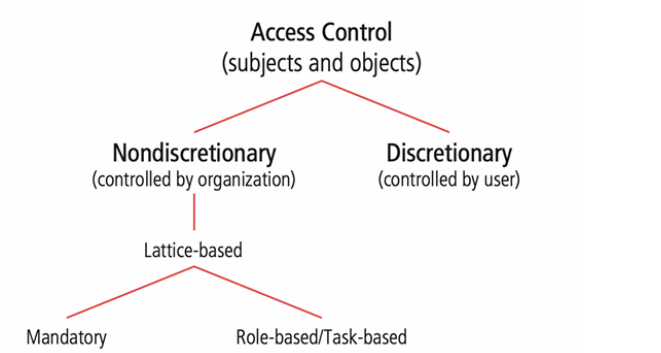
IAS 2 Reviewer

ACCESS CONTROL



Access Control Approaches

The selective method by which the systems specify who may use a particular resource and how they may use it.

Discretionary Access Controls - access controls that are implemented at the judgment or option of the data user.

Nondiscretionary Access Controls – access controls that are implement by a central authority.

Lattice-based Access Control – Variation on mandatory access controls that assigns users a matrix of authorizations for particular areas.

Role-based Access Control – A nondiscretionary control where privileges are tied to the role or job a user is performing.

Task-based Access Control – A nondiscretionary control where privileges are temporarily granted to a user based on their task.

Mandatory Access Control – A required, structured data classification scheme that assigns a sensitivity or classification rating to each collection or information as well as each user.

Attribute-based Access Control – an access control approach whereby the organization specifies the use of objects based on some attribute of the user of the system.

> **Attribute** – A characteristic of a subject that can be used to restrict to an object.

ACCESS CONTROL MECHANISMS

Four Fundamental Functions of Access Control Systems

1. **Identification -** User
2. **Authentication -** Prove
3. **Authorization -** Allowed
4. **Accountability –** Track and Monitor

Identification – Seeks label or username known by the system.

Authentication – Requires validation and verification of an entity's unsubstantiated

> **3 Authentication Factors**
>
> 1. **Something you know** (Password, Passphrases, Virtual Password)
> 2. **Something you have** (Smart Card, Dumb Cards, Virtual Password)
> 3. **Something you are** (Fingerprints, Palm prints, Hand geometry and topography, retina and iris scans, voice pattern, signatures, keyboard kinetic measurements)

Authorization – matching of an authenticated entity to a list of information assets and corresponding access levels.

Accountability – ensures all actions on a system – authorized or unauthorized – can be attributed to an authenticated identity; also known as auditability.

Biometrics Access Control – Use of physiological characteristics to provide authentication.

Access Control Architecture Models

1. **TSSEC's Trusted Computing Base:** A critical concept in the Trusted Computer System Evaluation Criteria (TCSEC) also known as the orange book. Developed by the US Department of Defense to evaluate and classify the security of computing systems.
2. **ITSEC –** stands for Information Technology Security Evaluation Criteria, a European set of standards developed in the early 1990s to evaluate the security of information systems and products.
3. **Common Criteria –** An International Standard (ISO/IEC 15408) for Computer Security Certification.
4. **Bell-LaPadula Confidentiality Model –** A formal security model focused on maintaining confidentiality in multi-level security systems. It was developed in the early 1970s by David Bell and Leonard LaPadula.
5. **Biba Integrity Model –** A formal model designed to maintain the integrity of data in a system, ensuring that information cannot be improperly altered. Developed by Kenneth J. Biba in 1977.
6. **Clark-Wilson Integrity Model –** A security model designed to ensure the integrity of data by enforcing well-formed transactions and preventing unauthorized or improper modifications. Developed by David D. Clark and David R. Wilson in 1987.
7. **Graham-Denning Access Control Model –** A formal security model that defines how subjects and objects can be securely managed within a computer system.

8 Primitive Protection Rights

1. **Create Object**
2. **Create Subject**
3. **Delete Object**
4. **Delete Subject**
5. **Read Access Right**
6. **Grant Access Right**
7. **Delete Access Right**
8. **Transfer Access Right**

8. Harrison-Ruzzo-Ullman Model – An access control model designed to formally specify how systems manage access rights and control who can access specific resources in a secure and structured manner. Developed by Michael A. Harrison, Walter L. Ruzzo, and Jeffrey D. Ullman in 1976.

HRU is built on an access control matrix and includes a set of generic rights and a specific set of commands.

- Create Object/Subject
- Enter specific command or generic right into a subject or object
- Delete specific command or generic right into a subject or object
- Destroy Object/Subject

9. **Zero Trust Architecture** – An approach to access control in IT Networks that does not rely on trusting devices or network connections.

FIREWALLS

A firewall is a system, or group of systems, that enforces an access control policy between networks.

Common Properties

1. Firewalls are resistant to network attacks.
2. Firewalls are the only transit point between integral corporate networks and external networks because all traffic flows through firewalls.
3. Firewalls enforce the access control policy

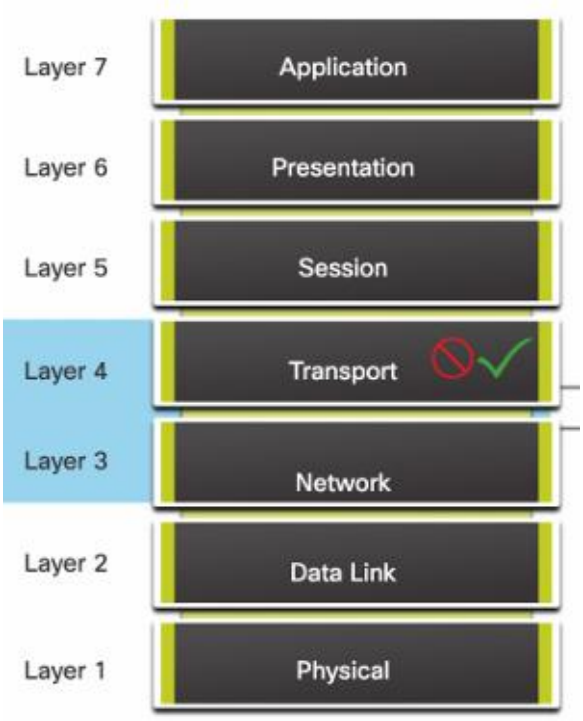
Benefits

1. Prevent exposure of sensitive hosts, resources, and applications to untrusted users.
2. Sanitize flow protocol, which prevents the exploitation of protocol flaws.
3. Blocks malicious data from servers and clients.
4. Reduce security management complexity by off-loading most of network access control to a few firewalls in the network.

Limitations

1. A misconfigured firewall can be a single point of failure.
2. Data from many applications cannot be passed over firewalls securely.
3. Users may try to install an unsafe application bypassing the firewall that can lead to exposure.
4. Network performance can slow down.
5. Unauthorized traffic can be tunneled or hidden as legitimate traffic through the firewall.

7 OSI Layers



TYPES OF FIREWALLS

1. **Packet Filtering Firewalls –** Usually a part of a router firewall, which permits or denies traffic based on Layer 3 and Layer 4 information.
2. **Stateful Firewalls –** Provide stateful packet filtering by using connection information maintained in a state table. It's classified at the network layer. It also analyzes traffic at OSI Layer 4 and 5.
3. **Application Gateway Firewall -** Filters information at Layers 3, 4, 5, and 7 of the OSI reference model.
4. **Next-Generation Firewalls –** Integrated intrusion prevention, application awareness and control to see block risky apps, upgrade paths to include future information feeds, techniques to address evolving security threats.
5. **Host-based Firewall –** A PC or server with firewall software running on it.

6. **Transparent Firewall –** Filters IP traffic between a pair of bridged interfaces.
7. **Hybrid Firewall –** A combination of the various firewall.

PACKET FILTERING BENEFITS AND LIMITATIONS

Advantages

1. Packet filters implement simple permit or deny rule sets.
2. Packet filters have a low impact o network performance.
3. Packet filters are easy to implement and are supported by most routers.
4. Packet filters provide an initial degree of security at the network layer.
5. Packet filters perform almost all the tasks of a high-end firewall at a much lower cost.

Disadvantages

1. Packet filters are susceptible to IP spoofing.
2. Packet filters do not reliably filter fragmented packets.
3. Packet filters use complex ACLs which can be difficult to implement and maintain.
4. Packet filters cannot dynamically filter certain services.

STATEFUL FIREWALL BENEFITS AND LIMITATIONS

Advantages

1. Stateful firewalls are often used as a primary means of defense by filtering unwanted, unnecessary, or undesirable traffic.
2. Stateful firewalls strengthen packet filtering by providing more stringent control over security.
3. Stateful firewalls improve performance over packet filters or proxy servers.
4. Stateful firewalls defend against spoofing and DoS attacks by determining whether packets belong to an existing connection or are from an unauthorized source.
5. Stateful firewalls provide more log information than a packet filtering firewall.

Disadvantages

1. Stateful firewalls cannot prevent application layer attacks because they do not examine the actual contents of the HTTP connection.
2. Not all protocols stateful.
3. It's difficult to track connections that use dynamic port negotiations.
4. Stateful firewalls do not support user authentication.

COMMON SECURITY ARCHITECTURES

1. Firewall design is primarily about device interfaces permitting or denying traffic based on the source, the destination, and the type of traffic.
2. Public Network -> Untrusted, Private Network -> Trusted
3. Typically, a firewall with two interfaces is configures as follows:
    a. Traffic origination from the private network is permitted and inspected as it travels toward the public network.
    b. Traffic originating from the public network and traveling to the private network is generally blocked.
4. A **Demilitarized Zone (DMZ)** is firewall design where there is typically one interface connected to the private

network, one outside interface connected to the public network, and one DMZ interface.

   a. Traffic origination from the private network is permitted and inspected as it travels toward the public network.
   b. Traffic originating from the DMZ network and traveling to the private network is usually blocked.
   c. Traffic originating from the DMZ network and traveling to the public network is selectively permitted based on service requirements.
   d. Traffic originating from the public network and traveling toward the DMZ is selectively permitted and inspected.
   e. Traffic originating from the public network and traveling to the private network is blocked.

5. Zone-based Policy Firewalls use the concept of zones to provide additional flexibility.
   a. A zone is a group of one or more interfaces that have similar functions or features.

LAYERED DEFENSE

1. **Network Core Security** – Protects against malicious software and traffic anomalies, enforces network policies, and ensure survivability.
2. **Perimeter Security** – Secures boundaries between zones.
3. **Communications Security** – Provides information assurance
4. **Endpoint Security** – Provides identity and device security policy compliance

A Network Administrator must consider many factors when building a complete in-depth defense:

1. Firewalls typically do not stop intrusions that come from hosts within a network or zone.
2. Firewalls do not protect against rogue access point installations.
3. Firewalls do not replace backup and disaster recovery mechanisms resulting from attack or hardware failure.
4. Firewalls are no substitute for informed administrators and users.

BEST PRACTICES FOR FIREWALLS

1. Position firewalls at security boundaries.
2. Deny all traffic by default.
3. Permit only services that are needed.
4. Ensure that physical access to the firewall is controlled.
5. Regularly monitor firewall logs.
6. Practice change management for firewall configuration changes.
7. Remember that firewalls primarily protect from technical attacks originating from the outside.
8. All traffic from the trusted network is allowed out.
9. The firewall device is never directly accessible from the public network or configuration or management purposes.
10. Simple Mail Transfer Protocol data is allowed to enter through the firewall but is routed to a well-configured SMTP gateway to filer and route messing traffic securely
11. All Internet Control Message Protocol data should be denied.

12. Telnet (Terminal Emulation) access should be blocked to all internal servers from the public networks.
13. All data that is not verifiably authentic should be denied.

RADIUS, DIAMETER AND TACACS

RADIUS and TACACS are systems that authenticate the credentials of users who are trying to access an organization's network via a dial-up connection

Remote Authentication Dial-In User Service: A computer connection system that centralizes the management of user authentication by placing the responsibility for authenticating each user on a central authentication server.

Diameter Protocol: Defines the minimum requirements for a system that provides authentication, authorization, and accounting services.

Terminal Access Controller Access Control System: Remote access authorization system that is based on a client/server configuration

3 Versions of TACACS

TACACS

Extended TACACS

TACACS+ - Uses dynamic passwords and incorporates two-factor authentication.

Kerberos: An authentication system that uses symmetric key encryption to validate an individual user's access to various network resources by keeping a database containing the private keys of clients and servers that are in the authentication domain it supervises.

1. **Authentication Server** – Authenticates clients and servers.
2. **Key Distribution Center** – Generates and issues session keys
3. **Kerberos Ticket Granting Service –** Provides tickets to clients who requested services. A ticket is an identification card for a particular client that verifies to the server that the client is requesting services.

KERBEROS PRINCIPLES:

1. Knows the secret keys of all clients and servers on the network.
2. Initially exchanges information with the client and server by using these secret keys.
3. Authenticates a client to a requested service on a server through TGS and by issuing temporary session keys for communications.

Secure European System for Applications in a Multivendor Environment (SESAME): An advanced network authentication protocol designed to enhance the security features of Kerberos while addressing some of its limitations, especially for large-scale, distributed environments.

Sesame separates its functions between two servers: the **Authentication Server** and the **Privilege Attribute Server**

AS – Verifies their identity

PAS – handles the authorization by issuing PACs.

VIRTUAL PRIVATE NETWORK

- A private, secure network operated over a public and insecure network; it uses encryption to protect the data between endpoints.

TYPES OF VPNs

1. **Trusted VPN** – Also known as legacy VPN, a VPN implementation that uses leased circuits from a service provider who gives contractual assurance that no one else is allowed to use these circuits that they are properly maintained and protected.
2. **Secure VPN –** A VPN implementation that uses security protocols to encrypt traffic transmitted across unsecured public networks.
3. **Hybrid VPN –** A combination of trusted and secure VPN implementations.

A VPN that proposes to offer a secure and reliable capability while relying on public networks must accomplish the following:

1. **Encapsulation**
2. **Encryption**
3. **Authentication**

IPSec, the dominant protocol used in VPNs, uses either transport or tunnel mode. It can be used as a stand-alone protocol or coupled with the **Layer Two Tunneling Protocol (L2TP).**

Transport Mode – The data within an IP packet is encrypted, but the header information is not.

Tunnel Mode – Establishes two perimeter tunnel servers to encrypt all traffic that will traverse an unsecured network.