ResearchGate

See discussions, stats, and author profiles for this publication at: https://www.researchgate.net/publication/292138198

Role of firewall Technology in Network Security

Article · December 2015

CITATIONS
0

READS
3,216

3 authors, including:

Mohammad Imran
Shaqra University
4 PUBLICATIONS **1** CITATION

SEE PROFILE

Some of the authors of this publication are also working on these related projects:

Development of a web based sementic system for analysis and identification of fingerprint pattern relationship with human genetics and environments View project

All content following this page was uploaded by Mohammad Imran on 31 January 2016.

The user has requested enhancement of the downloaded file.

Academic Science

International Journal of Innovations & Advancement in Computer Science
IJIACS
ISSN 2347 – 8616
Volume 4, Issue 12
December 2015

Role of firewall Technology in Network Security

[1]Mohammad Imran, [2]Dr.AbdulrahmanA.Algamdi, [3]Bilal Ahmad
[1]Lecturer, Department of Computer Science at college of science & Humanities,
Al-Dawadmi, Shaqra University,Kingdom Of Saudi Arabia.
[2] Dean of Information Technology and E-learning at Shaqra University, Shaqra,
Kingdom of Saudi Arabia
[3]Lecturer, Department of Computer Science at college of science & Humanities,
Al-Dawadmi, Shaqra University, Kingdom Of Saudi Arabia.

Abstract— *As the use of network resources are increasing, the attacks on network are spreading which causes loss of confidential information, loss of confidential data, spreading of virus in networks and computers. To avoid the attacks on networks and to restrict or block the information coming and going from network we required some security. Firewall technology results to protect the network from flow of traffic over internet.*

Index Terms—Firewall, Network, Traffic, Attacks

1. INTRODUCTION:

The word firewall illustrates the wall which is used to protect fire. The wall which was built to protect fire. In computer world the firewall protection refers to protect the network or computer from to block certain kinds of network traffic. It creates a barrier between trusted and untrusted network. It protects confidential information and protects the company from un-ethical use. Security of network from unauthorized access is the major role of firewall security.

Type of Attacks:

There is a list of attacks for which Firewall technology is used:

1. Socially engineered Trojans
2. Unpatched software
3. Phishing attacks
4. Network-traveling worms
5. Advanced persistent threats

Qualities of Good Firewall:

1. Any incoming or outgoing information must be coming through Firewall
2. Firewall will check and permit the authorized traffic only.
3. If any Trojans or phishing attacks on network, Firewall must be strong enough to protect network from these attacks.

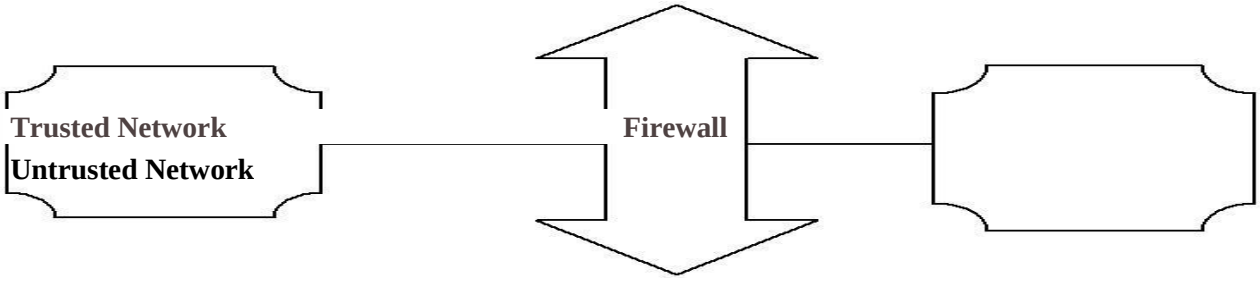

Figure (a)

To keep our information from these threats we must guarantee some security instruments such that inside data stay inside and outside data stay outside and keep outside assailants from entering in corporate system. One arrangement of this issue is the firewall. The primary assignment of firewall is to control stream of data

between PC systems. It ensures system by remaining in the middle of system and the outside world. The information move in any course must go through the firewall.

2. WORKING OF FIREWALL MANAGEMENT

There are two policies for firewall to work

1. Default- Deny Policy
2. Default – Allow Policy

Default-Deny Policy:

In Default –Deny policy the administrator of firewall create a list of allowed network services and rest of the network services are blocked.

Default – Allow Policy:

In Default –Allow policy the administrator of firewall create a list of not allowed network services and rest of the network services are allowed.

A default-deny way to deal with firewall security is by a wide margin the more secure, however because of the trouble in designing and dealing with a system in that form, numerous systems rather utilize the default-permit approach. How about we expect for the minute that your firewall administration project uses a default-deny approach, and you just have certain administrations empowered that you need individuals to have the capacity to use from the Internet. For instance, you have a web server which you need the overall population to have the capacity to get to. What happens next relies on upon what sort of firewall security you have.

3. TYPES OF FIREWALLS

1. Packet filtering firewall
2. Stateful firewall
3. Deep packet inspection firewall
4. Application-aware firewall
5. Application proxy firewall

Packet filtering firewall:

This kind of firewall has a rundown of firewall security rules which can protect traffic based on IP protocol, IP location and/or port number. Under this firewall administration program, all web activity will be permitted, including electronic assaults. In this circumstance, you need interruption aversion, notwithstanding firewall security, with a specific end goal to separate between great web activity (straightforward web demands from individuals scanning your site) and terrible web movement (individuals assaulting your website).

A parcel sifting firewall has no real way to see what matters. An extra issue with bundle sifting firewalls which are not stateful is that the firewall can't differentiate between an authentic return parcel and a parcel which professes to be from a built up association, which implies your firewall administration framework arrangement, will need to permit both sorts of bundles into the system.

Stateful firewall:

This is like a packet separating firewall, yet it is more wise about staying informed regarding dynamic associations, so you can characterize firewall administration standards, for example, "just permit bundles into the system that are a piece of an officially settled outbound association." You have comprehended the built up association issue depicted above, yet despite everything you can't differentiate in the middle of "good" and "terrible" web activity. You require interruption counteractive action to identify and piece web assaults.

Deep packet inspection firewall:

An application firewall really inspects the information in the bundle, and can accordingly take a gander at application layer assaults. This sort of firewall security is like interruption aversion innovation, and, in this manner, may have the capacity to give a portion of the same usefulness.

There are three provisos, then again: to begin with, for a few merchants, the meaning of "profound" reaches out to some specific profundity in the bundle and does not as a matter of course look at the whole packet. This can bring about missing a few sorts of assaults. Second, contingent upon the equipment, a firewall might not have satisfactory preparing energy to handle the profound bundle review for your system. Make sure to make inquiries about the amount of transmission capacity it can deal with while performing such examination. Lastly, implanted firewall administration innovation might not have the adaptability to handle all assaults.

Application-aware firewall:

Like deep packet assessment, aside from that the firewall comprehends certain conventions and can parse them, so that marks or guidelines can particularly address certain fields in the convention. The adaptability of this way to deal with PC firewall security is incredible and licenses the marks or principles to be both particular and complete. There are no particular downsides to this way to deal with firewall security as by and large it will yield upgrades over a standard "profound bundle assessment" approach. Then again, some genuine assaults may be disregarded (false negatives) in light of the fact that the firewall security parsing schedules are not sufficiently hearty to handle varieties in certifiable activity.

Application proxy firewall:

An application intermediary goes about as a middle person for certain application activity, (for example, HTTP, or web, movement), capturing all solicitations and accepting them before passing them along. Once more, an application intermediary firewall is like sure sorts of interruption counteractive action. The usage of a full application intermediary is, be that as it may, very troublesome, and every intermediary can just handle one convention (e.g. web or approaching email).

For an application intermediary firewall to be compelling as PC firewall insurance, it must have the capacity to comprehend the convention totally and to implement obstructing on infringement of the convention. Since usage of the convention being analyzed regularly don't take after a convention accurately, or on the grounds that implementers add their own particular expansions to a convention, this can bring about the intermediary blocking substantial activity (false positives). In light of these sorts of issues, end clients will frequently not empower these advances.

As should be obvious, there are territories of cover between interruption counteractive action and certain sorts of firewall security. The wording in this field is as yet being worked out, so it can be confounding now and again. Take in more about SecureWorks' Firewall Management.

4. FIREWALL LIMITATION

We have discussed the policies used by firewall and also discussed their types. It comes in our knowledge that Firewall provide us the security additionally a firewall is a to a great degree useful security measure for any organization. On other hand Firewall does not solve all the network issues it also has some limitation.

Direct internet traffic:

A firewall is just successful if there is single entry and exit point of network, but there is a situation where attacker can attack on network from other entry exit point, in this situation firewall cannot handle the attack successfully.

Virus attacks:

A firewall cannot totally ensure the inward system from infection dangers in light of the fact that it cannot check each incoming bundle for virus substance.

5. CONCLUSION

As we have examined so far that firewall is essential a portion of PC protection against infections, spyware, Trojans furthermore, different malwares furthermore between direct pernicious assaults from outside and outside of system. A decent firewall is the one that give full assurance of system without affecting the pace of our PC and our system access.

6. REFERENCES

- Enhancing Network Security in Linux Environment, Technical Report, IDE1202,February 2012
- Guidelines on Firewalls and Firewall Policy, Computer Security Division, National Institute of Standards and Technology Special Publication 800-41 Revision 1 Natl. Inst. Stand. Technol. Spec. Publ. 800-41 rev1, 48 pages (Sep. 2009) Gaithersburg, MD 20899-8930, September 2009
- Packet Filtering using IP Tables in Linux,"IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, July 2011"ISSN (Online): 1694-0814
- Linux - Wikipedia, the free encyclopediaen.wikipedia.org/wiki/Linux & Security Issues – Linux.orgwww.linux.org/article/view/security-issues & Quick HOWTO:Ch14 : Linux Firewalls Using iptables - Linux Home ...www.linuxhomenetworking.com/.../Quick_HOWTO_:_... - United States. &Packet filtering using iptables, http://netfilter.org/documentation/HOWTO/packet-filtering- HOWTO-7.html
- Michael R. Lyu and Lorrien K. Y. Lau,"Firewall Security: Policies, Testing and Performance Evaluation",& M. Goncalves, "Firewalls", McGraw-Hill, 1998 &Internet Firewalls and Securitywww.linuxsecurity.com/resource_files/firewalls/nsc/500619.html & Designing Scalable and Effective Decision Support for Mitigating ...web.eecs.umich.edu/.../securecomm11_vulnerability_m... - United States
- http://www.google.co.in/imgres?imgurl=http://computerclip arts.net
- http://www.milincorporated.com/a3-firewall-internet- security.html

View publication stats