Logo, company name

Description automatically generated

**GROUP ASSIGNMENT**

**(INDIVIDUAL WORK)**

**CT128-3-2-ISC**

**Implementation of Secure System**

**HAND OUT DATE: 3rd WEEK**

**HAND IN DATE: 14TH WEEK**

**INTAKE CODE:** APD2F2309CS(CYB)

**MODULE CODE:** CT128-3-2-ISC

**STUDENT NAME:** ABDULRAHMAN GAMIL

MOHAMMED AHMED

**STUDENT TP:**  TP071012

Contents

[1.0 Overview of Access Control List (ACL) 3](#_Toc168696558)

[1.1 Introduction 3](#_Toc168696559)

[1.2 Importance of Access Control List (ACL) 5](#_Toc168696560)

[1.3 How does an ACL Work 5](#_Toc168696561)

[1.4 Types of ACL 7](#_Toc168696562)

[1.5 Recent Issues and Challenges 14](#_Toc168696563)

[2.0 Vulnerabilities and Potential Attacks 16](#_Toc168696564)

[2.1 Vulnerabilities 16](#_Toc168696565)

[2.1.1 Overlapping Rules 16](#_Toc168696566)

[2.1.2 Complexity and Misconfiguration 17](#_Toc168696567)

[2.2 Potential Attacks 18](#_Toc168696568)

[2.2.1 IP Spoofing Attacks 18](#_Toc168696569)

[2.2.2 Denial of Services (DoS) Attacks 19](#_Toc168696570)

[3.0 Best Practices / Techniques 21](#_Toc168696571)

[4.0 Conclusion 23](#_Toc168696572)

[5.0 References 24](#_Toc168696573)

1.0 Overview of Access Control List (ACL)

1.1 Introduction

Implementing corporate security rules in an efficient manner is a fundamental responsibility of a network administrator. This task is particularly challenging in large companies and Internet service provider (ISP) settings. The expansion of the network's firewall and router count leads to the creation of an intricate architecture and a marked increase in network administration tasks.

Packet categorization is a crucial aspect of network security policy enforcement, created using Access Control Lists (ACLs). These ACEs are an ordered list of rules, collectively known as a packet categorization system. A router's ACL is composed of these ACEs, which are commonly referred to as packet classification, packet filtering, or ACL matching.

A packet is examined at various points as it goes through a router or firewall to determine whether it matches any ACLs. If a match is found, a predetermined set of actions is taken. An example might be an ACL that filters traffic on a network gateway, allowing or denying packets based on preset criteria. Traffic filtering provides administrators with a powerful mechanism to control the flow of packets. ACLs can be used to construct corporate VPNs along with security protocols like IPSec. VPNs are an effective alternative for leased lines because they use pre-existing Internet infrastructures. In a VPN, gateway devices are equipped with ACLs to classify traffic that is entering protected tunnels (Qian et al., 2001).

While ACLs are vital to ensuring the security of corporate networks, an ACL configuration can still be a tedious, slow, and error-prone process to verify and understand. Fig. 1. The following series of steps provides an example of a simple ACL configuration for filtering traffic on a Cisco router:

A black screen with white and blue text

Description automatically generated

1

1.2 Importance of Access Control List (ACL)

ACLs are important in network security because they help to do the following:

* **Secure Access**: ACLs, in limiting unauthorized access, secure sensitive data by limiting which users can access which servers, network segments, and services.
* **Defend Against Cyber threats**: ACLs make the network secure from malware and other cyber threats by blocking unused or vulnerable ports.
* **Optimize Network Bandwidth**: ACLs prioritize the important traffic. So, services that require more bandwidth, such as voice and video, remain high in quality. They also control and monitor network traffic (What Is Access Control List (ACL) and How Does It Work？ | FS Community, 2024).

1.3 How does an ACL Work

The operating system uses a filesystem Access Control List (ACL) table to determine which users can access which files or directories. Each object in the system has a security property that relates it to its ACL, which describes the access privileges of each of the users.

You may have come across an ACL when opening or editing a file on your computer. For instance, administrators may be the only ones with access to some files. When you log in as an administrator, you are not allowed access; however, access is allowed when you log in as an ordinary user.

Network ACLs and security groups share an aspect: that they have lists of users provided access to specific resources. A security group could be a set of users or groups, like visitors and administrators.

Before the operating system allows access to an item, the user's request for access is filtered against the ACL. Access is denied if a user has no authorization.

For switches and routers to filter traffic, they use network ACLs and not filesystem ACLs. The ACLs verify contents in packets against access parameters, by following set rules. The user either gets access or does not get access based on the result. When the device controls network traffic, it is acting as a filter for packets, searching for IP addresses, ports, and protocols (What Is a Network Access Control List (ACL)? | Fortinet, 2022).

1.4 Types of ACL

The following are the two main types of Access Control Lists (ACLs):

**1** **File system ACLs**: These are used to control who can access which files and directories on a computer system. They provide the operating system with a guideline of what users can do and in which files or locations. For example, one user might have read access to a file, whereas another user might have write access to the same file if there is a file system ACL in place. (Lutkevich, 2022).

A screen shot of a computer

Description automatically generated

2

**2 Networking ACLs**: These control access to network resources by setting rules for switches and routers. Networking ACLs specify the types of data that can enter or leave the network, as well as the actions that can be carried out by users while on the network. Networking ACLs are developed by a network administrator, and they operate by screening traffic according to predefined rules, in a manner like a firewall. For example, a networking ACL may allow traffic to websites while denying file-sharing traffic to maintain performance and security (Lutkevich, 2022).

A diagram of a computer network

Description automatically generated

3

ACLs can also be further classified into the following five broad categories based on how they identify and respond to traffic:

**1 Standard ACLs:** These are the most basic forms of ACLs, restricting only on the source IP address. They, therefore, provide limited traffic control by permitting or denying the entire protocol suite from a given source. A common example of an ACL might block all traffic from a particular IP address known to have been a source of malicious activity (upravnik, 2016).

A diagram of a computer network

Description automatically generated

4

**2 Extended ACLs:** These are more advanced forms of ACLs, made to be more specific in traffic control. This follows the fact that several factors are considered, such as source and destination IP addresses and port numbers. Accordingly, traffic filtering can be more specific. An extended ACL, for example, could permit HTTP traffic from an IP address while simultaneously rejecting FTP traffic in order to optimize resources and ensure network security (upravnik, 2016).

A diagram of a computer network

Description automatically generated

5

**3 dynamic ACLs:** Dynamic Access Control Lists (ACLs), also known as "Lock and Key" ACLs, enhance security by combining Telnet, authentication protocols, and improved ACLs. They control access based on specific characteristics and time periods, allowing more appropriate control once users are successfully authenticated through Telnet. Dynamic ACLs are useful for temporary access, such as allowing contractors temporary access to network resources. (What Is an Access Control List (ACL)? - IT Glossary | SolarWinds, 2024).

A close-up of a diagram

Description automatically generated

6

**4 Reflexive ACLs:** sometimes known as IP session ACLs, are used to filter IP traffic based on the session data emanating from higher levels of the OSI model. They are designed to permit IP traffic entering the network but to deny access to sources that are not verified or anything originating from without the network. This method enhances network security by restricting access from outside the network to only permitted traffic from inside. Reflexive ACLs are best suited for controlling and securing session traffic going outside (What Is an Access Control List (ACL)? - IT Glossary | SolarWinds, 2024).

A diagram of a diagram

Description automatically generated

7

**5 Time-based ACLs:** Extended Access Control Lists (ACLs) are a type of network security policy that allows network administrators to implement access control rules based on specific times of the day and week. This allows them to restrict or deny traffic at specific times, such as restricting access to network resources at the end of business hours. This type of ACL is useful for setting dynamic security policies, such as accessing key systems outside official working hours, to minimize the risk of unauthorized access. (What Is an Access Control List (ACL)? - IT Glossary | SolarWinds, 2024).

A diagram of a schedule

Description automatically generated

8

1.5 Recent Issues and Challenges

1. **Complexity of Large Network Infrastructures**: Many ACLs are distributed across multiple devices in large network environments. Keeping a record of these ACLs, understanding their dependencies, and ensuring that these ACLs conform to the general network and security regulations is cumbersome. Mistakes and misconfigurations can be easily triggered by the huge quantity of ACLs and their interactions (Kannan, 2024).

2. **Human error**: The set up of ACL is meticulous and, therefore, prone to human error. Common errors can result in disaster, like typographical IP addresses or improper order of rules. Furthermore, in a dynamic networking environment with changing roles and network architecture, network managers might find it very hard to handle redundant or obsolete policies. (Kannan, 2024)

3. **Lack of Centralized administration and Visibility**: When there is no centralized administration, it is hard to keep a precise view of the ACL rules across the network. Since visibility into discrepancies or misconfigurations is absent, it is difficult to fix them, and even if they are found, it is an arduous and time-consuming task to repair them. Dispersed network infrastructures are only compounded by this problem, necessitating centralized monitoring while often never realized (Kannan, 2024).

4. **Security Implications**: Serious security flaws may come out of improperly set ACLs. Rules that are not set correctly can open doors for attackers and provide access to network resources without authorization. This may cause sabotage, theft, or data breaches. For example, opening traffic to some malicious sources may make it more straightforward for a malicious attacker to initiate a network attack (Kannan, 2024).

5. **Operational inefficiency**: Excessively permissive ACLs might enable unnecessary network traffic, which results in wasteful use of network resources and poor performance. On the other hand, too strict ACLs might block valid traffic, which will damage important network functions. The balance is difficult to strike yet necessary to be struck (Kannan, 2024).

2.0 Vulnerabilities and Potential Attacks

2.1 Vulnerabilities

**What is vulnerability?** A security vulnerability in software and hardware components can lead to system confidentiality, integrity, or availability issues. Correcting these vulnerabilities often requires coding changes, but specification modifications or deprecations may also be necessary. (i.e., removing all affected protocols or functionality) will be necessary (NVD - Vulnerabilities, 2022).

2.1.1 Overlapping Rules

When multiple rules in an ACL apply to the same traffic but invoke different actions, they have overlapping rules. Overlapping rules can lead to unintentional security gaps, operational issues, and additional complexity in the management of ACLs. To keep your network safe and operational, you must understand and resolve overlapping rules (Overlapping ACL Rules, 2016).

**Description**: Conflicts resulting from redundant or overlapping ACL rules might undermine the desired security posture.

**Impact**: Attackers can more easily bypass security mechanisms or disrupt legitimate traffic due to these types of disputes.

**Optimization**: Use ACL optimization tools to eliminate redundant or overlapping rules, to create a concise and efficient rule set.

2.1.2 ****Complexity and Misconfiguration****

While Access Control Lists (ACLs) are critical for maintaining security in a network, their complexity can result in errors that compromise security, leading to problems in operation. Effective network security requires an understanding of the causes and effects of complexity and misconfiguration (Wen et al., 2006).

**Description**: As the size of networks grows, ACLs become more complex. Human error can create misconfigurations in applying rules.

**Impact**: Incorrectly set ACLs may either be too permissive, allowing unauthorized access, or be too restrictive, leading to operational difficulties in authorized access.

**Mitigation**: Use automated tools to perform configuration management; perform comprehensive testing on ACL rules; and conduct regular audits to help reduce error rates.

2.2 Potential Attacks

Even when they are a fundamental part of network security, Access Control Lists (ACLs) can fall prey to several types of attacks unless they are deployed and administered properly. Some of the potential attacks are:

2.2.1 IP Spoofing Attacks

IP spoofing is a method used by attackers to alter their identity by altering the source address of packets, making them appear as originating from a trustworthy source, thereby changing their identity.

A computer screen with words and a diagram

Description automatically generated with medium confidence

9

**Description**: To bypass ACLs that restrict traffic based on IP addresses, attackers spoof themselves as the originating IP address.

**Impact**: Unauthorized access to network resources, allowing attackers to pose as trustworthy people or systems.

**Mitigation**: IDS can be used to detect and stop spoofing packets, and the use of strong IP filtering is recommended in conjunction with anti-spoofing techniques.

**How IP Spoofing Operates**  
1. **Packet Creation**: By using a faked source IP address, attackers create network packets. One can use custom scripts or a variety of tools to construct these packets.  
2. **Transmission of Packets**: The target network receives fraudulent packets. The victim thinks the packets are coming from a reliable source since the source IP has been spoofing.  
3. **Manipulation of Responses**: The attacker must handle responses provided to the fake IP address if the attack entails two-way communication. Additional methods, such as man-in-the-middle (MitM) assaults, are frequently needed for this (What Is IP Spoofing? - Zenarmor.com, 2022).

2.2.2 Denial of Services (DoS) Attacks

A Denial of Service (DoS) attack is a method where unauthorized requests are thrown at a target to prevent legitimate users from accessing the network resource, often done through IP spoofing, making identification and prevention more complex.

A diagram of a computer network

Description automatically generated

10

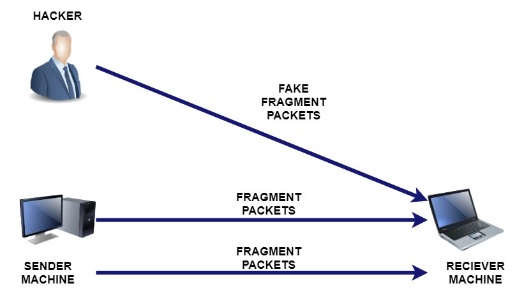
**Description**: Cyber criminals search the network for weak ports that are not well protected by ACLs.

**Impact**: Deciding on what service is a vulnerable point that can be exploited as a launch pad for further attacks.

**Mitigation**: Ensure that ACLs are configured to avoid unnecessary open ports, regularly check port configurations, and use firewalls and intrusion detection systems to detect and prevent port scanning (Omran Hawedi et al., 2020).

2.2.3 Fragmentation Attacks

Fragmentation attack is a process of trying to put together and break packets in data over a network. Attackers take advantage of this process to bypass security.



11

**Description**: Attackers break down malevolent payloads to avoid inspection and filtering by ACL.

**Consequences**: Malicious traffic is allowed to enter the network when security measures are bypassed.

**Mitigation**: Employ advanced IDS, devices that can reassemble and inspect broken packets, and ensure the correct setup of ACLs to handle fragmented traffic (Access Control Lists and IP Fragments, 2021).

3.0 Best Practices / Techniques

1. **Start your ACL by establishing a Deny All Rule:** Denial of service (DoS) improves security by creating a controlled environment where only essential communications are allowed, reducing potential vulnerabilities and allowing for careful permission building for specific traffic types. (Sushant Katare, CISSP, 2024).
2. **Take Advantage of the Implicit Deny:** Most network devices have an implicit deny statement at the end of an ACL that essentially denies all traffic not following the stipulated rules. Understanding this default behavior and using it in making your network security stronger is important. Your defense against possible dangers becomes strong when you realize and take advantage of the implicit deny, making certain that any unauthorized or unexpected traffic is instantaneously denied (Sushant Katare, CISSP, 2024).
3. **Simplify and Organize ACLs**: Complex ACLs can be more difficult to maintain and more prone to mistakes. To improve accuracy and expedite maintenance, go for simplicity and organization. To aid with comprehension and simplify troubleshooting, use comments and naming standards that are obvious. By keeping things organized and simple, you may reduce the possibility of errors in setup and increase the general effectiveness of administering your network security settings (Sushant Katare, CISSP, 2024).
4. **Test and Verify:** Carry out thorough testing and verification processes in a controlled environment before installing ACLs in a production environment. This enables you to evaluate the ACLs' intended behaviour, spot any conflicts or unexpected results, and adjust settings as necessary. By doing thorough testing, you can make sure that your ACLs operate as planned, reducing the possibility of errors or vulnerabilities when they are implemented in live settings (Sushant Katare, CISSP, 2024).
5. **Monitor and Review:** Regularly assess and evaluate ACL management decisions to detect changing security and business requirements. Regular upgrades account for modifications to threaten landscapes or network infrastructure. Vigilant and flexible ACL maintenance ensures a strong security posture that adapts to company needs, ensuring a robust security posture (Sushant Katare, CISSP, 2024).

4.0 Conclusion

In conclusion, Access Control Lists (ACLs) perform an essential function within the network security infrastructure through the facilitation of traffic filtering and access control. There are some challenges involved in implementing and administering them, including complexity and the potential for human errors. Network administrators should exercise caution when implementing ACLs. Organizations can enhance their overall security posture and safeguard their critical information from unauthorized access by implementing steps to streamline ACL administration and minimize exposure. Ongoing monitoring and recurrent evaluations are necessary to ensure that ACLs remain functional in the face of emerging challenges in security. In the ever-evolving world of cybersecurity, maintaining the integrity and resilience of a network defense ultimately will involve a proactive approach to ACL management.

5.0 References

* + Qian, J., Hinrichs, S., & Nahrstedt, K. (2001). ACLA: A Framework for Access Control List (ACL) Analysis and Optimization. *IFIP Advances in Information and Communication Technology*, 197–211. <https://doi.org/10.1007/978-0-387-35413-2_18>
  + *What Is a Network Access Control List (ACL)? | Fortinet*. (2022). Fortinet. https://www.fortinet.com/resources/cyberglossary/network-access-control-list

‌

* + Lutkevich, B. (2022). *access control list (ACL)*. Networking; TechTarget. https://www.techtarget.com/searchnetworking/definition/access-control-list-ACL

‌

* + upravnik. (2016, January 26). *ACL Types: Standard and Extended - Study CCNA*. Study CCNA. https://study-ccna.com/types-of-acls/

‌

* + *What Is an Access Control List (ACL)? - IT Glossary | SolarWinds*. (2024). Solarwinds.com. https://www.solarwinds.com/resources/it-glossary/access-control-list-acl

‌

* + *What is Access Control List (ACL) and How Does It Work？ | FS Community*. (2024). Knowledge. https://community.fs.com/article/what-is-access-control-list-acl-and-how-does-it-work.html

‌

* + Kannan, Y. (2024). Access control list (ACL) Compliance Verification and Alarm Systems: Strengthening Network Security. *Authorea (Authorea)*. https://doi.org/10.22541/au.171011477.72357180/v1

‌

* + *What is IP Spoofing? - zenarmor.com*. (2022). Zenarmor.com. https://www.zenarmor.com/docs/network-security-tutorials/what-is-ip-spoofing

‌

* + Omran Hawedi, Kaled Ben Taher, Yousef Abodhir, & Yousef Abuadlla. (2020, April 6). *Using Access Control List Againest Denial of Service Attacks Using Access Control List against Denial of...* ResearchGate; unknown. https://www.researchgate.net/publication/340464274\_Using\_Access\_Control\_List\_Againest\_Denial\_of\_Service\_Attacks\_Using\_Access\_Control\_List\_against\_Denial\_of\_service\_attacks

‌

* + *Access Control Lists and IP Fragments*. (2021, July). Cisco. https://www.cisco.com/c/en/us/support/docs/ip/generic-routing-encapsulation-gre/8014-acl-wp.html

‌

* + *NVD - Vulnerabilities*. (2022). Nist.gov. https://nvd.nist.gov/vuln

‌

* + *Overlapping ACL rules*. (2016). Solarwinds.com. https://documentation.solarwinds.com/en/success\_center/ncm/content/ncm-overlappingaclrules.htm

‌

* + Wen, E., Wong, W., & Gibson, J. (2006). *NAVAL POSTGRADUATE SCHOOL MONTEREY, CALIFORNIA THESIS Approved for public release; distribution is unlimited VALIDATING NETWORK SECURITY POLICIES VIA STATIC ANALYSIS OF ROUTER ACL CONFIGURATION*. https://apps.dtic.mil/sti/pdfs/ADA462558.pdf

‌

* + Sushant Katare, CISSP. (2024, March 4). *Understanding Access Control Lists (ACLs) for Robust Cybersecurity*. Medium; Medium. https://sushantkatare.medium.com/understanding-access-control-lists-acls-for-robust-cybersecurity-428b1926d6df

‌