any organization. As an integrated firewall, Web proxy and VPN server and gateway, ISA Server can be configured to act in each of these roles or be set up to provide only a subset. As an integrated solution, ISA server offers the following features: network layer firewall, an application layer inspection security gateway, forward and reverse Web proxy and caching server, remote access VPN server, site to site VPN gateway.

When it comes to user mobility, the ISA server offers some interesting features in the domain of user mobility. ISA server solves the mobility issues by using a dual formula. It means that the ISA server solves the mobility issues by presenting two solutions for a certain problem.

As said before, ISA server is one of the few servers that solves the user mobility. The technology used to allow user mobility is user based access rules. By introducing user based access rules, ISA server allows the administrators to connect layer 3 or 4 information with layer 5 information, the user name. This type of filtering would allow unique filtering based on user names and group.

The ISA firewall enables this functionality by offering a piece of software to be installed on the clients, which is called a firewall client.

The firewall client software transparently sends user information to the ISA server. This information comprise of user credentials (user name and NTLM hash). In this way, the ISA server has information about the clients in the network and it is possible to build firewall rules based on user names or groups. The user has to be connected with an account from the Active Directory or with a mirrored account on the ISA server. For example, if you have an Active Directory domain, users should log on to the domain, and the ISA Server 2006 firewall must be a member of the domain. The ISA Server 2006 firewall is able to authenticate the user and allows or denies access based on the user's domain credentials.

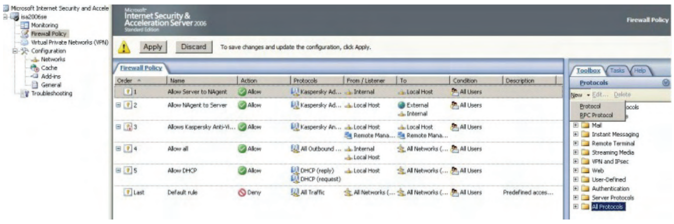
The other way to enforce user mobility is by using the ISA web proxy. This way, clients don't need to install extra software. This approach brings some limitations, which allow only rules for the web traffic. Every other traffic is filtered the good old fashion way via the use of IP addresses.

The approach that the ISA server uses has some disadvantages. One of the disadvantages is that when the web proxy approach is used, only the web traffic gets the possibility for user mobility. The firewall client approach brings the disadvantage that the ISA firewall is dependent on the firewall client, and vice versa. If the link between the firewall client and the ISA fails, the user of that system will lose the mobility.

Another general disadvantage of the ISA firewall is that is only supports Microsoft Windows environments. User mobility on other operating systems, like Linux, Mac OS X is not support.

D. Analysis of NuFW firewall

Another interesting player from the identity based firewall market is the NuFW. NuFW is a firewall solution developed by the french open source company INL. NuFW is based on the Linux operating system. The core of NuFW is the Linux firewall which is extended with the Firewall add-on Netfilter. NuFW extends the previously described Netfilter solution by adding the charm of user identity to the firewall. With NuFW, the firewall permissions follow an authenticated user instead of a PC's address. The NuFW concept allows admins to define not only user based firewall rules, but also rules that enforce policies upon IP addresses. The Identity concept allows that the security policy can be enforced for a user no matter where he or she is on the network. This also lends itself to marrying the firewall with an SSO (single sign on) authentication system. NuFW offers the following features: authenticates any connection that goes through the security gateway or only from/to a chosen subset or a specific protocol, filters packets with criteria such as application and OS used by the users, offers Single Sign On to clients.



To save changes and update the configuration, click Apply.

Firewall Policy

Order	Name	Action	Protocols	From / Listener	To	Condition	Description
1	Allow Server to NAgent	Allow	Kaspersky Ad...	Internal	Local Host	All Users	
2	Allow NAgent to Server	Allow	Kaspersky Ad...	Local Host	External Internal	All Users	
3	Allows Kaspersky Anti-Vi...	Allow	Kaspersky An...	Local Host Remote Mana...	Local Host Remote Mana...	All Users	
4	Allow all	Allow	All Outbound ...	Internal Local Host	All Networks (...	All Users	
5	Allow DHCP	Allow	DHCP (reply) DHCP (request)	Local Host	All Networks (...	All Users	
Last	Default rule	Deny	All Traffic	All Networks (...	All Networks (...	All Users	Predefined acces...

Fig. 3. Example User Based policy on Microsoft ISA 2006

In order for NuFW to work, it requires that he client install the NuFW client. Same as with the ISA server, this client sends user information to the NuFW firewall. NuFW can me authenticated by using and LDAP server or by using a database which stores user name information. NuFW uses the following authentication algorithm, which is shown on figure 3:

NuFW clients can be installed on almost every platform. In general all major platforms are support, Windows, Mac OS X and Linux.

The NuFW approach along with its advantages has some disadvantages. The first disadvantage is the same as with Microsoft ISA server, and it is because NuFW uses agents to authenticate users on the hosts. Another disadvantage is that NuFW generates a big overhead because on every packet is sends authentication request. In high load networks this can be a big issue, because the network will be extra utilized because of NuFW authentication packets.

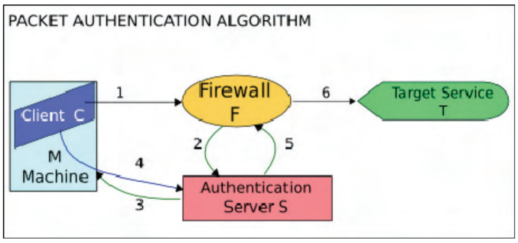


Fig. 3. NuFW authentication algorithm

E. Analysis of Checkpoint User Authority

One of the most advanced solutions regarding identity based firewalls is Checkpoint's User Authority. Check Point UserAuthority brings Web and network applications into one centrally managed security framework by leveraging Check Point's proven networking, encryption and authentication technologies. UserAuthority transparently integrates "best of breed" authentication mechanisms into network applications, enabling intelligent authorization decisions based on a connection's security context: user identity and profile information, encryption and authentication parameters, networking information and desktop security parameters. UserAuthority is the "security glue" that binds Web and network applications to users, Check Point VPN-1/FireWall-1 to create a Secure Virtual Network for the enterprise.

The key features of UserAuthority can be defined as the following: identity based firewall rules, identity based remote access rules, single sign-on to web applications.

The approach that User Authority uses is similar to the ones used with Microsoft ISA server and NuFW. One of the biggest differences that UserAuthority brings into the identity firewall schema is the ability to integrate it with remote access. By doing this, the user gets all of his resources anywhere.

In order to work, UserAuthority needs the network clients to install Checkpoint's SecureAgent. This software is agent based software that sends user credentials to the UserAuthority. By logon, SecureAgent detects the user name and sends the information to the UserAuthority server. When the user tries to pass through a security gateway to access his or her resources, the security gateway asks the UserAuthority server to identify the user that tries to access the resource. Upon successfully verifying the user, the security gateway grants access to the resources.

The disadvantage that this solution brings is the dependency on the SecureAgent, because if the agent doesn't work properly the whole concept of identity based firewall will not work.

IV. Conclusion and Future Work

Figures From the analysis we can conclude that every solution analyzed had the need of using an agent. This can lead to a conclusion that it is the weakness of these identity based firewall because the whole filtering is based upon information that is sent by the clients. If the clients fail to send information, then the whole user mobility concept fails. This brings us to the summary that the identity based firewall technology as it has some flaws.

Our future work on this topic will be to design an identity based firewall which will allow identity based traffic filtering without using software that has to be installed on every client PC. The solution will operating system features which will allow us to filter the traffic by using the user identity. In this way we will achieve that without installing agents on user workstations.

Comparison between the analyzed systems and the system that we will design is shown on table1.

	Microsoft ISA 2006	NuFW	CheckPoint UserAuthority	Our Design
L3, L4 filtering	✓	✓	✓	✓
Identity based filtering without agents	✓	×	×	✓
Identity based filtering with agents	✓	✓	✓	×
Network overhead	×	✓	×	✓
Multiple OS Support	×	✓	×	×

Table 1: comparison chart between the analyzed solutions and our design

References

[1] "CheckPoint UserAuthority", www.checkpoint.com.
[2] Microsoft ISA server 2006, www.microsoft.com
[3] NuFW, www.nufw.org
[4] Amon, C., Shinder, T., Carasik-Henmi, A.: The Best Damn Firewall Book Period, Syngress, 2003
[5] Noonan, W., Dubrawsky, I.:Firewall Fundamentals, Cisco Press, 2006
[6] Zwicky, E., Cooper, S., Chapman, D.:Building Internet Firewalls, O'Reilly Media Inc., 2000.