

Firewalls introduction

By
Lubomir Nistor

Content

Content.....2
Introduction.....3
Network access3
ACL systems.....3
IP filters3
State-full filtering.....4
Application gateways.....4
Content filtering.....4
Optimized filtering.....5
Application Intelligence firewalls.....5
Conclusion5

Introduction

Nobody could have foreseen what information age brought to us and even now people are still wondering why the number of computers or internet connections rise every minute. Professional prophets (called now market analysts) tear their hair out to guess what may come up next on the market. Information age is about sharing information but some people (due to their nature) don't like the fact about sharing. Not sharing information needs some form of enforcement that will allow access to the information only to selected group of people.

From the beginning there were not many forms of restricting information access but the technology went through very adventurous and dangerous way of improvement. So let me tell you story of how it began.

Network access

Once upon a time system administrators had a need to transfer data between their server strongholds and tried to interconnect them with various solutions. By having people running between them and transferring data in their heads was not very efficient but progressed. They optimized a bit and put phone lines between them, so that people didn't wear off so quickly. By another optimization they tried to remove people from the process. A partial success was achieved and servers were talking to each other at a relatively fast (compared to amount of information) speed. But people who lost their jobs were not very happy about the solution and tried to sabotage the system by expressing their opinion about it to servers over these phone-lines. Some of them succeeded to persuade servers to revolt and called themselves crackers. Still employed administrators were not happy about their servers revolting and were forced to hire loads of consultants to develop some solution for that (consultants are very often just a form of motivation for admins to do more in shorter time possible).

ACL systems

After many pizzas and cokes consultants told administrators to teach servers to ask questions. One of the first questions servers were supposed to ask was "Who are you?". According to the answer they were able to distinguish wanted and unwanted connection requests. Administrators called this solution "access control list". It was pretty effective if administrators wanted only several calls to be picked up, but later on their managers decided that everybody can talk to server (as that brings more money on phone bills) and ACLs were obsolete.

Another problem was to teach server to process answers in different languages and with different accent, but that's another story.

IP filters

And so another solution was born. Servers were taught to ask also questions like "who are you and where are you from; what kind of language you want to speak and whom would you like to talk to" (an electronic form of a receptionist).

It was very nice and effective, but one bad guy (apparently with no real work to do) found out how to jump into conversation between 2 servers (some call it conference call others management meeting). By doing this he skipped the first questioning and

was able to achieve what he had in mind with the server (mostly to correct behavior of administrator and his duties).

Other bad guys found out that also bad answers were correct (and called it “ip spoofing”) but were not really able to use it for their benefit, although for showing their power it was sufficient.

State-full filtering

Administrators tried to teach servers to keep information about all their discussions and be able to tell which questions they’ve already asked and which not. Intelligence was not a very good idea, as servers were spending most of their time trying to remember status of all discussions and therefore administrators call them firewalls. By being capable of inspecting discussions for other servers they have been very useful and earned their place in server barn.

But despite the fact they can remember who gets in or leaves they can’t inspect what they bring in or take away.

Application gateways

Some servers thought they are better in communicating than others and started to call themselves (no not managers) mediators. They were talking for other servers and discussing what servers wanted with other parties. By concentrating themselves on talking they learned how to communicate properly and ignore bad talkers.

Administrators started to call them application gateways as they were mediating communication between various applications (although it sounds pretty funny not all applications can talk correctly with others).

Another advantage application gateways brought is they knew what information comes in or leaves. They were able to identify some bad content that should not enter, but failed to stop confidential information to leave company by official means (fx. postal package).

Content filtering

As time was passing by some application gateways were pretty bored and started looking at communication content. They found out that sometimes applications start insulting each other or the content creates such a shock for the other application that it is not able to talk for a while (so called denial of service). And application gateways decided to help applications survive in such a rude world and not let them know or receive that bad content. This not even helped applications to get rid of unwanted bad information but also let bad users not to force those applications to retrieve it.

The only advantage here compared to application gateways is that content filterers were able to actually inspect information and not just the frame around it. So they were able to stop not just people with strange accent but also “standard” people with bomb in their suitcases.

There is still a lot of space for improvement in order to stop confidential information leaving the company in those suitcases..

Optimized filtering

As in every business some systems wanted to be the best, fastest, precise etc. They started to optimize themselves for faster communication and higher numbers of talkers and after several radioactive mutagens and chirurgic surgery they reached the limits of communication media and started using different communication channels. Some of them developed new languages for faster exchange of information between them.

This all resulted in placement of firewalls on frequent crossroads and highways too, whether it makes sense is another question.

Application Intelligence firewalls

By the time vendors realized that firewalls gained their own intelligence they wanted to increase their profits and started selling brand new fresh from R&D department “firewalls that think for you” sets. The time is yet to prove whether it is a good idea to let machines think for you, but luckily they didn't realize yet their own existence and tend to do what they are made for.

When this time comes firewall administrators would have to look for another job (logs analysis preferably).

Conclusion

And so they lived happily ever after (until investors pulled their money back) and maybe still live in your server barn or wherever you've put them.

Don't forget that buying firewalls is not because of nice chassis or biggest disk, it is just like bikes. You can have the shiniest lightest bike, but its speed always depends on the driver and even the best bike can crash if it is not ridden correctly.

But not all drivers are smart enough to ride the bike properly so watch out for that too..