



ITEC 85C

Information Assurance and Security

Learning Module

Ramil V. Huele
Instructor I



Security Technology: Firewalls

Objectives:

- Recognize the important role of access control in computerized information systems, and identify and discuss widely-used authentication factors
- Describe firewall technology and the various approaches to firewall implementation

I. Introduction

- Technical controls are essential to a well-planned information security program, particularly to enforce policy for the many IT functions that are not under direct human control.
- Networks and computer systems make millions of decisions every second and operate in ways and at speeds that people cannot control in real time.
- Technical control solutions, properly implemented, can improve an organization's ability to balance the often conflicting objectives of making information readily and widely available and of preserving the information's confidentiality and integrity.

II. Access Control

- Access control is the method by which systems determine whether and how to admit a user into a trusted area of the organization—that is, information systems, restricted areas such as computer rooms, and the entire physical location.



- Access control is achieved by means of a combination of policies, programs, and technologies. Access controls can be mandatory, nondiscretionary, or discretionary.

A. Mandatory Access Control

- A security model that enforces strict access control policies on resources based on predefined rules and labels.
- In MAC, access decisions are determined by the system or security administrator, rather than individual users or processes.



- The primary objective of MAC is to protect sensitive information and maintain the confidentiality, integrity, and availability of resources.
- Key components and characteristics of Mandatory Access Control:



1. **Labels and Classification:**

MAC relies on labels or security classifications assigned to both subjects (users, processes) and objects (files, directories) within the system. These labels indicate the sensitivity level or access permissions associated with each subject or object. Labels can be represented as security clearances, levels of trust, or categories such as "top secret," "confidential," or "public."

2. **Security Policies:**

A security policy defines the rules and restrictions for accessing resources based on their labels. These policies are typically predefined by the system administrator or security personnel. The policies determine which subjects can access specific objects based on the security labels assigned to them. For example, a policy might dictate that only users with a "top secret" clearance can access files labeled as "top secret."

3. **Access Decisions:**

In a MAC model, access decisions are made based on the security labels of both the subjects and objects involved. The system enforces the policies by allowing or denying access to resources accordingly. Access decisions are typically made at the time of a subject's request to perform an operation on an object.

4. **Hierarchical Access Levels:**

MAC often employs a hierarchical model of access levels, where objects with higher sensitivity levels cannot be accessed by subjects with lower security clearances. This ensures that only authorized



individuals or processes with appropriate clearances can access resources with higher levels of sensitivity.

5. **Centralized Administration:**

MAC systems are typically centrally managed by

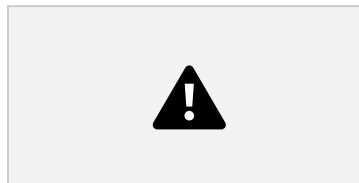


administrators who define and enforce access control policies. This centralized approach provides greater control over the system and ensures consistency in enforcing access restrictions.

6. **Strong Security:**

MAC provides a high level of security by strictly enforcing access controls based on predetermined policies. It reduces the risk of accidental or intentional data breaches by limiting access to resources based on the security classifications assigned to subjects and objects.

7. **Complex Configuration and Administration:**



Implementing and managing MAC can be more complex compared to other access control models, such as discretionary access control (DAC) or role-based access control (RBAC). MAC systems require careful planning, configuration, and ongoing maintenance to ensure proper labeling, policy enforcement, and administration.

- o Mandatory Access Control is commonly used in environments with high-security requirements, such as government agencies, military organizations, and critical infrastructure systems.
- o By enforcing strict access controls based on predefined rules and security labels, MAC helps protect sensitive information and mitigate the risks associated with unauthorized access or data leakage.

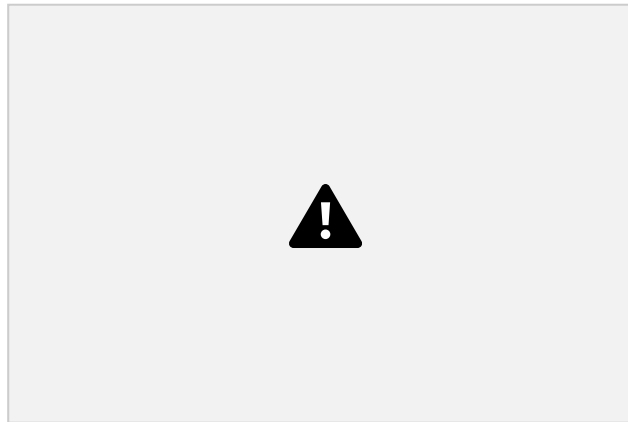
B. Nondiscretionary Control

- is a strictly-enforced version of MACs that are managed by a central authority in the organization and can be based on an individual's role.
- also known as Rule-Based Access Control (RBAC), are a type of access control model that determines access permissions based on predefined rules and regulations.

DEPARTMENT OF COMPUTER STUDIES – COMPUTER SCIENCE PROGRAM
CAVITE STATE UNIVERSITY – Imus Campus

69 Information Assurance and Security

- In contrast to discretionary access control (DAC) where access decisions are left to the discretion of the resource owner, nondiscretionary controls impose restrictions and permissions based on predefined policies. This approach ensures consistent and uniform access control across the system.



- Key features and characteristics of Nondiscretionary Control:

1. Rule-Based Policies:

Nondiscretionary control relies on predefined rules and policies that govern access to resources. These rules are typically based on organizational policies, regulations, compliance requirements, or industry standards. The rules outline who can access specific resources and under what conditions.

2. Role-Based Access Control (RBAC):

One common implementation of nondiscretionary control is RBAC. RBAC assigns roles to individual users or groups and grants access permissions based on the roles assigned. Each role is associated with a set of permissions or privileges, and users are assigned roles that align with their responsibilities and job functions.

RBAC simplifies access management by managing access at the role level rather than assigning permissions directly to individual users.

3. Access Decision Enforcement:

In nondiscretionary control, access decisions are enforced systematically based on the defined rules and policies. When a user requests access to a resource, the system evaluates the predefined

rules to determine if the user meets the requirements to access that resource.

If the user's attributes match the access criteria specified in the rules, access is granted; otherwise, it is denied.

DEPARTMENT OF COMPUTER STUDIES – COMPUTER SCIENCE PROGRAM
CAVITE STATE UNIVERSITY – Imus Campus

70 Information Assurance and Security

4. **Consistent and Uniform Access Control:**

Nondiscretionary control ensures consistent access control across the system. Access decisions are based on standardized rules and policies, eliminating the potential for variations in access permissions that can occur in discretionary access control models.

This helps maintain a uniform security posture throughout the organization and reduces the risk of inconsistent or arbitrary access decisions.

5. **Access Change Management:**

Nondiscretionary control requires careful management of access rules and policies. As organizational needs change, access rules may need to be updated or modified.

It is essential to have a well-defined process for managing access changes, including adding or removing roles, updating permissions, and ensuring that the changes align with the overall security objectives and compliance requirements.

6. **Audit and Accountability:**

Nondiscretionary control provides enhanced audit and accountability capabilities. Since access decisions are based on predefined rules, it becomes easier to track and monitor access activities.

The system can generate access logs, reports, and audits to demonstrate compliance, investigate security incidents, or identify potential policy violations.

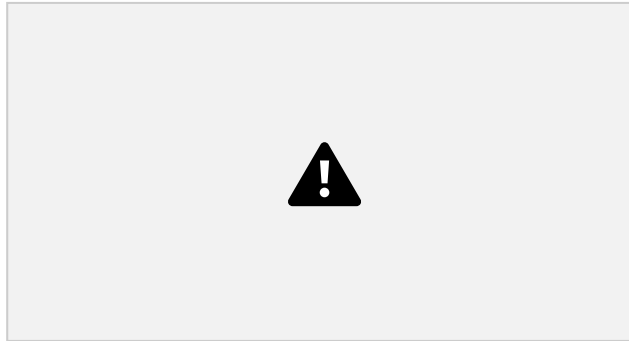
- o Nondiscretionary controls, particularly RBAC, are widely used in various industries and organizations to ensure consistent access management, simplify administration, and enforce access policies based on predefined rules and roles.

- o By implementing nondiscretionary control, organizations can achieve more structured and efficient access control processes while maintaining a higher level of security and compliance.

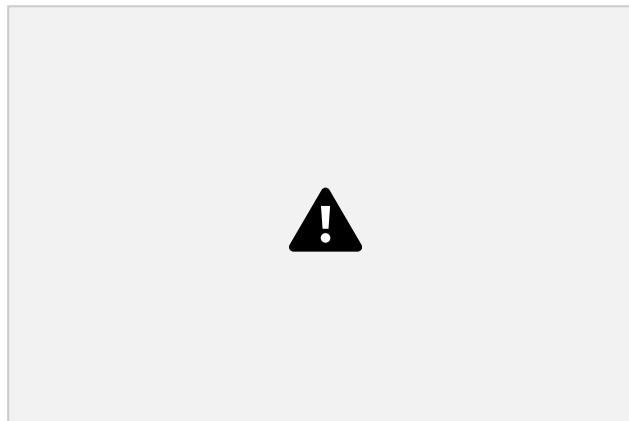
C. **Discretionary Access Control**

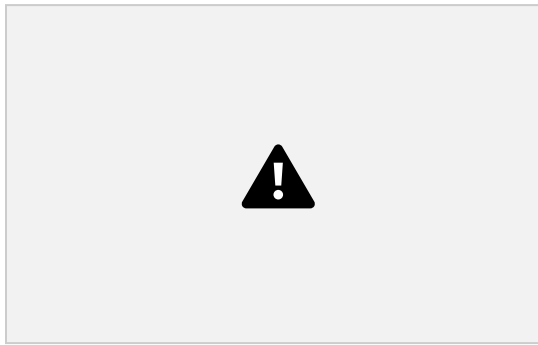
- Discretionary Access Control (DAC) is an access control model that allows resource owners to have control over granting or restricting access to their resources.

- In DAC, the resource owner has discretion or the freedom to decide who can access their resources and what level of access they can have. It is a commonly used access control model in various operating systems and file systems.



- In a discretionary access control model, the following key elements are involved:
 1. **Resource Owners:** Each resource within the system, such as files, folders, or objects, is associated with an owner who has control over that resource. The owner is typically the creator of the resource or a designated administrator.
 2. **Access Control Lists (ACLs):** An Access Control List is a data structure associated with each resource. It contains a list of access control entries (ACEs) that define the access permissions for different users or groups. Each ACE specifies the user or group and the specific access rights they have to the resource (e.g., read, write, execute).
 3. **User and Group Identities:** Users are individual accounts registered within the system, while groups are collections of users with similar access requirements. DAC allows resource owners to assign specific users or groups to ACEs in the ACL.





4. **Access Decisions:** When a user requests access to a resource, the operating system or security system checks the ACL associated with that resource. It evaluates the access control entries to determine if the user's identity matches any entries and whether they have the necessary permissions to perform the requested operation.
5. **Permissions and Privileges:** DAC provides a range of permissions that can be assigned to users or groups, such as read, write, execute, delete, or modify. These permissions determine what actions a user can perform on a resource.
 - o Discretionary Access Control is commonly implemented in various operating systems, such as Windows, Unix, and Linux.
 - o It provides a flexible access control model where resource owners have autonomy in managing access to their resources while requiring responsible decision-making and coordination to maintain a secure environment.

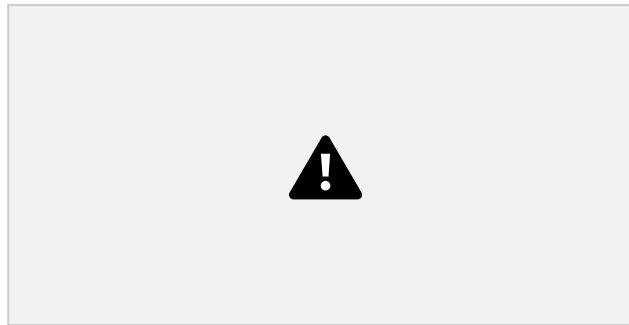
III. Firewall

- In commercial and residential construction, firewalls are concrete or masonry walls that run from the basement through the roof, to prevent a fire from spreading from one section of the building to another.
- A firewall in an information security program is similar to a building's firewall in that it prevents specific types of information from moving between the outside world, known as the untrusted network (for example, the Internet), and the inside world, known as the trusted network.
- The firewall may be a separate computer system, a software service running on an existing router or server, or a separate network containing a number of supporting devices.
- Firewalls can be categorized based on various criteria, including their architectural design, the layer of the network stack at which they operate, and their filtering capabilities.

Here are some common categories for classifying firewalls:

1. **Network Layer Firewalls:**

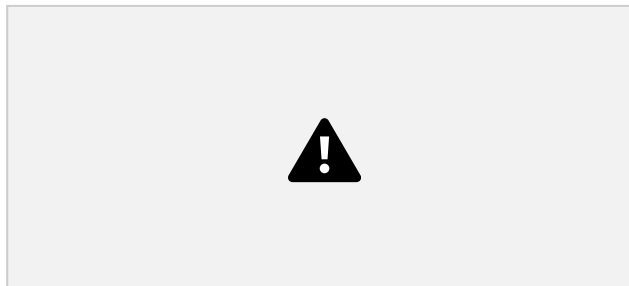
- Also known as packet-filtering firewalls, they operate at the network layer (Layer 3) of the OSI model.



- They examine individual packets of network traffic based on predefined rules or filters, such as source and destination IP addresses, ports, and protocols.
- Network layer firewalls are typically efficient and can provide basic protection against common network-based attacks.

2. **Application Layer Firewalls:**

- Also referred to as proxy firewalls, they operate at the application layer (Layer 7) of the OSI model.
- These firewalls act as intermediaries between the client and the server, inspecting the application-layer protocols such as HTTP, FTP, or SMTP.



- Application layer firewalls provide more granular control over network traffic by analyzing the contents of packets and enforcing protocol specific security policies.

3. Stateful Inspection Firewalls:

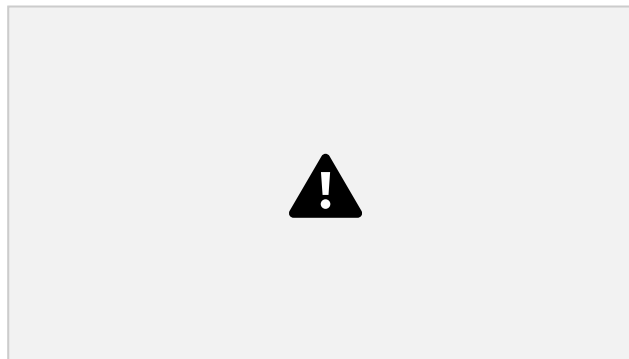
- ☞ Stateful inspection firewalls combine elements of network layer and application layer firewalls.
- ☞ They maintain a stateful connection table that keeps track of the state and context of network connections.



- ☞ Stateful inspection firewalls can monitor the entire lifecycle of network connections, allowing them to make more informed access control decisions based on the connection's history and context.

4. Next-Generation Firewalls (NGFWs):

- ☞ NGFWs integrate traditional firewall functionality with additional advanced security features, such as intrusion prevention systems (IPS), deep packet inspection (DPI), and application awareness.
- ☞ They provide enhanced visibility and control over applications, users, and content, enabling more sophisticated threat detection and prevention capabilities.



- ☞ NGFWs often incorporate threat intelligence feeds, VPN capabilities, and other security features to offer comprehensive network protection.

5. Hardware Firewalls:

- ☞ Hardware firewalls are standalone devices specifically designed for

performing firewall functions.

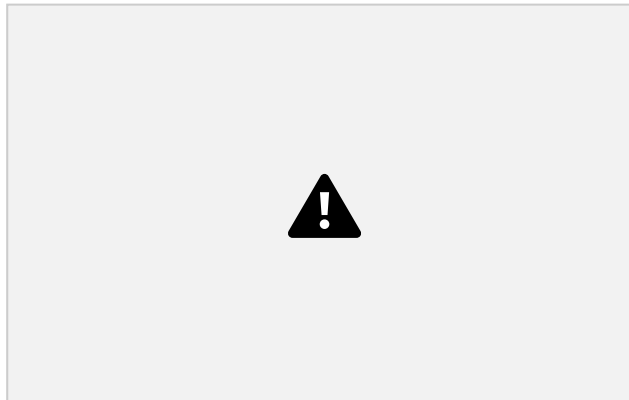
- 📖 They are typically implemented as dedicated appliances or routers with built-in firewall capabilities.



- 📖 Hardware firewalls often offer higher performance and scalability, making them suitable for protecting enterprise networks or network segments.

6. Software Firewalls:

- 📖 Software firewalls are software applications installed on individual computers or servers to provide local firewall protection.
- 📖 They can be host-based firewalls that run directly on the operating system or third-party firewall software installed separately.



- 📖 Software firewalls are commonly used on personal computers or small network environments.


DEPARTMENT OF COMPUTER STUDIES – COMPUTER SCIENCE PROGRAM
CAVITE STATE UNIVERSITY – Imus Campus

76 Information Assurance and Security

A. Selecting the Right Firewall

- When trying to determine which is the best firewall for an organization, you should consider the following questions:


1. Which type of firewall technology offers the right balance between protection and cost for the needs of the organization?


2. What features are included in the base price? What features are available at extra cost? Are all cost factors known?
 3. How easy is it to set up and configure the firewall? How accessible are the staff technicians who can competently configure the firewall?
 4. Can the candidate firewall adapt to the growing network in the target organization?
- The most important factor is, of course, the extent to which the firewall design provides the required protection. The second most important factor is cost.
 - Cost may keep a certain type out of reach. As decisions, certain necessary in order to solution under the stipulated by
- 

certain make, model, or with all security compromises may be provide a viable budgetary constraints management.

B. Best Practices for Firewalls

- This section outlines some of the best practices for firewall use. Note that these rules are not presented in any particular sequence.


 All traffic from the trusted network is allowed out. This allows members of the organization to access the services they need. Filtering and logging of outbound traffic can be implemented when required by specific organizational policies.


 The firewall device is never directly accessible from the public network for configuration or management purposes. Almost all administrative access to the firewall device is denied to internal users as well.

 Simple Mail Transport Protocol (SMTP) data is allowed to enter through the firewall, but is routed to a well-configured SMTP gateway to filter and route messaging traffic securely.

DEPARTMENT OF COMPUTER STUDIES – COMPUTER SCIENCE PROGRAM CAVITE STATE UNIVERSITY – Imus Campus

77 Information Assurance and Security

 All Internet Control Message Protocol (ICMP) data should be denied. Known as the ping service, ICMP is a common method for hacker reconnaissance and should be turned off to prevent snooping.

 Telnet (terminal emulation) access to all internal servers from the public networks

should be blocked. At the very least, Telnet access to the organization's Domain Name System (DNS) server should be blocked to prevent illegal zone transfers and to prevent attackers from taking down the organization's entire network.

☂ When Web services are offered outside the firewall, HTTP traffic should be blocked from internal networks through the use of some form of proxy access or DMZ architecture.

☂ All data that is not verifiably authentic should be denied. When attempting to convince packet-filtering firewalls to permit malicious traffic, attackers frequently put an internal address in the source field. To avoid this problem, set rules so that the external firewall

blocks all inbound traffic with an organizational source address.

- By following these best practices, organizations can strengthen their firewall security posture and better protect their networks and sensitive data from unauthorized access and cyber threats.

C. Firewall Rules



DEPARTMENT OF COMPUTER STUDIES – COMPUTER SCIENCE PROGRAM CAVITE STATE
UNIVERSITY – Imus Campus

78 Information Assurance and Security

- Firewall rules, also known as access control rules or firewall policies, are a set of predefined instructions or criteria that determine how a firewall should handle network traffic.
- These rules specify which network connections or packets should be allowed, denied, or restricted based on various criteria, such as source and destination IP addresses, ports, protocols, and other parameters.
- Firewall rules are configured within the firewall's rulebase, which is essentially a collection of individual rules organized in a specific order of precedence. When network traffic passes through the firewall, it is evaluated against these rules to determine how it should be handled.

- Each firewall rule typically consists of the following components:
 1. **Source Address:** The IP address, IP range, or network subnet from which the network traffic originates.
 2. **Destination Address:** The IP address, IP range, or network subnet to which the network traffic is intended.
 3. **Protocol:** The network protocol associated with the traffic, such as TCP (Transmission Control Protocol) or UDP (User Datagram Protocol).
 4. **Source Port:** The port number or port range from which the network traffic originates.
 5. **Destination Port:** The port number or port range to which the network traffic is intended.
 6. **Action:** The action to be taken when a network connection matches the rule's criteria, such as "Allow," "Deny," or "Drop."
 7. **Additional Criteria:** Additional parameters or conditions that further refine the rule, such as time-based rules, VLAN (Virtual Local Area Network) considerations, or specific flags associated with the traffic.
- Firewall rules are evaluated sequentially, typically from top to bottom, until a match is found. Once a match is found, the action specified in the rule is applied to the network traffic. It is crucial to define firewall rules in a specific order, considering the desired security policy and any dependencies between rules.
- Firewall rules can be configured to implement various security policies, such as allowing specific applications or services, restricting access to specific IP

DEPARTMENT OF COMPUTER STUDIES – COMPUTER SCIENCE PROGRAM
CAVITE STATE UNIVERSITY – Imus Campus

79 Information Assurance and Security

addresses or networks, or blocking certain types of traffic based on known vulnerabilities or attack patterns.

- Regular review and maintenance of firewall rules are essential to ensure that they align with changing business requirements and evolving security threats. Outdated or unnecessary rules should be removed, while new rules should be added as needed to accommodate new applications, services, or network changes.
- Below are sample firewall rules:



Rule Set 1: Responses to internal requests are allowed. In most firewall implementations, it is desirable to allow a response to an internal request for information. In dynamic or stateful firewalls, this is most easily accomplished by matching the incoming traffic to an outgoing request in a state table.



Rule Set 2: The firewall device is never accessible directly from the public network. If attackers can directly access the firewall, they may be able to modify or delete rules and allow unwanted traffic through. For the same reason, the firewall itself should never be allowed to access other network devices directly.



DEPARTMENT OF COMPUTER STUDIES – COMPUTER SCIENCE PROGRAM CAVITE STATE
UNIVERSITY – Imus Campus

80 Information Assurance and Security

Rule Set 3: All traffic from the trusted network is allowed out. As a general rule it is wise not to restrict outbound traffic, unless separate routers and firewalls are configured to handle it, to avoid overloading the firewall. If an organization wants control over outbound traffic, it should use a separate filtering device.



Rule Set 4: The rule set for the Simple Mail Transport Protocol (SMTP) data is shown in Table 6-9. As shown, the packets governed by this rule are allowed to pass through the firewall, but are all routed to a well-configured SMTP gateway.

It is important that e-mail traffic reach your e-mail server and only your e-mail server. Some

attackers try to disguise dangerous packets as e-mail traffic to fool a firewall. If such packets can reach only the e-mail server, and the e-mail server has been properly configured, the rest of the network ought to be safe.



Rule Set 5: All Internet Control Message Protocol (ICMP) data should be denied. Pings, formally known as ICMP Echo requests, are used by internal systems administrators to ensure that clients and servers can communicate.

Rule Set 6: Telnet (terminal emulation) access to all internal servers from the public networks should be blocked. Though not used much in Windows environments, Telnet is still useful to systems administrators on Unix/Linux systems.






DEPARTMENT OF COMPUTER STUDIES – COMPUTER SCIENCE PROGRAM CAVITE STATE
UNIVERSITY – Imus Campus

82 Information Assurance and Security

Rule Set 7: When Web services are offered outside the firewall, HTTP traffic (and HTTPS traffic) should be blocked from the internal networks via the use of some form of proxy access or DMZ architecture. With a Web server in the DMZ you simply allow HTTP to access the Web server, and use rule set 8, the cleanup rule to prevent any other access.

Rule Set 8: The cleanup rule. As a general practice in firewall rule construction, if a request for a service is not explicitly allowed by policy, that request should be denied by a rule. The rule shown in Table 6-15 implements this practice and blocks any requests that aren't explicitly allowed by other rules. ®



DEPARTMENT OF COMPUTER STUDIES – COMPUTER SCIENCE PROGRAM
CAVITE STATE UNIVERSITY – Imus Campus