International Journal of Information and Computation Technology.
ISSN 0974-2239 Volume 4, Number 1 (2014), pp. 53-58

http://www. irphouse.com /ijict.htm

Analysis of ACL in ASA Firewall

Tomar Kuldeep[1], Tyagi S.S[2] and Chawla Harsha[3]

[1]Research Scholar, Department of CSE,
ManavRachna International University,Faridabad, INDIA.
[2]Prof & Head, Department of CSE, ManavRachna International University
Faridabad, INDIA.
[3]M.Tech Scholar, Department of Computer Science & Engineering, NGFCET,
Maharshi Dayanand University, Palwal, INDIA.
E-mail: [1]kuldeep_karan@yahoo.com, [2]shyam.fet@mriu.edu.in,
[3]harshachawla19@gmail.com [1]www.mriu.edu.in,[2]www.mriu.edu.in,[3]www.ngfcet.com

Abstract

Now a day's internet is a part of our life. The access of Internet is increasing day by day so; we also have to focus on that what have to be access on our network. In this Paper we will analyze the implementation of access control list in ASA firewall and analyze that whether it is fully capable of restricting the attacks or not. For ensuring high security on our networks we have to ensure that the unwanted data should not enter our network and the restricted data/policy should be monitor easily, for this monitoring we have proposed ACL Viewer through which we can easily monitor the rules and policies implemented by network administrator.

Keywords: ACL, ASA firewall, Network Security;

1. Introduction

The importance of Network Security has increased with the growth of internet [6].Internet systems and components are apt to security risks (See example [7]).These security risk tends to harmful effect on our useful information. A current challenge is to invent and study appropriate theoretical models of limiting the untrusted sites from emerging networks. One of the methods is ACL. ACL is a conceptual view in computer security system and it is used to implement the privilege separation [8]. To supervise the incoming and outgoing traffic in networking, we used Access Control

List and they are similar to firewalls [8]. It is an sorted sequence of rules and each rule towards permit or deny any packet that it matches. [11]

In this we analyze the security rules and policies deployed to identify and correct some policy anomalies [9]. Cisco provides Adaptive Security Appliance (ASA) firewall which is capable to use in packet filtering, packet inspection against the attacks like Access Attacks, Reconnaissance Attacks, and Denial of Service (DoS)[1,2] attacks. Thus, any traffic that is not permitted from the untrusted to trusted interface will be denied [10].

In this paper we will analyze the implementation of ACL in ASA firewall to provide security using policies and rules. For monitoring this, we proposed the ACL viewer tool that shows all policies to overcome the problem of network administration.

2. Background

First we will concentrate on the Cisco routers which implement ACLthat filter inbound and outbound traffic [10, 14]. The router examines each packet to determine whether to forward or drop the packet, on the basis of the criteria you specified within the access lists (see Fig. 2.1).Developer ofCisco develops the Cisco works tool that is used to enhance the performance of networking.ACL Manager helps you manage Access Control Lists (ACLs) on Cisco routers [15]. It presents a user-friendly graphical user interface that allows you to concentrate on the security of your network without having to learn the complex syntax of ACLs [14, 15].

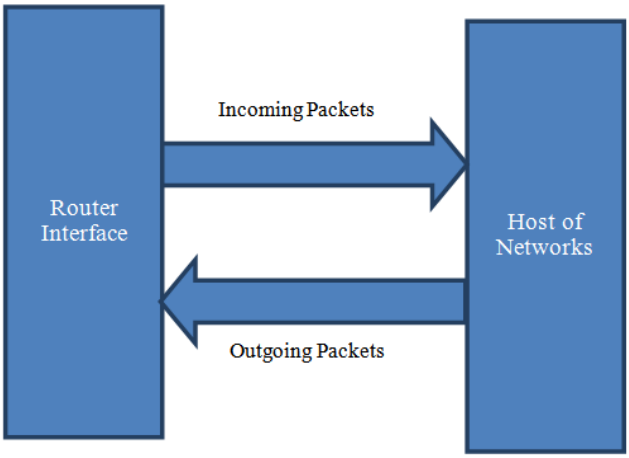

Fig. 2.1: Access list ingress/egress.

Cisco provides several types of ACLs on its hardware. Standard ACL: It filter the only the source addressExtended ACL: It filter source and destination address [5, 14, 15]. Standard IP ACLs are numbered 1 through 99, while extended ACLs are numbered 100 through 199. The format and syntax of standard and extended ACL are different. However our focus and our work will be on extended ACL in Cisco routers. Therefore our design will be based on extended ACL [14, 15].

2.1 How ASA firewall implements ACL

The best place to block unwanted IP traffic is at the network perimeter. This is done with firewalls or routers by implementing large access control lists (ACLs)[15].The Fig. 3.1 shows proposed implementation of ACL in ASA firewall and URL filtering is feature of ASA that will work filter the URL[15]

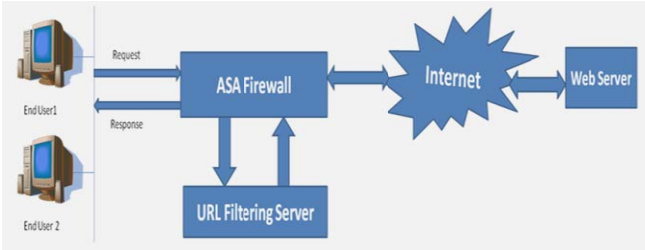

Fig. 3.1: ASA implement Access Control List.

This Fig. works as when End user request for http page to web server then its request reach on ASA before web server as well as URL filtering. URL filtering is powerful feature of ASA firewall. When URL filtering received the request and checks its database for taking decision on request as describe in policies. URL filtering send look-up response to ASA firewall .Then ASA firewall performs action on receiving Look-up responses either request denied or allowed depending upon the policies define on URL filtering. In this manner we can implement ASA for the purpose of controlling the access list [15].

2.1.2URL filtering

URL Filtering Server is main feature of ASA firewall. It can be used as Access Control by defining policies in configuration of URL Filtering Server. It has some advantage:-

- By URL Filtering, we can communicate with our desired host directly.
- Time of data transferring will decrease due to fix URL.
- It works only on outbound traffic.
- It filters URL as well as domain name specified in URL and words.
- It reduces network traffic.
- It ensures that load of other traffic is not affected [15].

3. Proposed Work

3.1 Analysis of Tool design

In the contrast of some big organization like we take example of University. There are various challenges for administrator and the management that what kind of traffic should be access to students and to faculties. So it is necessary for admin, Head of the department to monitor the access list frequently. Which is not possible for all the departments as admin is not access to everyone? So, taking this problem into account we have proposed an ACL viewer which works on client machine and they can view

the policies and rules implemented on the ASA firewall or on any server administration in the network. According to the problem we proposed ACL Viewer tool .This tool will do the following things:

3.1.1 Show all the permissions assigned to a Trustee

Whenever we want to see all the trusted sites that describe in policies of URL filtering then it is very easy to see using ACL Viewer Tool. It shows not only the trusted sites as well as all the policies or rules in URL filtering on the client side.

3.1.2 Show inheritance information

As we describe above that URL filtering filter the domain and words. For Example: if want to filter www.facebook.com/friends only. Then it shows the all information with sub domain to domain.

3.1.3 Resolve all the object-guides - property, property-set and object types

It shows all the object property, property set related to HTTP page that will be granted for permission.

This tool work works on client side that is connected to server through LAN and ASA firewall implement on Server as shown in Fig. 3.1 .We can used window server 2000 or any other Server to implement it.

4. Conclusion and Future Work

In this paper we have analyze the problem faced by the university management related to restricting unwanted traffic. How the policies and rules can be monitored the individual head, so that they can suggest the administrator that what kind of traffic they want to have. For this we have proposed the ACL viewer which works on client end. It will be very effective in case of getting information related to server and firewall. Our, next step will be to develop ACL Viewer and implement it on the network.

References

[1] Y. Xiang, Y. Lin, W.L. Lei and S.J. Huang,Detecting DDOS attack based on network self-similarity,Internet Protocols Technology and Applications (Voip)

[2] AmeyShevtekar, KarunakarAnantharam, and Nirwan Ansari, Low Rate TCP Denial-of-Service Attack Detection at Edge Routers, IEEE COMMUNICATIONS LETTERS, VOL. 9, NO. 4, APRIL 2005

[3] F.A. El-Moussa, N. Linge and M. Hope, Active router approach to defeating denial-of-service attacks in networks, IET Commun., Vol. 1, No. 1, February 2007

[4] Zesheng Chen, *Member, IEEE*, and ChuanyiJi, *Senior Member, IEEE*, An Information-Theoretic View of Network-Aware Malware Attacks, IEEE Transactions On Information Forensics And Security, VOL. 4, NO. 3, September 2009

[5] Alex X. Liu Eric Torng Chad R. Meiners, Compressing Network Access Control Lists -Supplement
[6] Stallings, W.: Cryptography and Network Security: Principles and Practice, 3rd edn. Prentice-Hall,Englewood Cliffs (2003)
[7] Cheswick, E.R., Bellovin, S.M.: Firewalls and Internet Security. Addison-Wesley, Reading (1994)
[8] PrakashChandrasekaran, Access Control Lists, ISEA, IMSc, 22 May 2006
[9] The Impact of IP Access Control Lists on Firewalls & Routers - A business case for specializednextperimeter security
[10] www.cisco.com/en/US/products/ps6120/prod_models_comparison.html.
[11] V. Grout, J. McGinn,Optimisation of Policy-Based InternetRouting using Access-Control Lists, Centre for Applied Internet Research (CAIR)University of Wales, NEWI PlasCoch Campus.
[12] Ramy K. Khalil, Fayez W. Zaki , Mohamed M. Ashour, and Mohamed A. Mohamed,-A Study of Network Security SystemsIJCSNS International Journal of Computer Science and Network 204 Security, VOL.10 No.6, June 2010
[13] Alex X. Liu, Member, IEEE, and Mohamed G. Gouda, Member, IEEE, Firewall Policy Queries, IEEE Transactions On Parallel And Distributed Systems, VOL. 20, NO. 6, JUNE 2009
[14] Abdulelah A. Al-Wabel,Hamad I. Al-Shayea,ACL Analysis Tool, King Saud University College of Computer and Information Sciences
[15] www. Cisco.com.