# Access Agent: Improving The Performance Of Access Control Lists

Thelis R. S., Lakshani H. G. S., Samarawickrama S. S., KavinMukesh A., Wickramasinghe W. A. S. M., Dhammearatchi D.

**Abstract:** The main focus of the proposed research is maintaining the security of a network. Extranet is a popular network among most of the organizations, where network access is provided to a selected group of outliers. Limiting access to an extranet can be carried out using Access Control Lists (ACLs) method. However handling the workload of ACLs is an onerous task for the router. The purpose of the proposed research is to improve the performance and to solidify the security of the ACLs used in a small organization. Using a high performance computer as a dedicated device to share and handle the router workload is suggested in order to increase the performance of the router when handling ACLs. Methods of detecting and directing sensitive data is also discussed in this paper. A framework is provided to help increase the efficiency of the ACLs in an organization network using the above mentioned procedures thus helping the organization's ACLs performance to be improved, to be more secure and the system to perform faster. Inbuilt methods of Windows platform or Software for open source platforms can be used to make a computer function as a router. Extended ACL features allow the determining of the type of packets flowing through the router. Combining these mechanisms allows the ACLs to be improved and perform in a more efficient manner.

**Index terms**: Access Control Lists, Extranet, Sensitive data, dedicated device, router workload, Meta-ACL profile, extended ACL

## 1 INTRODUCTION

MAINTAINING a secured and faster network is quite a challenge for a large organization with confidential data nowadays. Since the rapid growth of networked computers, security has been a concern. Before the 90s, networks were rarely used by the general public of heavy internet users. During these times, security was not considered critical, however with the addition of more sensitive information being placed on networks, it would grow in importance. In the 21st Century accomplishing specific tasks in every day needs with technology, one need to have a thorough knowledge of what needs to be performed. The proposed system try out to reduce the work-load of the router via allocating the access level to a computer. The proposed research is directed to computer networks, and more specifically, to a system and method for security access to network elements. Network resources and information are a principle asset of modern companies and must be protected against unauthorized access for usage, external threats, updates and violations, since these resources are being used in various elements such as switches, routers, signaling transfer points (STPs), mainframe computers, database servers, etc., Background of the research and the related researches conducted in this field are reviewed in chapter II. The approach taken to provide the solution is briefly described in chapter III. Finally the conclusion of the research and the future works that can be done regarding this research are also stated at the end of the research paper.

## 2 BACKGROUND AND RELATED RESEARCHES

Various researches have been carried out to discover new ways to stabilizing or to improve security of a computer network. The system follows the procedure of Firewalls that are developed to protect networks from unauthorized accesses. Various third parties may attempt to penetrate a network to obtain sensitive information or disrupt the functioning of the network. Firewalls guard against these threats and also inspect packets and sessions to determine if they should be transmitted or dropped. The firewalls have become a single point of network access which causes the traffic to be analyzed and controlled. The system implement a dedicated network device. The device which receive and transmits network traffic for limit the access to the local network. The system failed to access the degree of sensitiveness of their contents. The mechanism automatically detects privacy requirements of the publisher of data by the information that is sensitive. The reader with required qualification only can access such data [6]. Implementing redundancy in a business organization network is a necessity, thus the use of multiple firewalls is considered for this research. Policy mining approach is used to achieve the objectives of the research. An additional process for network access control policy mining is used. A method is shown on how to verify security properties of consistency when firewalls are being deployed. However this research does not focus on reducing the workload of the router when handling access lists, nor does it detect the sensitive data sent by a particular node. The proposed system will be built with the capability of tracking and detecting sensitive data and controlling network traffic. By using a dedicated computer to perform the tasks of the router, the router workload will be shared and reduced allowing the router to process faster. [8] In this research it discusses about how to control access to data entities in a computer network. It defines a method that uses a relational database to store the details about access rights of the users accessing a computer network. When the user tries to access the network, the application server will retrieve the access rights of that user with the use of a query. Then privilege levels for each user will be defined depending on the data entities the user is allowed to access. However this research does not facilitate controlling the packet flow or load balancing of the devices handling the Access Control. Proposed system discusses the lacking features of this research including router load balancing when handling Access Lists and the detecting and controlling of data packet flow .[4] The system follow the security mechanism called security policy to guard against external attacks and to control internal user access to the network elements. The network security mechanisms include an authentication server, a credential server, and a network element access server. System follow security mechanisms that can effectively control access to network elements and protect network resources. The system uses the concept of network-wide centralized user administration. The concept controls the access to individual network elements and access to network resources. System controls the user access by authentication method. Credential server manage the user privileges in the network associated with the authentication server. The network elements includes a separate local access control means operating with security mechanisms to facilitate secure communication of data over the network. The system does not consider about the dedicated devices used for access controlling. The proposed system follow this method to increase the secure level of the network to better levels by implement a dedicated network device such as a router positioned between a local network and an external network, most of the time the Internet, or between local networks. The system selectively examine packet payloads to figure out when new channels are to be opened. This mechanism help the system to be well maintained [5]. In this research it mainly focuses on dynamic access control for enterprise networks. Enterprise network security involves set of real time, defensive methods that are being used in an enterprise to protect its business network from external threats to their IT system. The research argues that the network layer with mechanisms for dynamic access control can remedy these ills. The research propose  a system for securing enterprise networks, where the network elements themselves enforce dynamic access control policies based on both flow-level information and real-time alerts. This research does not involve about router load balancing, data tracking or detecting sensitive data. In the proposed system the research group will discuss about router load balancing, data tracking and detect sensitive data. [7] The research focuses on user privacy in Online Social Networks (OSN). Users tend to expose their sensitive information accidentally in online textual messages because of the lack of technical knowledge of the user or the inflexibility of the access control mechanisms used in OSNs. The system detects such sensitive data depending on the publisher of the message with the use of an automatic semantic annotation mechanism. Then the system automatically generates a cleansed version of the publication according to the targeted audience of the data to control the access. Although this system keeps track of sensitive data and secure user access privacy, it does not provide a solution to prevent unauthorized users from accessing any of the sensitive data. The proposed system will track the sensitive data and prevent them from being accessed by third parties in order to secure the network access and sensitive data privacy [10]. Requirements for specification and implementation of access control policies have become more important in industrial networked systems. A twofold model for analysis of ACL policies includes three main components. They are; security policy document, control user access, high level network policy. Security policy document in the proposed system covers some important parts. For controlling user access, it needs a Meta ACL is generated. In the proposed system, the main purpose is to find a method to automate ACL system and also lessen the workload of a router. High level network policy should provide facilities to have a simpler, faster and more secured network. In order to do load balancing and good performance, and also to do access control, with the use of a dedicated device, our group intends to test whether a router and computer or a computer itself can handle ACL processing because computer is a more intelligent device compared to a router. The concept of style sheets transformation driven firewall access list generation will be used to secure network access. Controlling data traffic can be done in a few ways. Use two gateway routers in a larger LAN. Using ACL permitted actions, the traffic can be divided among two routers [9]. The research discusses about global server load balancing (GSLB). GSLB is popular for its disaster recovery functionality as well as for more intelligent direction of traffic of optimal site selection. In this research it is focused on identifying of the selected best IP addresses from GSLB algorithm and the selection metric used to decide on an IP address as the best one and the data includes a count of the selected best IP addresses selected via the GSLB algorithm. This research does not involve any type of controlling of data traffic, controlling user access or securing network access. Therefore in the proposed system we would facilitate traffic controlling, user access controlling, securing network access and detection of sensitive data. [2] This research is a concept, and also can be recognized as a method to make a secured network system which contains a few important components. They are; Meta ACL profile, data registry, security policy document, securing network policy, usage of firewalls. When there is a large network with multiple users, routers and switches with a lot of user access controls, it is difficult to create user access lists to every router and switch manually. It will increase the workload of a gateway device of a network. A router doing traffic filtering can deploy ACLs with thousands of rules. Due to the complications regarding ACL configuration language, large ACLs can easily become redundant, inconsistent, and difficult to optimize or even understand. There will be considerable amount of routers in the network topology of the proposed system. If it is done manually, all of the ACLs need to be configured in a consistent manner to enforce the corporate security policy. Although it takes a lot of time and it may not be accurate at all. There will be redundant ACLs, which is inconsistent. In order to overcome this problem, we need a novel framework to automate ACL analysis and make the network simpler. A set of algorithms is introduced to detect and remove redundant rules, discover and repair inconsistent rules, merge overlapping or adjacent rules, mapping an ACL with complex interleaving permit/deny rules to a more readable state containing all permits or denies, and finally generate a meta-ACL profile based on all ACLs along a network path. Traffic filtering is also needed. Data registry will keep the useful information about the network such as information related to the topology of the network. Documents that contain network security policies are linked to the registry data structure. When automating, and working with different devices, data registry is very important. Network security policy, is an outline for the network access with some defined rules. It determines how policies are enforced and lays out some of the basic architecture of the organization's security or network environment. It will cover the use of passwords and encryption, email attachments and more. For the proposed system we need a good network security policy which will balance the security and the network traffic both. Firewall devices block certain kinds of network traffic, forming a barrier between a trusted and non-trusted network. But, when there is a larger network with many divisions, requirements may differ making it more complex. [3] It is the task of the network administrator to correctly implement ACL in a large network environments of enterprise security policy which is a difficult task. With the topology of a plurality of routers, all ACL needs in a consistent manner the implementation of enterprise security policy configuration. In such a situation, manual analyzation of ACLs to ensure security policy is installed correctly is nearly an impossible task. In this research paper, an algorithm is introduced to detect and remove redundant rules, find and fix inconsistent provisions, merge overlapping or adjacent rules map complex cross license ACL in a more readable form containing all licenses or to reject the final calculation based on a blend of all ACL files and to generate a meta-ACL profile following the processes. This meta-ACL profile will help the Administrator understand the flow of traffic of the network once it is applied to the traffic filtering ACLs. A library named ACL Analysis (ACLA) is created based on the information provided on the research paper. A new framework for automated ACL analysis is provided in this research paper, greatly simplifying implementation and verification of corporate security policies at the network level security policy implementation, including configuration using ACL packet classification policy. [1]

## 3 OUR APPROACH

Currently, if there is a network with bigger LANs connected with different departments, the organization needs different access controls for different departments. That means routers in the network need to be programmed with different access control lists (ACLs). ACL is a helpful feature for controlling the filtering process of network traffic as well as providing an added feature of security. Using Network ACLs can be done the following; Permit or deny incoming traffic depending on remote subnet IPv4 address range to a virtual machine input endpoint.

- Use of blacklist IP addresses.
- Creating multiple rules per Virtual Machine (VM) endpoint.
- Specify up to 50 ACL rules per VM endpoint.
- Use rule ordering to ensure the correct series of rules are applied to a given VM endpoint (from lowest to the highest).
- Specify an ACL for a specific remote subnet IPv4 address.

There are two types of ACLs defined by the Cisco. Standard ACLs: This type of ACL is the simplest one since it only considers IP addresses when filtering. In other words, this ACL can be used only when there’s a need to permit or deny traffic from a certain host IP address or a certain source network. Extended ACLs: This type of ACL is the most preferred one and the most advanced as well. Using this type of ACL it allows to filter traffic based on: Source IP address, Destination IP address, Protocol (TCP or UDP), Port Numbers (Ftp 21 etc.). In the proposed research, to enhance the security and control IP traffic, Extended ACLs are suggested. If ACL is programmed manually, it is a very time consuming task. There will be a number of redundant ACLs which will make the network slower. In the proposed research the main purpose is to use a computer which is faster and can do more work load instead of a router. It can be divided in to two main parts. They are Windows based and Linux based. The main requirement is that the computer has to have at least two fast network interfaces installed in the system. Computer can either have two network cards or one network card and a wireless card. On Windows computers, the process of setting up this router functionality is called Internet Connection Sharing. A mechanism known as IP forwarding can also be used to make a computer function as a router connecting 2 to 3 separate networks. Linux based methods; there are four networking software. They are DD-WRT X86, ZeroShell, RouterOS, Untangle. These software are made for small networks using few computers without the need of a router. Computer is an intelligent machine that will help to identify sensitive data. The mechanism automatically detects the information that is sensitive depending on the privacy requirements of the publisher of data, with regard to the type of reader that may access such data. Finally, access control mechanism automatically creates sanitized versions of the user’s publications according to the type of reader that accesses them. In order to reduce the workload of the router user can implement ACLs in the computers. It will be more helpful to prevent threats including hackers, data theft etc. The components of this research are discussed in sub sections below.

### 3.1 Router Load Balancing

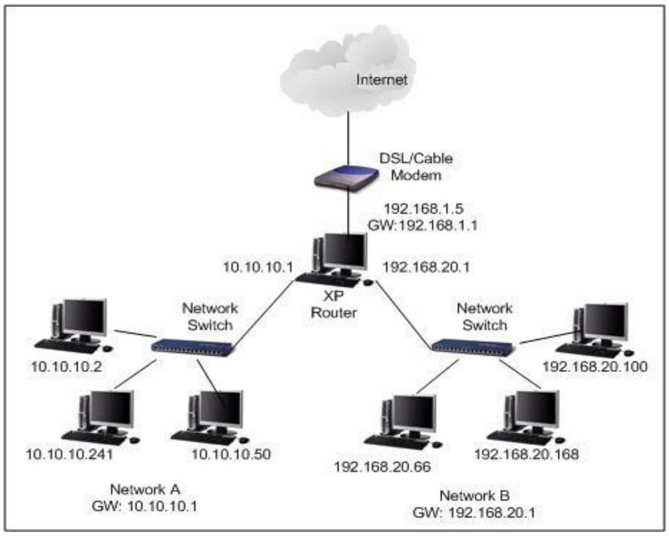
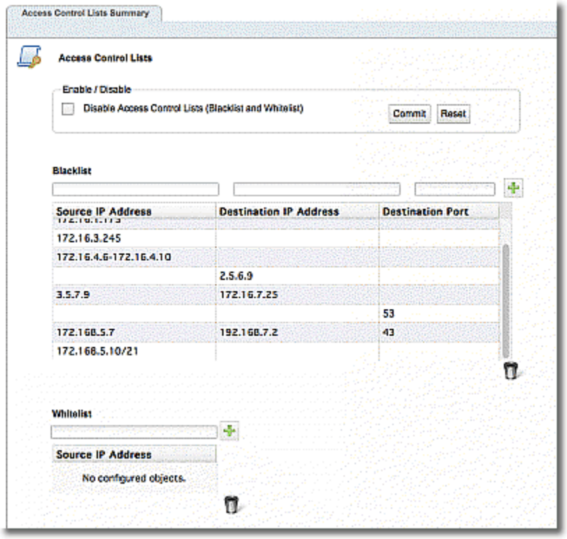


***Fig. 1.*** *IP forwarding using Windows XP platform (Source: http://www.home-network-help.com/images/xxp-router-network.jpg.pagespeed.ic.BjDSsKeQZx.jpg)*

The proposed research suggests a method that turning a computer into a gateway and router for network to balance the router workload. In Windows platform this can be performed using either IP forwarding method or Internet Connection Sharing. The software DD-WRT X86, ZeroShell, RouterOS and Untangle can be used to make a computer perform as a router in a small network. It is an ideal way to get advanced features over what is already provided in consumer-level routers. By converting computer into a router to share the workload, the intention is to free some of the work of the router to make it perform faster and to prevent the router from overloading/ overheating. The targeted network is a small sized business organization network which allows access for a selected group of outliers

(Extranet). Adding some features such as virtual LANs, multiple SSIDs, hotspot and captive portal, and VPN server and client capabilities are possible in a computer that acts as a router. Some machines provide network-wide antivirus, spam, and Web filtering. The proposed research includes a method that can receive the ordered list based on a set of performance metrics related to access conditions to host servers to arrange network addresses corresponding to the domain name. The order of IP addresses, and typically selects the first IP address on the list, when accessing the corresponding host server. The ordered list of network address is sent as a response to the query. The data related to the query is tracked. This tracking feature allows better understanding of Global Server Load Balancing policy decisions such as those related to performance, maintenance, troubleshooting and intelligent installation of large-scale flexible Global Server Load Balancing networks [2].

### 3.2 Controlling User Access



Access Control Lists Summary

Access Control Lists

Enable / Disable

□ Disable Access Control Lists (Blacklist and Whitelist)

Blacklist

| Source IP Address | Destination IP Address | Destination Port |
|---|---|---|
| 172.16.1.113 | | |
| 172.16.3.245 | | |
| 172.16.4.6-172.16.4.10 | | |
| | 2.5.6.9 | |
| 3.5.7.9 | 172.16.7.25 | |
| | | 53 |
| 172.168.5.7 | 192.168.7.2 | 43 |
| 172.168.5.10/21 | | |

Whitelist

| Source IP Address |
|---|
| No configured objects. |

***Fig. 2.*** *Fortinet ACL whitelist and blacklist [Source: http://help.fortinet.com/coyotepoint/10-3-2f/Content/Protection/AcessContList_Summary.gif)*

Various techniques are associated with controlling user accesses to objects and other data entities .There are

- Access Control Lists (ACLs)
- Storage of a capabilities list
- Firewalls

Among these techniques, the proposed research will be using ACLs: This technique which is commonly used in file systems, involves the storage of an ACL for each data entity to which the access is to be controlled. The ACL for a given data entity will usually be in a list of the users that have access to the data entity, together with the access rights of each such user regarding the data entity. Each time a request is sent to the entity, the data entity's ACL is searched to determine whether the requested access is authorized. ACLs possesses two types of lists to control the user access to a network depending on the user's IP address, namely Whitelist and Blacklist. The whitelist allows access for a specific IP address or an address range. If the address or the range is included in the blacklist that packet will be dropped. If the address or range is a sub part of a larger range defined in the blacklist, the whitelist will take precedence for the specified addresses. If the blacklist is free of addresses and there are only addresses listed in the whitelist, then only the addresses listed in the whitelist are allowed and connections from all other addresses are blocked.

### 3.3 Controlling Data Traffic

ACLs support data traffic controlling. The process is done in the router by controlling whether the packets received are forwarded or dropped based on criteria specified within the ACL. These criteria may include source IP address, destination IP address or any other relevant information of the packets received. ACL can be implemented in firewall routers between an external network and the LAN network or it can be implemented between separate parts of the same network. The focus of this research is to implementation of the router between the LAN and the external network to secure the data that is flowing out of the network or to prevent irrelevant traffic generated from unauthorized third party outliers. Use of Extended ACLs (figure 5 in Appendix) are suggested for this research implying that the ACLs must be implemented for each protocol of the network. The criteria statements have to be clearly defined as every ACL contains "deny all traffic" criteria statement at the end of the statements list, which will drop whatever the packet that does not match any other criteria defined. The order in which the criteria statements are listed deemed important as the list will be checked in a sequential order once a packet is received, until a match is found. The statements listed below the matching statement will not be checked, hence an ordered ACL will help the router to perform faster and more efficiently.

### 3.4 Detecting Data Types and Data tracking

The type of packets forwarded or blocked can also be determined using ACLs. As stated above in section C, implementing Extended ACLs require implementation of ACLs for each protocol on a network interface, which allows the tracking of the type of data flowing through the network, for example: sharing of emails can be allowed in the network while preventing the TELNET communications [11]. Tracking of the source and destination of a packet can be determined using the IP addresses. Using the statements listed in ACLs, it is suggested to generate a meta-ACL profile [1] [3] to provide a better understanding of the network including the destination and the source of the packet sent to the outside of the network. Analyzation of the meta-ACL profile will allow the network administrator to identify any sort of unauthorized access to the network as well as leakage of sensitive information of the organization to a third party through an employee.

## 4 Conclusion

Maintaining a well performing ACL is very important in a network. This research paper discusses about a method to share the workload of the router that is handling the ACL, with a computer that is solely dedicated for the stated purpose to prevent the router from overloading. This paper also focuses on the technology of tracking the data flowing outside of an extranet with the use of ACLs to detect sensitive data and prevent it from reaching unauthorized third parties. Internet Connection Sharing and IP forwarding methods are used for Windows platforms and Software: DD-WRT X86, ZeroShell, RouterOS and Untangle are used for Open source platforms to convert a computer into a router to share the workload of a router. Extended ACLs and IP addresses are used to detect the type, source and destination of the packets sent from the network and a packet will be dropped if it is directed to an unauthorized destination. A meta-ACL profile will be generated based on the criteria of the ACL to allow a better understanding of the network. A combination of these technologies are suggested by the research group to improve the performance of a router inside a small organization network.

## 5 Future work

The major drawback of the proposed research is that it is only limited to a small organization extranet where only a few network interfaces or sub interfaces are implemented. With the use of a higher performance computer it might be possible to apply this system to a larger network. Analyzing of the machine generated meta-ACL profile may take less effort if an algorithm is introduced to perform the said task using the router itself or the computer sharing the router workload.

## Acknowledgement

We thank Mr. Dhishan Dhammearatchi for providing the assistance and feedbacks/ comments to carry out this research and steering us in the right direction. We would also like to thank the SLIIT Computing (PVT) LTD and other individuals/groups that helped us achieve this target.

## References

[1] J. Qian, S. Hinrichs and K. Nahrstedt, "ACLA: A Framework for Access Control List (ACL) Analysis and Optimization", Communications and Multimedia Security Issues of the New Century, pp. 197-211, 2001.

[2] S. Kommula, I. Hsu, R. Jalan and D. Cheung, "Patent US7254626 - Global server load balancing", Google Books, 2016. [Online]. Available: http://www.google.com/patents/US7254626. [Accessed: 02- Feb- 2016].

[3] L. Cheng, "Style sheet transformation driven firewall access list generation", Google Books, 2002. [Online]. Available: http://www.google.com/patents/US20020184525. [Accessed: 03- Feb- 2016].

[4] R. Brown and R. Greenberg, "System and method for controlling access to data entities in a computer network", Google Books, 1999. [Online]. Available: http://www.google.com/patents/US5941947. [Accessed: 03- Feb- 2016].

[5] J. He and R. Hall, "Security system and method for network element access", Google Books, 2000. [Online]. Available: http://www.google.com/patents/US6088451. [Accessed: 02- Feb- 2016].

[6] S. Fan and S. Truong, "Access control for networks", 2001. [Online]. Available: https://www.google.com/patents/US6219706. [Accessed: 02- Feb- 2016].

[7] A. Nayak, A. Reimers, N. Feamster and R. Clark, "Resonance", Proceedings of the 1st ACM workshop on Research on enterprise networking - WREN '09, 2009. [Online]. Available: http://dl.acm.org/citation.cfm?id=1592684. [Accessed: 02- Feb- 2016].

[8] S. Hachana, N. Cuppens-Boulahia and F. Cuppens, "Mining a high level access control policy in a network with multiple firewalls", Journal of Information Security and Applications, vol. 20, pp. 61-73, 2015.

[9] I. Cibrario Bertolotti, L. Durante, L. Seno and A. Valenzano, "A twofold model for the analysis of access control policies in industrial networked systems", Computer Standards & Interfaces, vol. 42, pp. 171-181, 2015.

[10] M. Imran-Daud, D. Sánchez and A. Viejo, "Privacy-driven access control in social networks by means of automatic semantic annotation", Computer Communications, vol. 76, pp. 12-25, 2016.

[11] "Cisco IOS Security Configuration Guide, Release 12.2 - Access Control Lists: Overview and Guidelines [Cisco IOS Software Release 12.2]", Cisco, 2016. [Online]. Available: http://www.cisco.com/c/en/us/td/docs/ios/12_2/security/configuration/guide/fsecur_c/scfacls.html. [Accessed: 01- Mar- 2016].

## APPENDIX

***TABLE 1***

*RELATED RESEARCHES AND COMPONENTS*

| Features<br>Researches | Simplified access list | Meta-ACL profile | Global server/router load balancing | Sorted IP list | Selecting best IP address | Data tracking | Data registry | Security policy document | Controls user access | Securing network access | Registration database | Dedicated device(s) for access control | High level network policy | Use firewalls | Detect sensitive data | Control data traffic |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| ACLA: A framework for Access Control List analysis and optimization [1] | ✓ | ✓ | × | × | × | × | × | × | ✓ | ✓ | × | × | × | × | × | × |
| Statistical tracking of global server load balancing for selecting the best network address from ordered list of network addresses based on a set of performance metrics [2] | × | × | ✓ | ✓ | ✓ | ✓ | × | × | × | × | × | × | × | × | × | × |
| Style sheets transformation driven firewall access list generation [3] | × | ✓ | × | × | × | × | ✓ | ✓ | × | ✓ | ✓ | × | ✓ | ✓ | × | × |
| System and method for controlling access to data entries in a computer network [4] | × | × | × | × | × | ✓ | ✓ | × | ✓ | × | ✓ | × | × | × | × | × |
| Security system and method for network element access [5] | × | × | × | × | × | × | × | × | ✓ | ✓ | ✓ | × | × | × | × | × |
| Access control for networks[6] | × | ✓ | × | × | × | × | × | × | ✓ | × | × | ✓ | × | ✓ | × | ✓ |
| Resonance: dynamic access control for enterprise networks. [7] | × | × | × | × | × | × | × | × | ✓ | ✓ | × | ✓ | × | × | × | ✓ |
| Mining a high level access control policy in a network with multiple firewalls [8] | × | × | × | × | × | × | × | ✓ | ✓ | ✓ | × | × | ✓ | ✓ | × | × |

| | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| A twofold model for the analysis of access control policies in industrial networked systems [9] | × | × | × | × | × | × | × | ✓ | ✓ | × | × | × | ✓ | × | × | × |
| Privacy driven access control in social networks by means of automatic semantic annotations [10] | × | × | × | × | × | ✓ | × | × | ✓ | ✓ | ✓ | × | × | × | ✓ | × |
| Proposed system | × | × | ✓ | × | × | ✓ | × | × | ✓ | ✓ | × | ✓ | × | × | ✓ | ✓ |

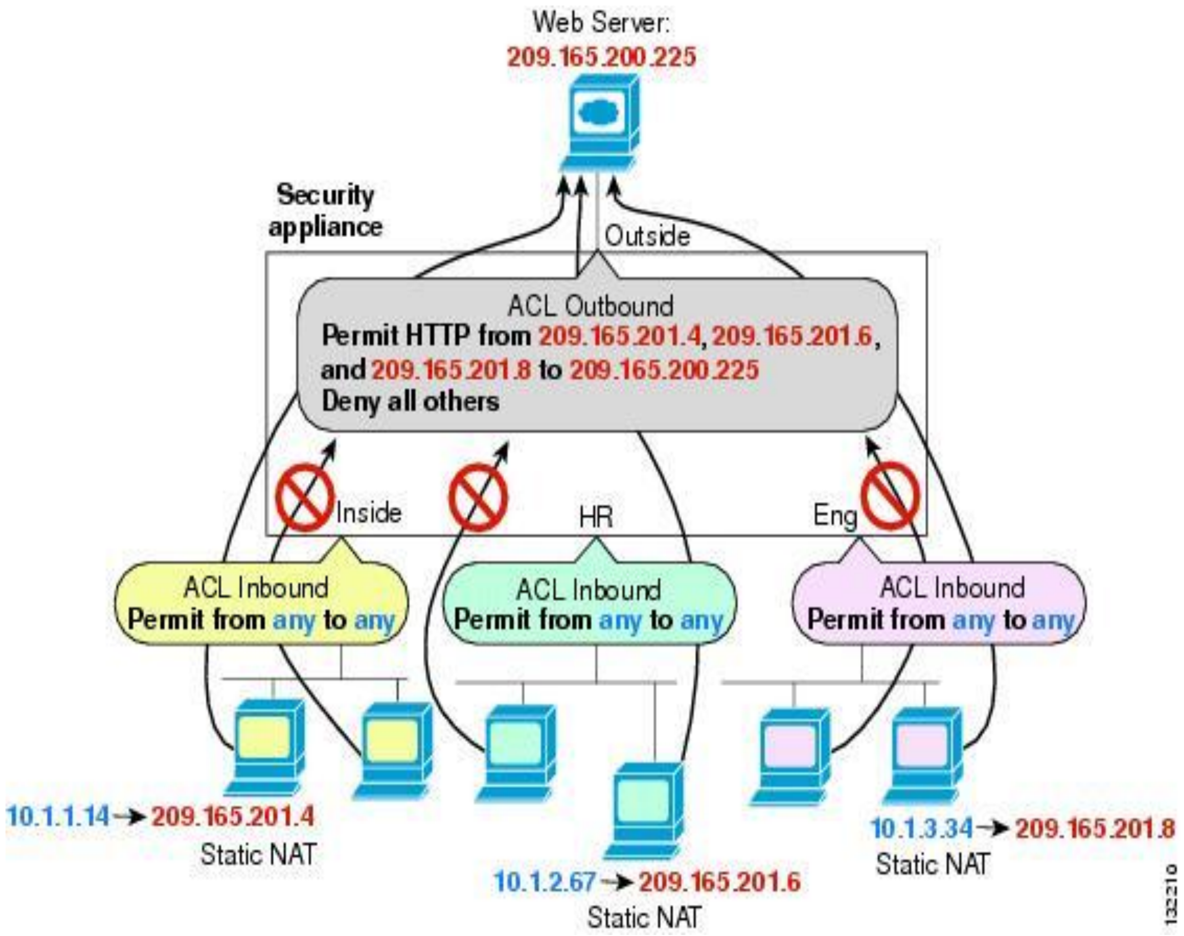


***Fig. 3.** Outbound ACL*
*(**Source:** http://www.cisco.com/c/en/us/td/docs/security/asa/asa70/configuration/guide/config/nwaccess.html)*

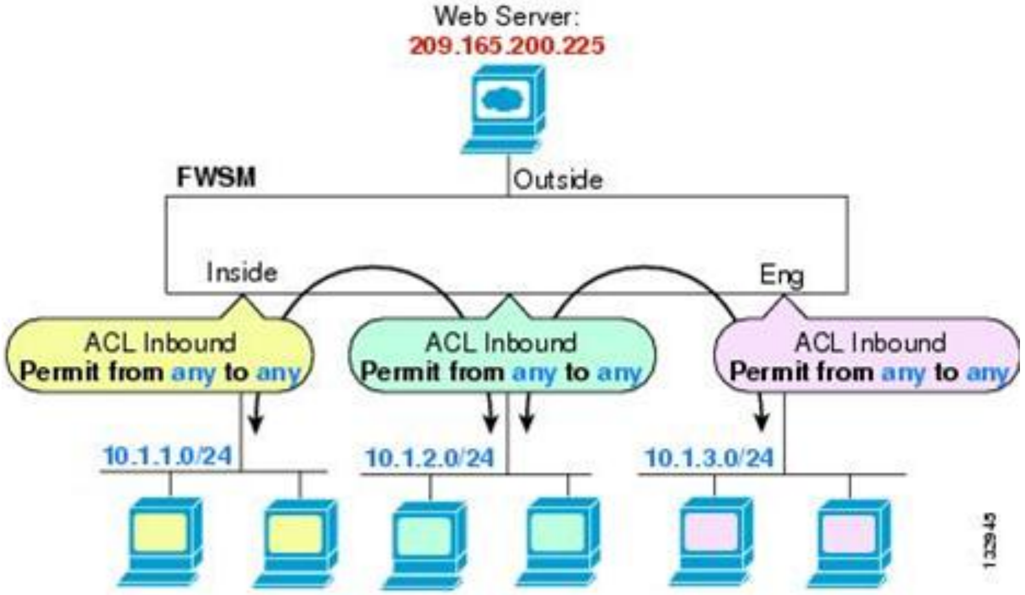
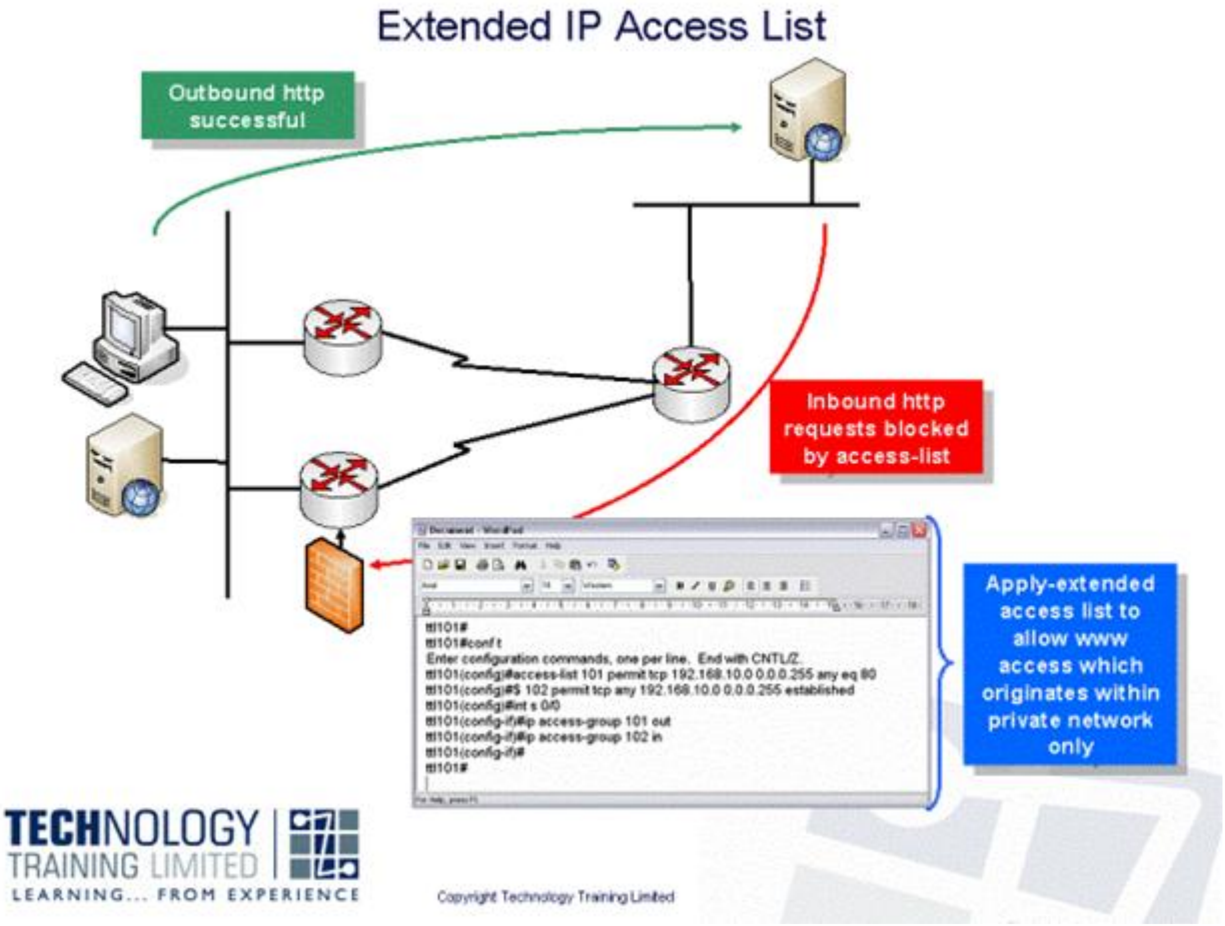


Fig. 4. Inbound ACL (Source: http://www.cisco.com/c/en/us/td/docs/security/fwsm/fwsm31/configuration/guide/fwsm_cfg/mwacc_f.html)


Extended IP Access List
Outbound http successful
Inbound http requests blocked by access-list
Apply-extended access list to allow www access which originates within private network only
TECHNOLOGY TRAINING LIMITED
LEARNING... FROM EXPERIENCE
Copyright Technology Training Limited

```
ttl101#
ttl101#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
ttl101(config)#access-list 101 permit tcp 192.168.10.0 0.0.0.255 any eq 80
ttl101(config)#$ 102 permit tcp any 192.168.10.0 0.0.0.255 established
ttl101(config)#int s 0/0
ttl101(config-if)#ip access-group 101 out
ttl101(config-if)#ip access-group 102 in
ttl101(config-if)#
ttl101#
```

***Fig. 5.*** *Extended IP ACL (Source: http://www.technology-training.co.uk/ciscoipaccesslists_49.php)*