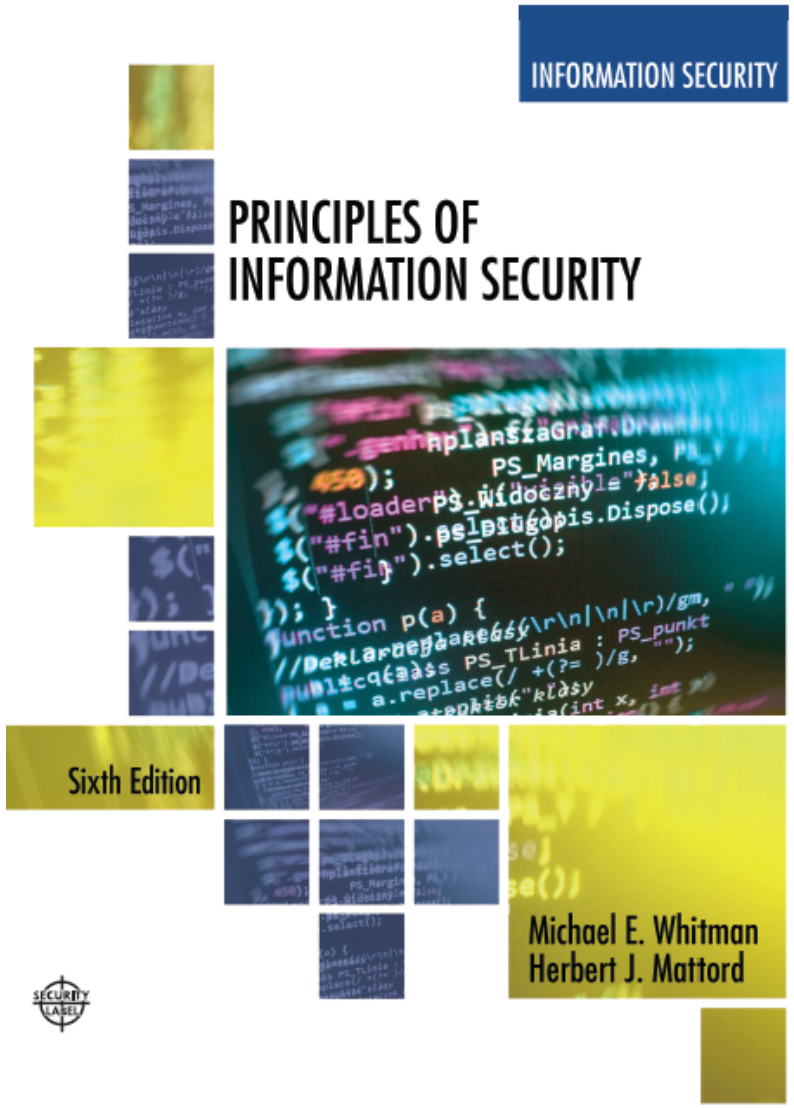


Source: Principles of Information Security

Chapter 6

Security Technology: Access Controls, Firewalls & VPNs

Dr. Ibrahim Waziri Jr.

Learning Objectives

- Upon completion of this material, you should be able to:
  - Understand and discuss the role of access control
  - Define authentication and explain the common authentication factors
  - Describe firewall technologies
  - Understand the various approaches to firewall implementation
  - Describe virtual private networks (VPNs) and discuss the technology that enables them

Introduction

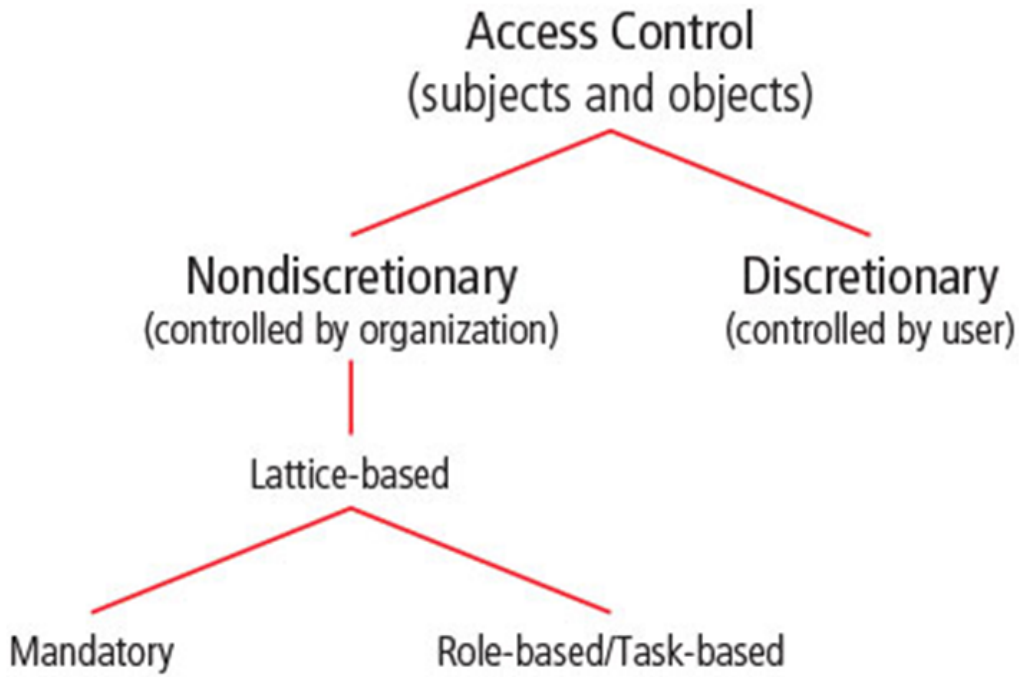
- Technical controls are essential in enforcing policy for many IT functions that are not under direct human control.

- Technical control solutions, when properly implemented, improve an organization's ability to balance the objectives of making information readily available and preserving the information's confidentiality and integrity.

Access Control (AC) – Models/Approaches

Access control: A selective method by which systems specify who may use a particular resource and how they may use it.

1. Mandatory (MAC)
2. Discretionary (DAC)
3. Role-Based (Non-Discretionary)
4. Attribute-based (ABAC)
5. History-Based (HBAC)
6. Identity-Based (IBAC)
7. Organization-Based (OrBAC)
8. Rule-Based (RAC) aka (RuBAC)



Access Control - Mechanisms

All access control approaches rely on the following four mechanisms, which represent the four fundamental functions of access control systems:

1. Identification: I am a user of the system.
2. Authentication: I can prove I'm a user of the system.
3. Authorization: Here's what I can do with the system.
4. Accountability: You can track and monitor my use of the system.

1 - Identification

The access control mechanism that requires the validation and verification of an unauthenticated entity's purported identity.

Example:

Entity = Ibrahim Waziri Jr (user)

Identifier = iwazirijr

2 - Authentication

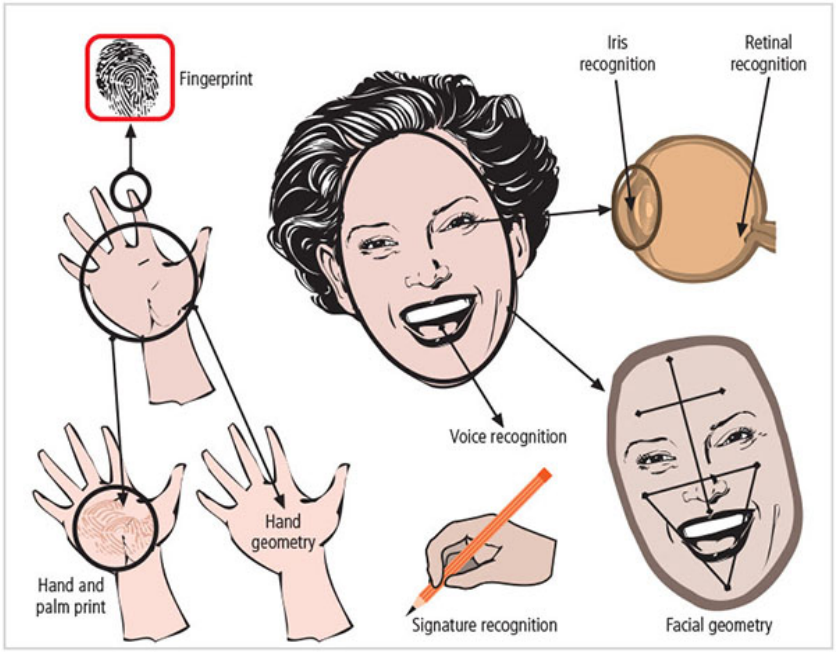
The access control mechanism that requires the validation and verification of an unauthenticated entity's purported identity.

3 Authentication factors are:

1. Something you **know** (such as a password)

2. Something you **are** (such as a fingerprint)

3. Something you **have** (such as a smart card)



Biometrics:

- Approach based on the use of measurable human characteristics/traits to authenticate identity.
- Only fingerprints, retina of eye, and iris of eye and DNA are considered truly unique.
- Evaluated on false reject rate, false accept rate, and crossover error rate.
- Highly reliable/effective biometric systems are often considered intrusive by users.

2 – Authentication – Ranking of Biometrics Effectiveness and Acceptance

Biometrics	University	Uniqueness	Permanence	Collectability	Performance	Acceptability	Circumvention
Face	H	L	M	H	L	H	L
Fadal Thermogram	H	H	L	H	M	H	H
Fingerprint	M	H	H	M	H	M	H
Hand Geometry	M	M	M	H	M	M	M
Hand Vein	M	M	M	M	M	M	H
Eye: Iris	H	H	H	M	H	H	H
Eye: Retina	H	H	M	L	H	L	H
DNA	H	H	H	L	H	L	L
Odor and Scent	H	H	H	L	L	M	L
Voice	M	L	L	M	L	H	L
Signature	L	L	L	H	L	H	L
Keystroke	L	L	L	M	L	M	M
Gait	M	L	L	H	L	H	M

- Note: H = High, M = Medium, and L = Low.
- Source: Principles of Information Security

3 - Authorization

The access control mechanism that represents the matching of an authenticated entity to a list of information assets and corresponding access levels.

Authorization can be handled in one of three ways:

- Authorization for each authenticated user
- Authorization for members of a group
- Authorization across multiple systems

4 - Accountability

The access control mechanism that ensures all actions on a system—authorized or unauthorized—can be attributed to an authenticated identity. Also known as auditability.

Accountability is most often accomplished by means of system logs and database journals, and the auditing of these records.

Access Control Architecture Models

Illustrate access control implementations and can help organizations quickly make improvements through adaptation.

- Trusted computing base (TCB) – Part of TCSEC
- Information Technology Security Evaluation Criteria (ITSEC)
- The common criteria
- Bell-LaPadula confidentiality model
- Biba Integrity model
- Clark-Wilson integrity model
- Graham-Denning access control model

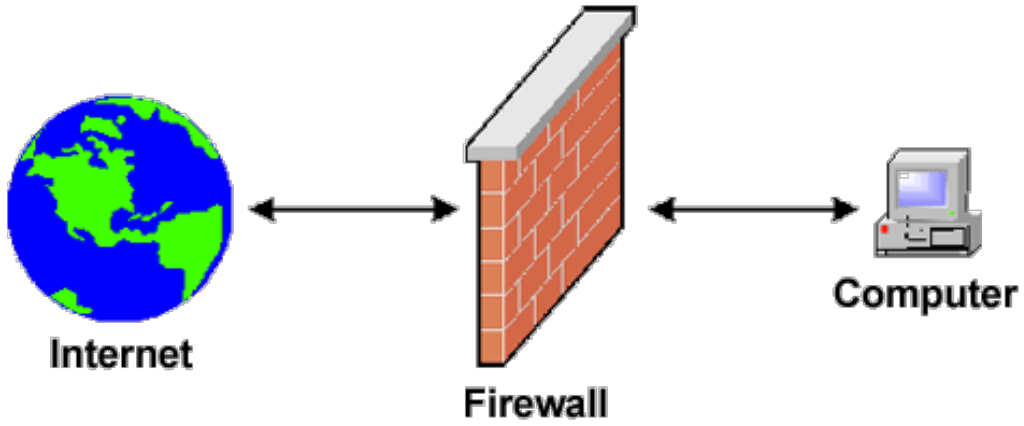
Firewalls

A combination of hardware and software that filters or prevents specific information from moving between the outside (untrusted) network and the inside (trusted) network.

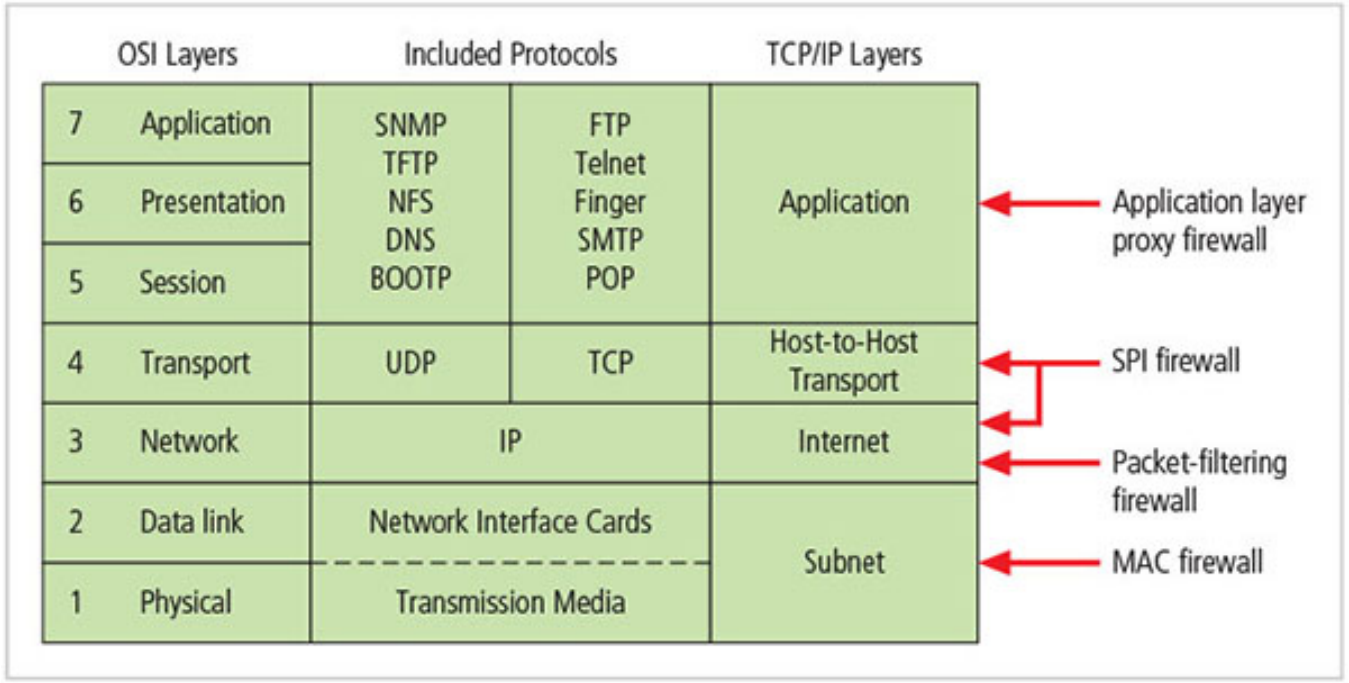
Firewall Processing Modes:

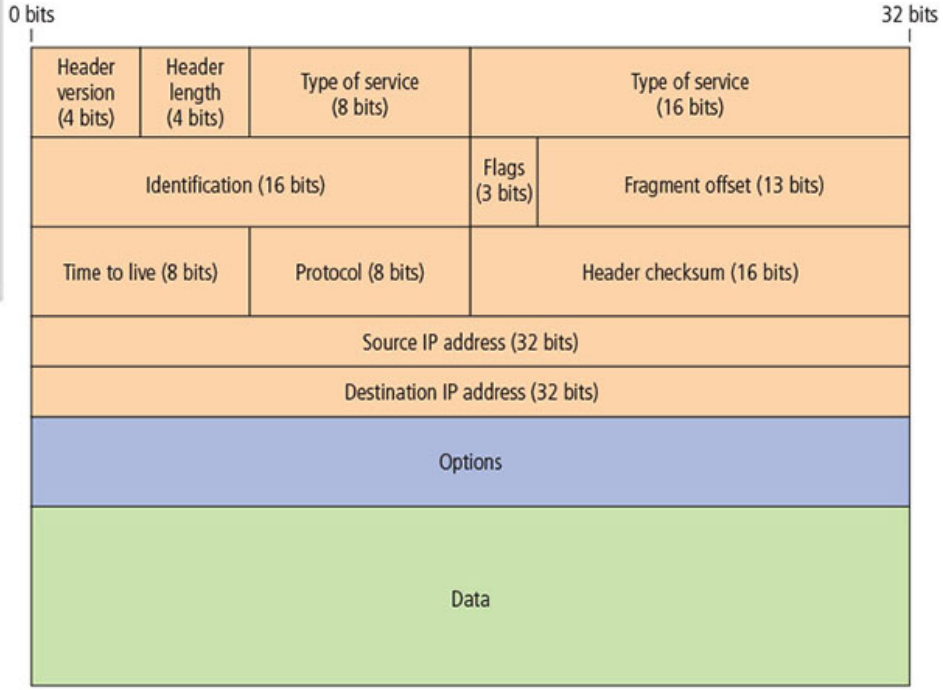
Processing modes by which firewalls can be categorized:

1. Packet filtering
2. Application layer proxy
3. MAC layer firewalls
4. Hybrids



Recap: Network Layers/Models



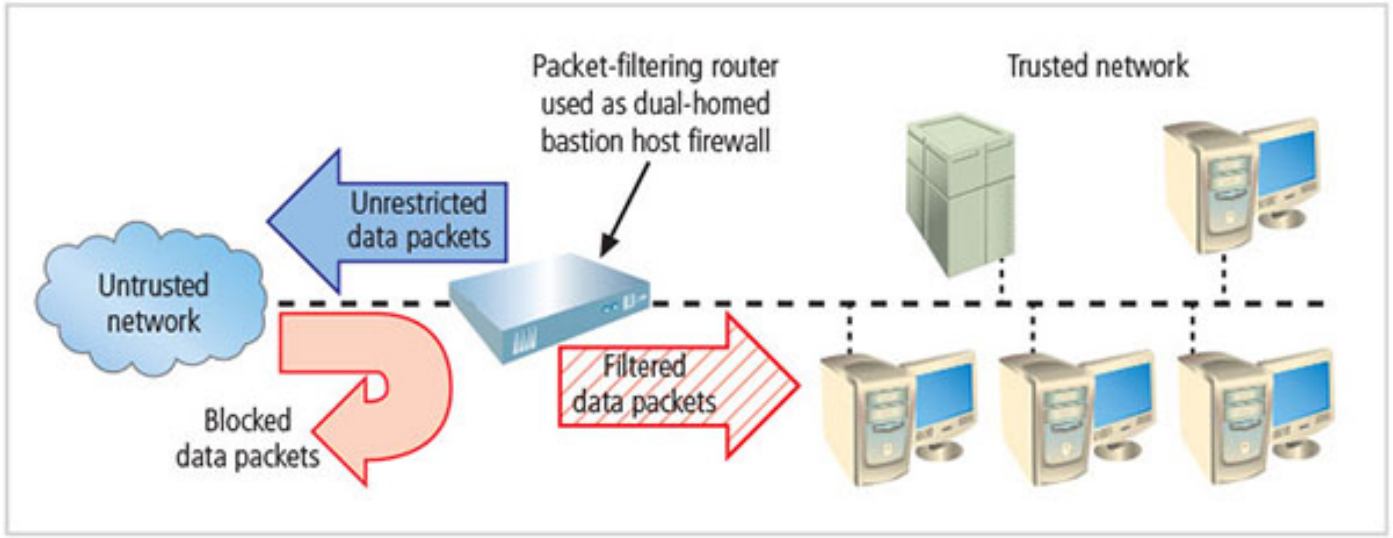


1 - Packet-Filtering Firewalls

Packet-filtering firewalls examine the header information of data packets. Most often based on the combination of: IP source and destination address -- Direction (inbound or outbound) -- TCP or UDP source and destination port requests

Packet-filter Firewall Types:

- Stateful Firewall
- Stateless Firewall

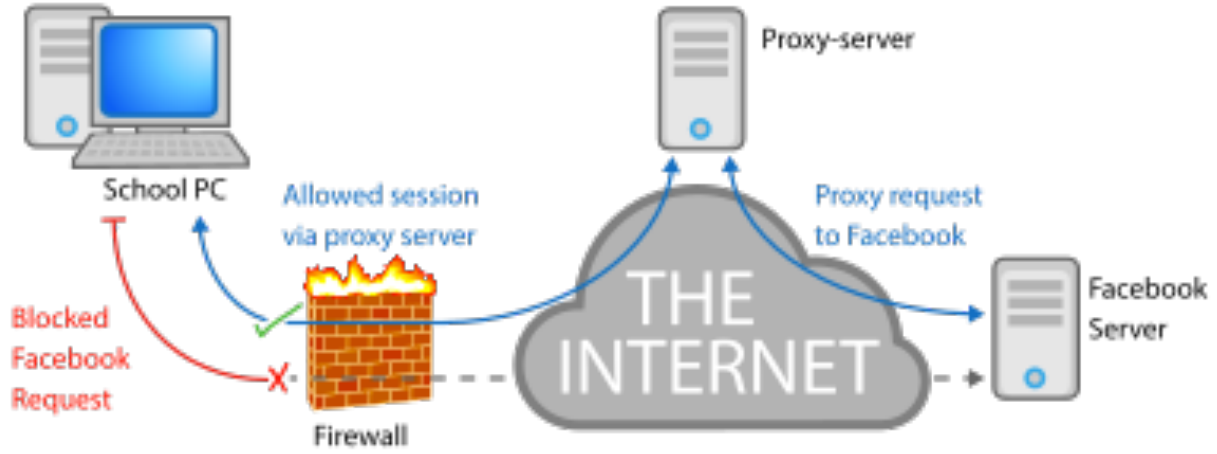


Simple firewall models enforce rules designed to prohibit packets with certain addresses or partial addresses from passing through the device.

2 - Application Layer Proxy Firewall

A device capable of functioning both as a firewall and an application layer proxy server.

Often placed in unsecured area of the network (e.g., DMZ)



Source Address	Destination Address	Service (e.g. HTTP, SMTP etc.)	Action (Allow or Deny)
172.16x.x	10.10.x.x	Any	Deny
192.168.x.x	10.10.10.25	HTTP	Allow
192.168.0.1	10.10.10.10	FTP	Allow

Additional control required to protect internal systems.

3 - MAC Layer Firewalls

- Designed to operate at media access control sublayer of network's data link layer.
- Make filtering decisions based on specific host computer's identity.
- MAC addresses of specific host computers are linked to access control list (ACL) entries that identify specific types of packets that can be sent to each host; all other traffic is blocked.

4 – Hybrid Firewalls

- Combine elements of other types of firewalls, that is, elements of packet filtering and proxy services, or of packet filtering and circuit gateways
- Include the Next Generation Firewall (NGFW) and Unified Threat Management (UTM) devices

Firewall Architectures

Firewall devices can be configured in several network connection architectures.

Best configuration depends on three factors:

- Objectives of the network
- Organization's ability to develop and implement architectures
- Budget available for function

Three common architectural implementations of firewalls:

- Single bastion hosts
- Screened host architecture
- Screened subnet architecture (with DMZ)

Firewall Architectures

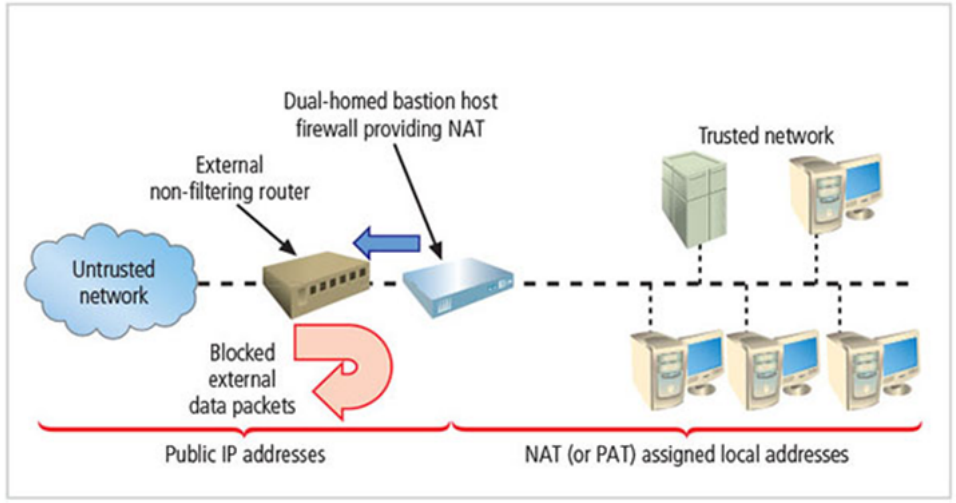


Figure 1: Dual-homed Bastion Host

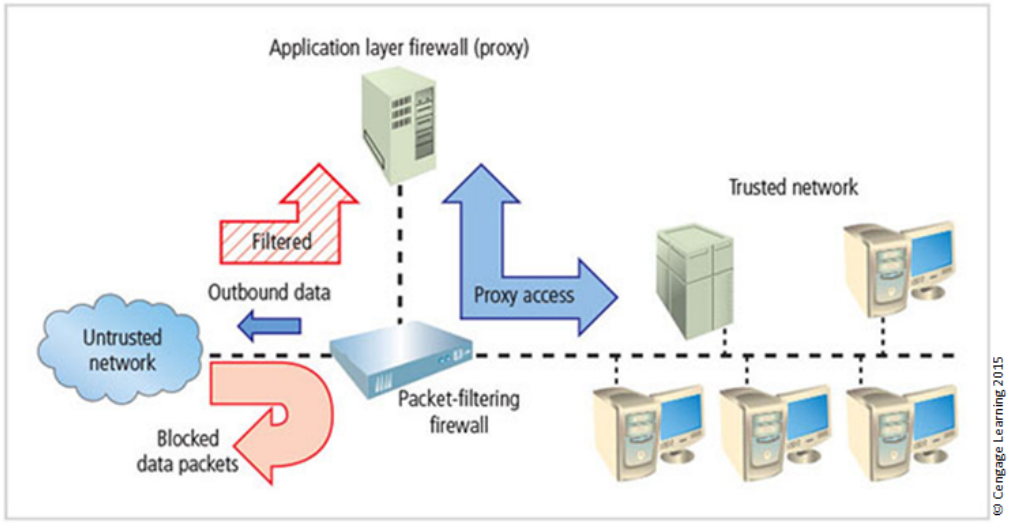


Figure 2: Screened Host

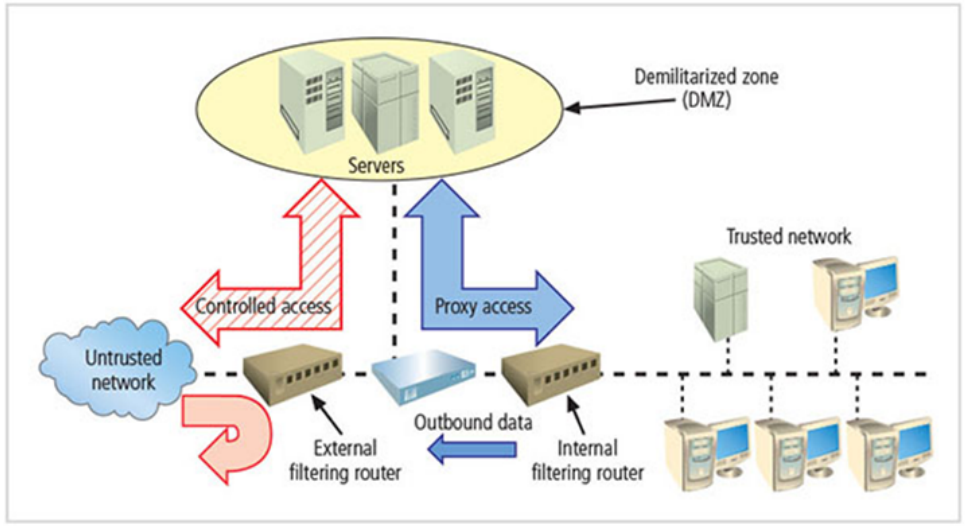


Figure 3: Screened Subnet

Selecting, Configuring and Managing Firewall

- When selecting the right firewall, consider the following factors:
  - Technology
  - Cost
  - Ease of set up and configuration
  - Adaptation

- Best practices
  - Deny-all – allow by exception
  - Block well-known (common) ports
  - Each devices should have its unique set of rules etc.

Protections: Content Filters & Remote Connections

Content Filters:

A software program or hardware/software appliance that allows administrators to restrict content that comes into or leaves a network

Remote Connections

- Connection to resources from a different (remote) location -- When individuals seek to connect to an organization’s network, a more flexible option must be provided.
- Options such as virtual private networks (VPNs) have become more popular due to the spread of Internet.

Remote Access

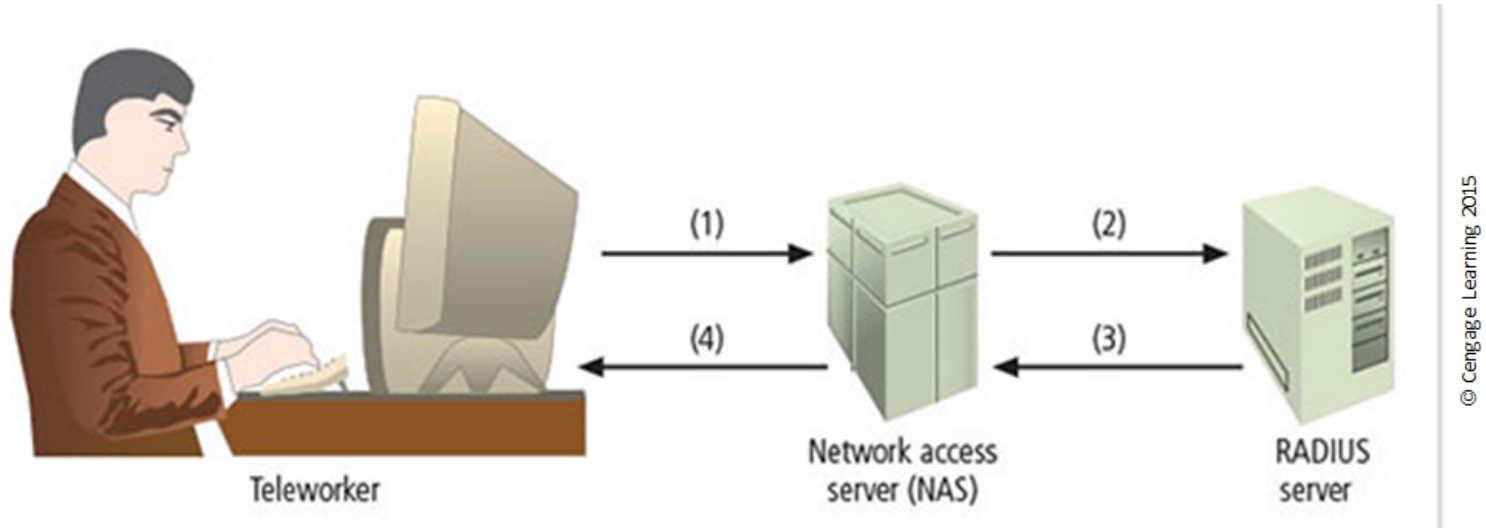
Dial-Up

- Unsecured, dial-up connection points represent a substantial exposure to attack.
- Attacker can use a device called a war dialer to locate the connection points.
- War dialer: automatic phone-dialing program that dials every number in a configured range and records number if a modem picks up.

Authentication Process:

- RADIUS
- TACACS
- Diameter
- CHAP
- Kerberos
- SESAME etc.

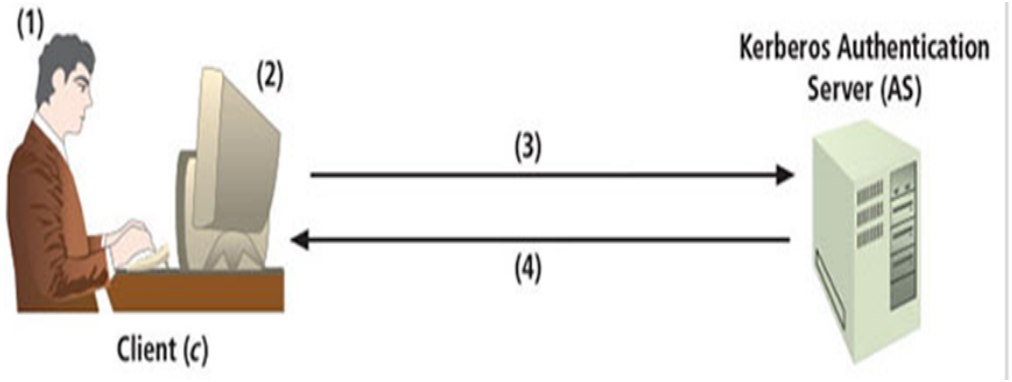
RADIUS Configuration



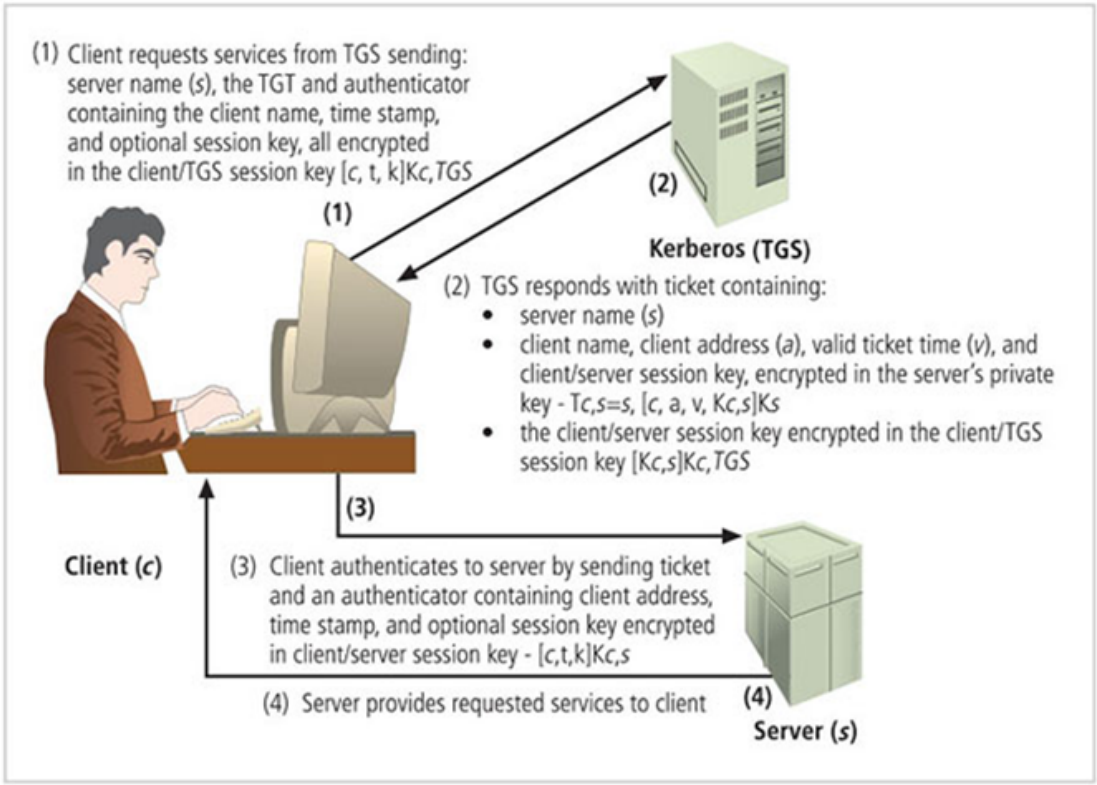
RADIUS configuration

1. Remote worker dials NAS and submits username and password
2. NAS passes username and password to RADIUS server
3. RADIUS server approves or rejects request and provides access authorization
4. NAS provides access to authorized remote worker

Kerberos Login



1. User logs into client machine (c)
2. Client machine encrypts password to create client key (Kc)
3. Client machine sends clear request to Kerberos Authentication Server (AS)
4. Kerberos AS returns ticket consisting of:
   - Client/TGS session key for future communications between client and TGS [Kc,TGS], encrypted with the client's key
   - Ticket granting ticket (TGT). The TGT contains the client name, client address, ticket valid times, and the client/TGS session key, all encrypted in the TGS' private key



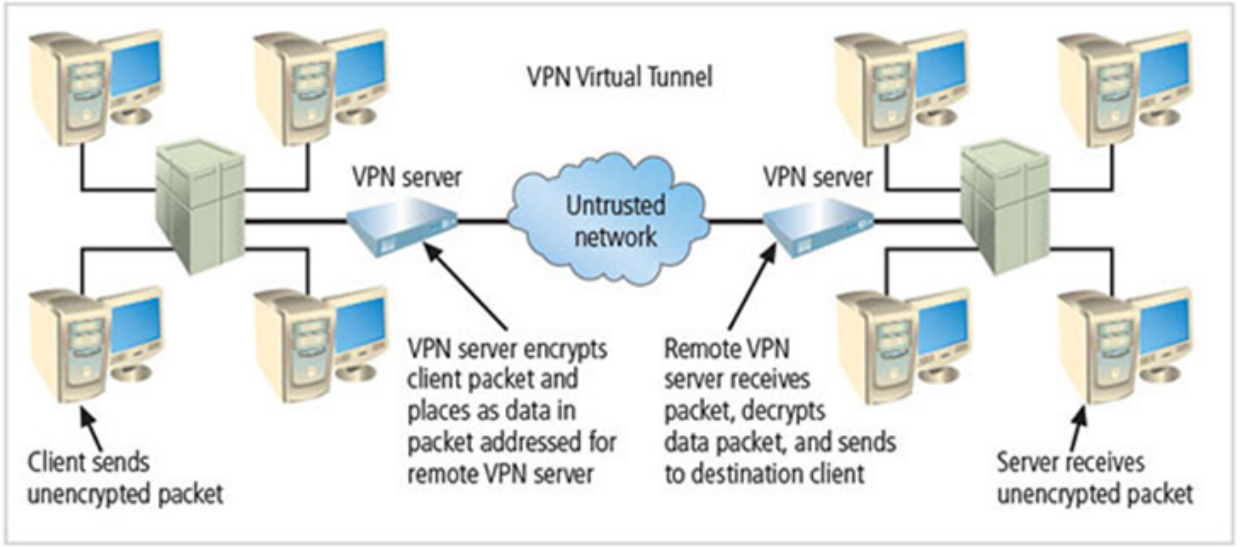
Virtual Private Networks (VPNs)

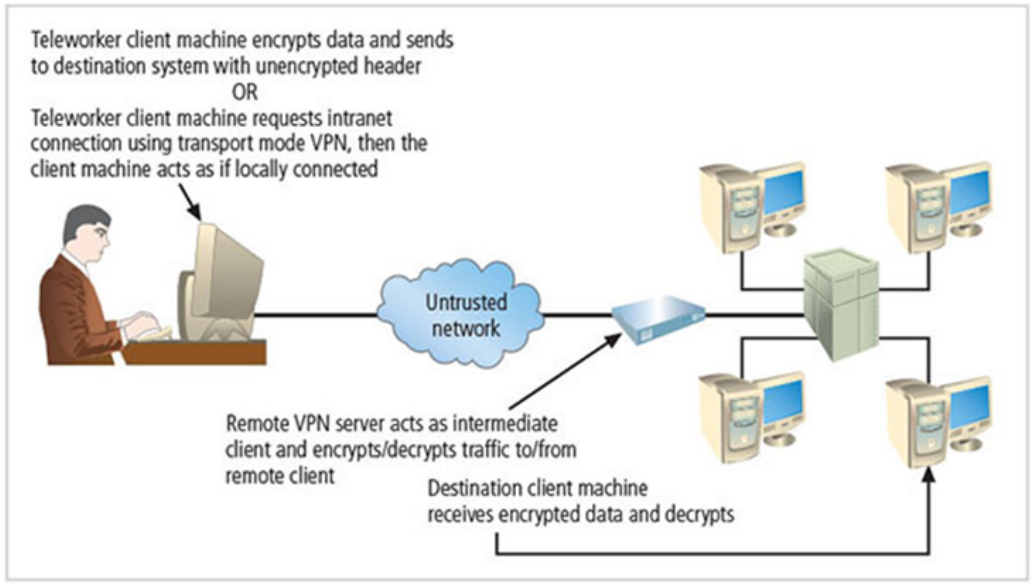
Private and secure network connection between systems; uses data communication capability of unsecured and public network.

Three VPN technologies are:

- Trusted VPN
- Secure VPN
- Hybrid VPN (combines trusted and secure)

- VPN modes are:
  - Transport mode
  - Tunnel mode





VPN must accomplish:

- Encapsulation of incoming and outgoing data
- Encryption of incoming and outgoing data
- Authentication of remote computer and perhaps remote user as well

Summary

- Access control is a process by which systems determine if and how to admit a user into a trusted area of the organization.
- All access control approaches rely on identification, authentication, authorization, and accountability.
- A firewall is any device that prevents a specific type of information from moving between the outside network, known as the untrusted network, and the inside network, known as the trusted network.
- Firewalls can be categorized into four groups: packet filtering, MAC layers, application gateways, and hybrid firewalls.
- Packet-filtering firewalls can be implemented as static filtering, dynamic filtering, and stateful inspection firewalls.
- The three common architectural implementations of firewalls are single bastion hosts, screened hosts, and screened subnets.
- Dial-up protection mechanisms help secure organizations that use modems for remote connectivity.
- VPNs enable remote offices and users to connect to private networks securely over public networks.