Firewalls

Miguel Frade & Francisco Santos

POLITÉCNICO DE LEIRIA | ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO

Introduction

The Need for Firewalls

- Internet connectivity is no longer optional for organizations
  - the information and services available are essential

INTRODUCTION

The Need for Firewalls

- Internet connectivity is no longer optional for organizations
    - the information and services available are essential
- but Internet access enables the outside world to reach and interact with local network assets
    - this creates a threat to the organization
    - it is difficult to equip each device with strong security features
    - may not be sufficient and in some cases is not cost-effective

The Need for Firewalls

- Internet connectivity is no longer optional for organizations
    - the information and services available are essential
- but Internet access enables the outside world to reach and interact with local network assets
    - this creates a threat to the organization
    - it is difficult to equip each device with strong security features
    - may not be sufficient and in some cases is not cost-effective
- the **firewall** is an alternative, or at least complement to host-based security services
    - it is a system designed to prevent non-authorized network access to, or from, a private network
    - commonly inserted between the premises network and the Internet
    - to provide a single point where security and auditing can be imposed

Firewall design goals

- all traffic must pass through the firewall by physically blocking all access to the local network except via the firewall
- only authorized traffic, as defined by the local security policy, will be allowed to pass
- the firewall itself should be immune to penetration
  - this implies the use of a hardened system with a secured operating system

Firewall access control techniques

- **IP address and protocol values** – based on the source or destination addresses and port numbers
- **direction of flow** – inbound or outbound
- **application protocol** – based on authorized application protocol data, *e. g.* SMTP, HTTP
- **user identity** – based on the users authentication, typically for inside the network
- **network activity** – based on considerations such as the time or request, *e. g.* only in business hours; rate of requests, *e. g.* to detect scanning attempts; or other activity patterns

Firewall limitations

- cannot protect against attacks that bypass the firewall
- cannot protect against internal threats, such as a disgruntled employee or an employee who unwittingly cooperates with an external attacker
- improperly secured wireless LAN may be accessed from outside the organization
- a device that may be used and infected outside the corporate network, and then attached and used internally
- cannot protect against software bugs

Types of Firewalls

TYPES OF FIREWALLS

Different types of firewalls

1. Packet Filtering
   - stateless
   - stateful
2. Circuit-Level Gateway
3. Application-Level Gateway

TYPES OF FIREWALLS

Packet filtering firewall

- applies a set of rules to each incoming and outgoing IP packet
- then forwards or discards the packet
- typically configured to filter packets going in both directions
- examples: Windows firewall, Linux IPtables, FreeBSD pfSense

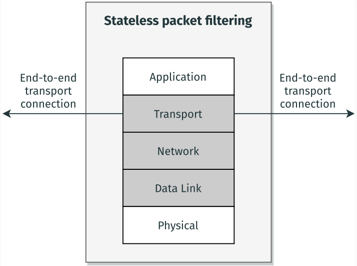
TYPES OF FIREWALLS

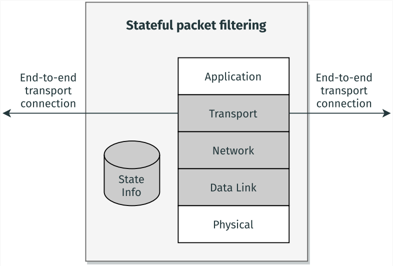
Packet filtering firewall

- applies a set of rules to each incoming and outgoing IP packet
- then forwards or discards the packet
- typically configured to filter packets going in both directions
- examples: Windows firewall, Linux IPtables, FreeBSD pfSense
- filtering rules based on
    - IP protocol
    - source and destination IP address
    - source and destination port numbers
    - interface
    - direction (incoming, or outgoing)

TYPES OF FIREWALLS

Packet filtering firewall types


Stateless packet filtering
End-to-end transport connection
Application
Transport
Network
Data Link
Physical
End-to-end transport connection


Stateful packet filtering
End-to-end transport connection
Application
Transport
State Info
Network
Data Link
Physical
End-to-end transport connection

- doesn't store connection state information
- must permit inbound network traffic for all dynamic ports for connections to occur → this creates a vulnerability

- stores connection state information
- only permits inbound network traffic for a dynamic port if an outgoing connection occurred first

TYPES OF FIREWALLS

Packet filtering firewall

Advantages

- transparent to users
- simplicity
- very fast

TYPES OF FIREWALLS

Packet filtering firewall

Advantages

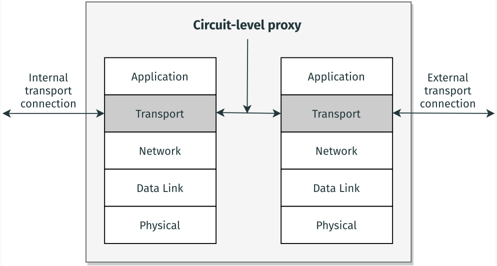
- transparent to users
- simplicity
- very fast

Disadvantages

- most do not support user authentication
- limited information available on the logs
- vulnerable to IP address spoofing
- vulnerable to source routing attacks
- might be vulnerable to tiny fragment attacks

TYPES OF FIREWALLS

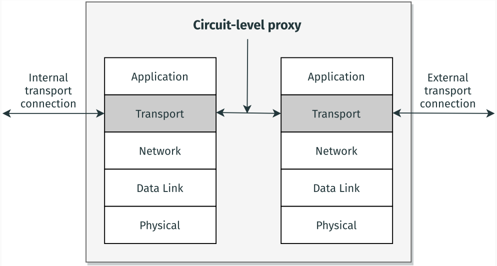
Circuit-level Gateway



Description

- does not permit an end-to-end TCP connections
- the gateway sets up two TCP connections
- after the connection is established does not inspect the contents
- SOCKS is an example of this type of firewalls

Circuit-level Gateway



Description

- does not permit an end-to-end TCP connections
- the gateway sets up two TCP connections
- after the connection is established does not inspect the contents
- SOCKS is an example of this type of firewalls

Advantages

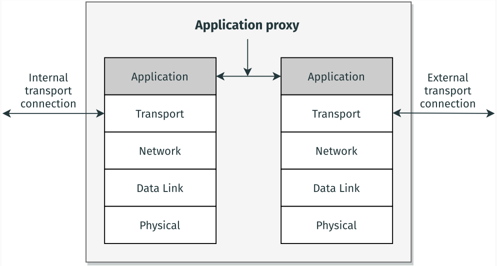
- faster than application proxies
- support for user authentication

Disadvantages

- slower than packet filtering firewalls
- internal users must be trusted 😱

TYPES OF FIREWALLS

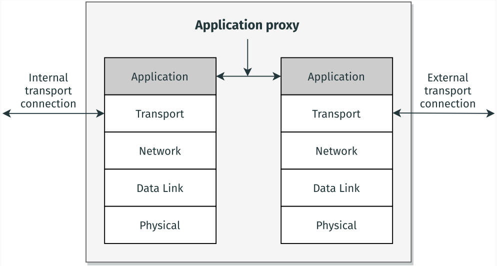
Application-level Gateway



Description

- does not permit an end-to-end TCP connections
- the gateway sets up two TCP connections
- SQUID is an example of this type of firewalls

Application-level Gateway



Description

- does not permit an end-to-end TCP connections
- the gateway sets up two TCP connections
- SQUID is an example of this type of firewalls

Advantages

- support for user authentication
- inspects the application layer contents
- lots of information available on the logs

Disadvantages

- more complex and the slowest type of firewall
- if a specific application protocol is not supported, then it cannot be forwarded

Firewall Location

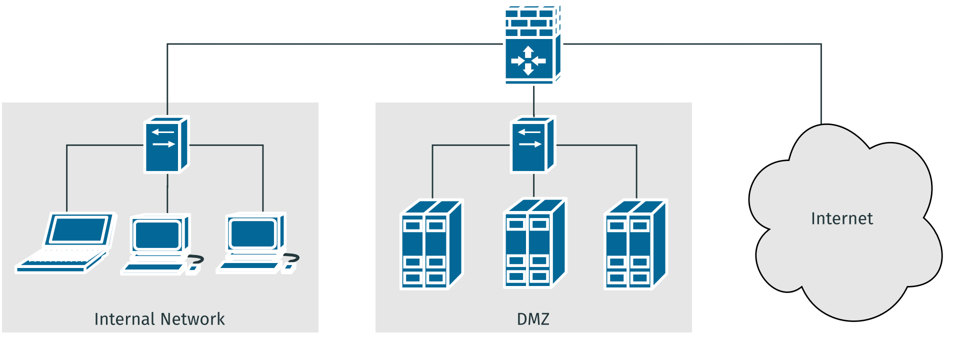
FIREWALL LOCATION

Firewall Locations and Topologies

- host-based
    - personal firewall software and firewall software on servers
    - can be used alone or as part of a distributed firewall configuration
- network-based
    - screening router – a single router between internal and external networks with a packet filtering firewall, typical for small office/home office (SOHO) applications
    - dedicated firewall appliance
        - inline with 2 network interfaces – a single firewall to separate the internal and external network
        - inline with 3 network interfaces – as a third interface for the DMZ, where externally visible servers are placed
        - double firewall – the DMZ is sandwiched between appliance firewalls
    - distributed firewall configuration – DMZ configuration where each server and user device has its own software firewall

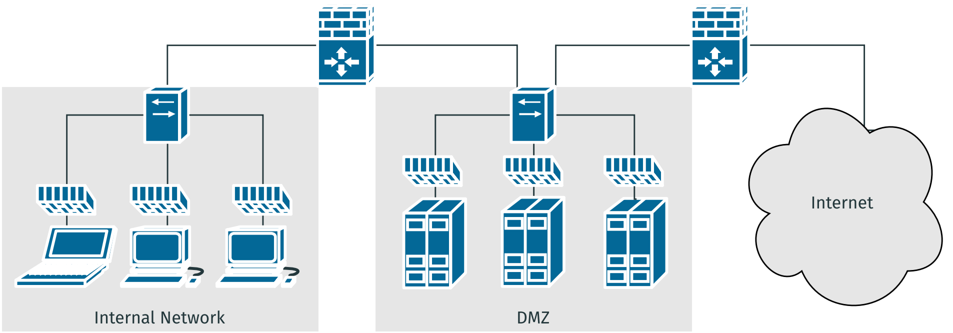
FIREWALL LOCATION

Firewall inline with 3 network interfaces



FIREWALL LOCATION

Double and distributed firewall configuration



Questions?