

A STUDY ON IMPLEMENTING PACKET FILTERING FIREWALL WITH CISCO IP ACCESS CONTROL LIST (ACL)

Imam Sutoyo¹, Mochamad Wahyudi²

¹ Study Program of Computer Engineering AMIK BSI

² Postgraduate Program of Computer Science STMIK Nusa Mandiri, Study Program of Computer Engineering AMIK BSI
imam@bsi.ac.id
wahyudi@nusamandiri.ac.id

Abstract

A computer network has become a necessity for any organization implementing a computer-based information system. Hence, keeping the security aspect is important to maintain the network performance so as to provide optimum service to its users and to be up against any attacks especially when it is connected to the Internet. This paper is intended to give input to computer network administrators who implement IP Access Control List (ACL) network security system as firewall. It discusses the strengths and vulnerabilities of packet filtering firewall using Cisco IP Access Control List (ACL). The findings of this study will give computer network administrators better understanding on implementing Packet filtering firewall with Cisco IP ACL and comprehending the potential security holes due to its vulnerabilities.

Keywords: *Vulnerabilities, Packet Filtering Firewall, Cisco IP Access Control List (ACL), Cracker*

I. INTRODUCTION

There are ways to secure computer networks. Firewall is one of techniques which is implemented in network security. In a firewall system, packet filtering is the basic method for its system design. Sysco System Inc. provides a packet filtering method called the IP Access Control List (ACL) in all its router products. ACL is used to filter inbound and outbound data packets.

ACL is a security facility in Cisco Internetwork Operating System (IOS) which is designed within Cisco routers. Therefore, when building a simple firewall system for an internetwork using Cisco router, the administrator does not necessarily need additional security ware.

Among its strengths, ACL also has its limitations. By understanding its vulnerabilities, ACL users can take the necessary actions to cover these limitations. Like most security software problems, vulnerabilities are potential to any exploitation carried out by crackers. The network administrator can identify this lackness using the vulnerability taxonomy method.

II. DISCUSSION

2.1. Firewall

Firewall is a well-known technology in the world of network security. Brenton (2003) defines firewall as a system or group of system which implement an access control policy on data traffic through

network access points. Firewall filters data which pass through access points in a network, both inbound and outbound data packets.

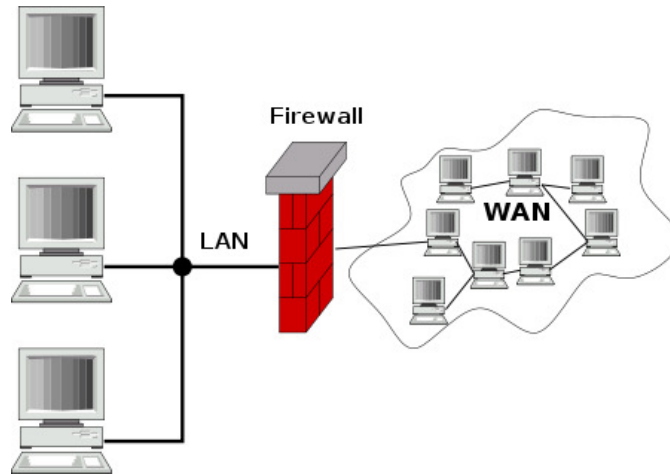


Figure 2.1. Firewall

There are kinds of firewall. Beny (2004) classifies firewall by its function:

1. Packet Filtering Firewall

In accordance with its name, this firewall filters every data packet. From the filtering result, the data packet is then determined either let to pass or denied.

This type of firewall is generally implemented on router, a hardware working in the network layer of an Open System Interconnection (OSI) model. Data filtering carried out by packet filtering firewall is based on the information processed in the layer that is the IP address.

The benefits of this type of firewall are: it is independent, adjustable with the system needs, high level of transparency and performance. On the contrary, this firewall is also has low level of security performance despite the abundant amount of threats against the network system. It is also vulnerable to IP Spoofing, does not have method to check on stateless connections, authentication method, and its performance is limited on network layer only.

2. Application Level Gateway

It is also known as proxy. It works as a medium between a host in the internal network and external resources accessed by the host. The most common name for this firewall is proxy server.

By using proxy server, the host in the internal network never directly connected with the network resource from outside the

network where it works. Every request for access to any resources out side the local network will be directed to proxy server. It will then determine whether or not to execute the connection.

The strengths of this firewall are having a better security performance than the packet filter firewall. It also has authentication and access control method, logging facility, and caching facility to save bandwidth. Yet, its limitations are unavoidable: it is less transparent to users where users' application should be configured to support the function of the proxy, and it has a lower performance than packet filter firewall.

3. Circuit Level Gateway

This firewall is an improvement of Application Level Gateway. Hence, both task principles are the same, which is as a medium between the host of the internal network and external resources accessed by the host. The difference is in the level or location in which the proxy function is executed.

This firewall has, more or less, similar strengths with Application Level gateway. But Circuit Level Gateway does not require application configuration like the Application Level Gateway. Furthermore, it enables any applications which do not support the proxy function. The weakness of this firewall is somewhat the same with Application Level Gateway. The difference is the application which is used should be

compatible with the running platform, for example, it should be compatible with the Application Programming interface (API).

4. Statefull Inspection

This is the most sophisticated firewall. The task principle of Statefull Inspection is actively monitoring any connections to show the status of those connections (statefull), so the administrator can execute the necessary actions when there are problems found in the connections.

The superiority of this firewall is seen from the highest level of security it has, its complete support and monitoring to all OSI layers, high performance level, and good scalability and transparency. The only weakness that this firewall has is it needs great resource, particularly when the connection is increasing in number.

2.2. Cisco IP Access Control List (ACL)

Access control is a security mechanism which is generally implemented in a security scenario of an information system. Access Control is applicable through three information system components: hardware, software, and brain ware.

One of examples in implementing Access Control through embedded hardware, specifically on a router, is what has been done by Cisco System Inc. in their router product series, the Cisco IP Access Control List (ACL). ACL is a security facility in Cisco router to filter data packet going to and from the router.

As Cisco describes (2008), "IP Access Control List is a series list which at least consists of one permit statement and probably one or more deny statements. The data packet filtering mechanism in ACL is based on both statements. A data packet will be proceeded if it meets the permit criterion but does not fit the deny statement. On the contrary, when the data packet does not fit the permit statement but meets the deny criterion, it will not be proceeded. The list of statements in the ACL is processed sequentially from the first until last line.

2.2.1. ACL Classification

There are two types of ACL, Standard ACL and Extended ACL. In accordance with its name, the Extended ACL has more complete filtering facilities than the Standard ACL. But both ACL complement each other.

As what Cisco proposes that the

Standard ACL will be effective if positioned at the destination location, while the Extended ACL should be positioned at the origin location of data packets.

1. Standard ACL

Standard ACL only filters data packet based on the IP address of the packet sender. When a data packet is coming through an interface or a router, the address of the sender is compared with the IP address which is defined in the ACL lines of statements implemented in the interface. Accordingly, the data packet is either let to pass or not.

Standard ACL is using numbering system from 1 to 99. The following is the syntax of the Standard ACL.

```
access-list access-list-number {deny | permit} source-ip-address [wildcard-mask]
```

Where:

- a. *Access-list*
The keyword used to make ACL
- b. *access-list-number*
The identity number of ACL, ranges from 1 to 99
- c. *{permit | deny}*
The action upon the data packet either let to pass or denied.
- d. *source-ip-address*
The sender's IP address
- e. *[wildcard-mask]*
The used wildcard

Example:

```
access-list 1 permit host 202.101.51.3  
0.0.0.0
```

The Standard ACL above only passes on data packet from IP address 202.101.51.3.

2. Extended ACL

The Extended ACL has more complete filtering facilities than the Standard ACL. Besides filtering data packet based on the Sender's IP address, Extended ACL can also be used to filter packet based on the destination IP address, port number, and type of protocol used.

The Extended ACL uses numbering from 100-199. The following is the syntax of Extended ACL.

```
access-list access-list-number {deny |
```

permit protocol *source-ip-address*
[wildcard-mask] *destination-ip-address*
[wildcard-mask] *operator*

Where:

- a. *access-list*
The keyword used to make ACL
- b. *access-list-number*
The identity number of ACL ranges from 100-199
- c. *{permit | deny}*
The action upon the data packet either let to pass or denied.

- d. *protocol*
The protocol name or number
- e. *source-ip-address*
The sender's IP address
- f. *destination-ip-address*
The destination IP address
- g. *[wildcard-mask]*
The wildcard used
- h. *operator*
The operator used

Table 2.1 Operator for *Extended ACL*

Operator	Explanation
eq (<i>equal</i>)	Determining one port number
neq (<i>not equal</i>)	The negation of operator eq
gt (<i>greater than</i>)	Used to determine the bigger port number range than the given port number
lt (<i>less than</i>)	Used to determine the smaller port number range than the given port number

Example:

```
access-list 100 permit tcp 202.101.51.3
0.0.0.0 host 172.16.1.1 0.0.0.0 eq 80
```

The Extended ACL above only passes packet from IP address 202.101.51.3 to TCP protocol IP with port number 80.

2.2.2. Setting the ACL on the Interface

The first step in using ACL is formulating filtering rules for the data packet through the lines of statements in ACL. Second, the rules are then set in an interface of a router.

Data packet filtering in an interface is applicable for both the incoming and outgoing data to and from the router through the interface. ACL which is set to filter data packet coming through an interface is called inbound ACL. ACL which is set to filter data packet going out through an interface is called outbound ACL.

The inbound ACL filters data packet coming through an interface router. When a data packet is coming in, it will be checked by matching it with the rules in the ACL set to the interface where the data is going through.

If the data packet fits with one line of permit statement, it then will be directly processed by routing it to its destination

network. So, the data packet will not need to be matched with other ACL statement lines. On the contrary, when the data packet meets one line of the deny statement, it will be rejected, and the router will send the ICMP destination unreachable packet to the sender. So, the data packet will not need to be matched with other ACL statement lines.

The outbound ACL filters data packet going out an interface router. When a data packet is going out, or requests to be routed out of the internal network, it will be matched with the rules in the ACL set to the interface where the data is going out.

If the data packet fits with one line of permit statement, it then will be directly processed by routing it to its destination network. So, the data packet will not need to be matched with other ACL statement lines. On the contrary, when the data packet meets one line of the deny statement, it will be rejected, and the router will send the ICMP destination unreachable packet to the sender. So, the data packet will not need to be matched with other ACL statement lines.

There are requirements in designing and setting the ACL in the interface:

1. There should be only one ACL for one protocol to one filtering destination
2. The *Standard ACL* should be set as near as possible with the destination location

- of the data packet.
3. The *Extended ACL* should be set as near as possible with the original location of the data packet.
 4. The filtering view should be from inside of the router. SO, interface router is seen as the entrance.
 5. Every statement is process sequentially from the first until the last line.
 6. At the last line of every ACL there is implicit deny line, that is a statement of deny all which functions to deny any packet that does not meet any one of the previous permit statements.
 7. The content of ACL should filter data packet from specific to general; for example, determining the rules of a host then the rules of groups of hosts.
 8. Checking or matching process based on the criteria is done first before applying permit or deny process.
 9. Do not manipulate an active ACL within an interface.
 10. Deleting an active ACL in an interface must be done carefully by firstly disabling the interface.
 11. If a data packet is denied, ACL will send ICMP Destination Unreachable packet to its sender.

2.3. Vulnerabilities Taxonomy Method

Krsul (1998) states that, "taxonomy is a theoretical study on classification, including basic foundation, principles, procedures and rules related to the classification." The classification method is used to facilitate easy analysis of an object or problem.

Taxonomy is generally known in the field of Biology. But it is also known in computer science particularly in Information Security study since the early development years of this science.

According to Wright (2007), "the need in a structured taxonomy (labeling system) for terms or facilities in information system security is not a new thing. These services have already been available since business and government use computer around the 70s."

An example of taxonomy method in Information System Security study is the vulnerability taxonomy. It is a systematic method used to explain the limitations of a system which is potential to exploitations from people unauthorized to the system, as well as the solutions to this problem.

As Krsul (1998) states, "the function of taxonomy is to guarantee the species division or sequencing execution to draw

generalization over the entire species. Taxonomy is used to predict the existence of unknown species by studying the patters of the already exist species." Therefore, taxonomy has a prediction value.

In conclusion, vulnerabilities taxonomy method is very useful for analyzing and classifying weaknesses of a system, or security system software, like firewall. By applying this method, we not only can define the causes of the weaknesses, the side effects, and the solution techniques, but also classify the variety of the weaknesses which will make the analysis easier. This analysis is not only for solving the current problems, but it is also useful as the basis for solving the future problems to come.

Kamara, et al (2003) classifies the causes of vulnerability related to firewall into seven categories:

1. Validation Error

Validation Error happens when program, tools, or system interacts with its environment in processing data from the environment without verifying the validity of the data.

There are three types of data which need validation: input, origin, and target. Input validation means checking whether the input data is suitable in terms of sequence number, type of data, and its format. Origin validation means checking whether the processed data is original, in accordance with what it represents. Target validation means checking whether the processed data is given to its rightful receiver. Target validation also makes sure that the data do not go to unrightfully recipient..

2. Authorization Error

Authorization Error is also called authentication error. It happens when a non authorized party is permitted to operate on the program, tools, even the system.

3. Aliasing (Serialization/Aliasing Error).

Serialization Error happens when there is exploitation on the system as the result of synchronized behaviors of two different systems which are allowed to run at the same time. Aliasing Error happens when there are two labels given to an object which causes changes in the content of the object. Consequently, it changes the object's previous validation result.

4. *Boundary Checking Error*

Boundary Checking Error happens as the result of failures in checking the definite boundaries which causes Buffer Overflow.

5. *Domain Error. Domain Error* happens when a security hole appear in a Domain. When a Domain is violated the information leaks out to unauthorized users.

6. *Weak/Design Error*

Weak/Design Error happens in the system designing process. An example of this mistake is weakness in the algorithm encryption where the cyphertext is easily encrypted.

7. Other errors. Errors which do not include in the six categories belong to this one.

2.4. The ACL Limitations

Cisco System Inc. creates ACL as basic security software in their router product series. ACL was designed to filter data packet which is the basic function of any firewall. It provides optimum security function, yet simple in designing and implementing.

A solid firewall system built of various security functions is not a sole solution to secure a system, even ACL which only filters data packet for its security function. Therefore, it is crucial to understand the limitations of ACL so the administrator can take the necessary action to maintain his network security maximally. The following is ACL's limitations, the analysis, and solution based on vulnerabilities taxonomy method:

1. ACL should be designed sequentially, particularly when the number of statements in the ACL is increasing. It will be more difficult to design, audit and maintain.

The error tendency of an ACL with many rule lines is on logic. It is hard to maintain logical consistency of all lines in the ACL. Some logic errors may appear, such as redundant statement lines, intersection statement lines, and inconsistent statement lines.

Redundant statement lines mean two or more lines have the same rule, where

one line is actually the subset of another line with a more complete rule statement.

Intersection statement lines means two or more lines have rules which overlap, where one line shares the same rule statement with another line or their filtering rules are intersecting.

Inconsistent statement lines means two or more lines have opposite statement rules, where there is a statement line which permits a certain data packet while there is also another line which denies the same data packet, or vice versa.

These logic errors emerge due to the improvement of the ACL. The more developed the network, the more statement rule lines in the ACL. Changes in the security policy also create difficulties in synchronizing the lines of the old and new rules. It requires good understanding of the ACL designing technique, carefulness, and perseverance to make an accurate and efficient ACL.

Cisco has provided a tool to manage ACL, the Cisco Works. It is a Graphical User Interface (GUI)-based application. It is used to monitor and manage Cisco's network ware. For ACL management, Cisco provides ACL Manager Facility to create, edit, and arrange statement lines and other managerial functions in ACL.

Based on vulnerabilities taxonomy, ACL limitations are more on the design error or weakness which causes difficulties to users. However, the simplicity of ACL design for the purpose of high performance should be comprehend by administrators that they can, therefore, minimize the effects of ACL vulnerabilities, yet they can gain benefits out of its simplicity.

2. ACL is a stateless packet filtering firewall. Meaning that ACL cannot check the authenticity of the intertwined connections. So long as the data packet meets the requirements in the ACL, it will pass. It is possible that a data packet with a valid IP address and is allowed to pass through is actually from a cracker who wants to exploits the system. It is untraceable because the cracker is using IP Spoofing.

Based on the vulnerabilities taxonomy, this is a validation error related to origin validation, in which ACL cannot or fail checking on the true IP address of the data packet due to IP Spoofing. So, the attacker can infiltrate the system and exploit the network by disguising the IP address.

3. ACL only filters data packets coming in through an interface in a router. These data packets are going from external network to internal network and vice versa. ACL cannot filter data packet from the router, like routing protocol data packet (OSPF hello), update routing packet, and the kind which is used by router to exchange routing information and ACL does nothing to check them.

Attackers can make route advertisement packets containing routes which can pass data packet to their network. If we use a protocol router, which is dynamic and provides easiness in administration management that static routing, then ACL cannot filter which the valid route advertisement is.

Static routing is safer than dynamic routing. Brenton (2003) states, "Although static routing needs a lot of maintenance, it is the safest technique to build your routing table. Dynamic routing, on the other hand, allows dynamic update on the routing table by using tools in the network. Attackers can exploit this facility to give false routing information to other routers in our network which will hinder the network to performance properly."

The solution to this problem is by using protocol routing with authentication and encryption features, like Open Shortest Path First (OSPF). It requires all routings participating in routing table exchange to give their password so their route information is acceptable. The password, routing table information given, and the cryptography key will be encrypted and enclosed in the update routing table packet.

Therefore, the route information exchange security is done by protocol routing which already has had OSPF feature. Without any security facilities, router that we used is vulnerable to illegal route information. Network administrators, thus, should be able to

check on the routing table of all routers in their networks manually with the instructions in IOS, through console and by using a terminal.

Based on vulnerabilities taxonomy, this ACL limitation is on design error or weakness, where it causes the Router to be vulnerable to illegal routing information from routing update packet sent by irresponsible people.

4. Once a packet meets the requirements of a statement line in ACL, either permit or deny statement, an appropriate following action will be executed. This packet will not be re-matched with the other lines. Consequently, ACL should be carefully designed to avoid error in executing action given upon a data packet which may open the possibility a data packet to be permitted instead of denied, or vice versa.

Although vulnerabilities taxonomy does not consider this absolutely as a design error, this is actually a design limitation of the ACL where it is designed to be simple and fast that it does not influence the performance if router. Once a packet fits one line in the ACL, then it will not be checked by the rest of the lines to save processing resource of the router.

5. ACL is not designed to detect attacks from inside, that is from the authorized users within the internal network who use the network resources to carry out their conducts. The authorized users are free to do anything within the network, both legal and illegal, without being detected by ACL.

To analyze the packet traffic within the internal network, an administrator needs a network analyzer program or traffic analyzer. This program is capable of catching every data packet in a network and analyzes it by comparing it with the network's attack operation mode database to determine the kind of activity carried out by the data packet owner.

If the data packet proven to be suspicious, that it matches the operation mode in the database, then the system takes immediate action by directly cutting out the connection or sending reports to the administrator of the system to execute any necessary act. This is done by security software called

Intrusion Detection System (IDS).

IDS do not consider whether or not the IP address of the data packet is valid. So long as the connection activity of data packet fits the attack operation mode in the IDS database, the system will see the connection and data packet as illegal and thus must be blocked.

This ACL vulnerability is a design error or weakness, in that ACL characteristic as stateless packet filtering.

6. ACL cannot recognize malware, like virus, worm, Trojan horse, and the kinds. Malware is the most effective weapon used by attackers to exploit or make a system collapse. ACL may pass a data packet which actually a malware as long as it meets the permit statement in the ACL list.

ACL can only apply access control through its filtering mechanism. It does not have a capability in recognizing and even handling malware. As Brenton (2003) states that, "Access Control cannot eliminate or detect the existence of a cosmetic program. Access control is only a method which helps the system to block infection caused by viruses. Meaning that, the implemented access control method either through filtering mechanism, authentication, or the kinds can only block malware to infiltrate. ACL cannot detect malware and furthermore, recovering infected resources. The system will need another application for the job that antimalware application.

When ACL blocks a malware it is based on an assumption that malware is only carried by data packet which is not allowed to pass by the statement rules in ACL where it is designed to allow clean and valid data packets. Attackers can easily disguise their malware into data packets that are considered clean and valid by ACL, like by using a valid IP address through IP Spoofing.

Based on vulnerabilities taxonomy, this limitation of ACL belongs to other errors category. In the case of IP spoofing, this weakness belongs to validation error.

7. The Standard and Extended ACL do not have authentication method. Users' authentication is to test the validity of

users when they access network resources.

Authentication method generally uses user's name and password. Users who want to access system resources must give their name and password. Then, the authentication mechanism executes query into the system database for the matched account. If the account is matched, users then can access the resource. If not, then the users cannot have access to the system resource.

Since Standard and Extended ACL do not have authentication method, then there is no testing mechanism to check on users who want to have access on the system resources. Anyone can enter the system so long as they can meet the rule requirements in ACL lists, for example a valid IP address. Therefore, attackers are seen as the authentic users of the system once they can access the system. This is due to the state that the valid users of the system do not use account which enables it to distinguish them from invalid users. In conclusion, with no authentication method there is no mechanism to determine legal from illegal users. Consequently, there is no access control based on user account in which ACL cannot execute authentication test to any connection requests in determining legal from illegal users.

Based on vulnerabilities taxonomy method, this limitation is as authorization error category where ACL cannot carry out an authentication function to any connection requests that it cannot distinguish legal users from illegal users.

III. Conclusion

3.1. Conclusion

Referring to the analysis, here are the conclusions that can be drawn:

1. Access Control concept is used as one of the techniques in securing the system.
2. Cisco IP Access Control List (ACL) from Cisco System Inc. is an example of access control implementation on system Router.
3. ACL is a series list of statements with at

- least one permit statement and possibly with to or more deny statement.
4. A data packet will be proceeded if it meets the permit criterion but does not fit the deny statement. On the contrary, when the data packet does not fit the permit statement but meets the deny criterion, it will not be proceeded, either.
 5. The list of statements in the ACL is processed sequentially from the first until last line. Once a packet meets the requirements of a statement line in ACL, either permit or deny statement, an appropriate following action will be executed. This packet will not then be re-matched with the other lines.
 6. There are two types of IP address Control List: Standarad ACL and Extended ACL.
 7. Standard ACL only filters data packet based on the IP address of the packet sender.
 8. *Extended ACL* is able to filter data packet based on IP address of the sender, destination IP address, port number, and type of protocol used.
 9. The system administrator must set ACL which is already designed on an interface of Router and determine its filtering tasks course.
 10. ACL which is set to filter data packet coming through an interface is called inbound ACL. ACL which is set to filter data packet going out through an interface is called outbound ACL.
 11. ACL can be set on every interface of a Router with a condition one ACL is for one protocol and one filtering course.
 12. *Standard ACL* must be set as near the data packet destination as possible to avoid blocking valid data packets.
 13. *Extended ACL* must be set as near the data packet origin as possible to save network bandwidth. The data packet is not allowed to access the network is if it should be rejected.
 14. At the last line of every ACL there is an implicit deny line, that is a statement of deny all which functions to deny any packet that does not meet any one of the previous permit statements
 15. If an ACL does not have either one permit or deny statement, then it will not allow any data packet to pass.
 16. Vulnerabilities taxonomy method is very useful for analyzing and classifying weaknesses of a system systematically which is not only useful for solving the current problems, but it is also useful as the basis for solving the future problems to come..
 17. ACL can be used to design Packet Filtering Firewall which will execute filtering tasks upon any data packets.
 18. ACL is not a total solution in building a firewall system, not even a sole security system.
 19. The more lines an ACL has the more difficult to maintain its statement consistency which results in higher error probability.
 20. In filtering process, an ACL uses Router's resources. Thus, it decreases the entire Router's performance.
 21. ACL is stateless, therefore, is not able to check on the status of every running connection within the network.
 22. ACL cannot recognize and handle malware attacks.
 23. ACL is vulnerable to IP Spoofing or an act of disguising IP address.
 24. ACL does not have authentication method that it cannot distinguish legal from illegal users.

3.2. Suggestions

The following are suggestions on implementing ACL as a network security ware:

1. If data packet filtering statements are still simple, use Standard ACL for easier design, maintenance, and audit.
2. When the filtering statements are more complicated, use Extended ACL to accommodate the rules.
3. Before making the ACL, design the data packet filtering statements carefully.
4. Do not implement ACL on Router unless you are certain that the statement lines suit the rules you wish to apply.
5. Use IDS (Intrusion Detection System) to overcome ACL limitations in detecting dangerous data packet infiltrating the network.
6. Use NAT (*Network Address Translation*) and PAT (*port Address Translation*), security features in Cisco Router, to support ACL security function by hiding the internal network IP addresses.
7. Use RADIUS (*Remote Authentication Dial-In User Service*) or TACACS+ (*Terminal Access Controller Access Control System*), both of which are provided by Cisco, to overcome ACL limitations in authentication.
8. Use other security ware such as proxy

- server, antimalware application, bastion host, and more to support ACL functions.
9. Use honeypot for a more optimum security which requires skillful brainware to move any attack attempts.
 10. Always update Cisco IOS by visiting the authorized site of Cisco to get white paper and other important reports concerning the ware you use for your

- network system.
11. Visit sites which give the latest information on computer network security to anticipate attacks, security holes, and bugs on the ware you use in your network system.
 12. Use a management application to help you manage ACL easily, like Cisco Works.

Bibliography

Al-Wabel Abdulelah A. dan Al-Shayea Hamid I. 2009. *ACL Analysis Tool*. King Saud University. Saudi Arabia.

Benardi, Beny. 2004. *Membangun Firewall dengan Cisco Router*. Penerbit PT Elex Media Komputindo. Jakarta.

Brenton, Chris dan Hunt, Cameron. 2005. *Network Security*. Penerbit PT Elex Media Komputindo. Jakarta.

Cisco System, Inc. *Cisco IOS Security Configuration Guide Release 12.2SX*
[\[http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_2sx/sec_12_2sx_book.html\]](http://www.cisco.com/en/US/docs/ios/security/configuration/guide/12_2sx/sec_12_2sx_book.html)
 (Accessed November 17, 2008)

Cisco System, Inc. TACACS+ and RADIUS

Comparison

[\[http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml\]](http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a0080094e99.shtml) (Accessed January 14, 2008)

Habtamu, Abie. 2000. *An Overview of Firewall Technologies*. Norwegian Computing Center. Norway.

Ivan Victor, Krsul. 1998. *Software Vulnerability Analysis*. Purdue University. The United States of America.

Kamara, Seny dkk. 2003. *Analysis of Vulnerabilities in Internet Firewalls*. Purdue University. The United States of America.

Wright, Craig S.. 2007. *A Taxonomy of Information Systems Audits, Assessments and Reviews*. SANS Institute. The United States of America.