Firewall Security

Ethical Hacking

Alessandro Brighente
Eleonora Losiouk

Master Degree on Cybersecurity

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

Firewalls

- Device filtering the packets passing through a single and unique route to the network
- Firewalls delineate the security perimeter of the network
- Demilitarized Zone (DMZ) = network connecting the untrusted world (e.g., internet) to the internal private network
- By keeping servers on the DMZ users inside the network can easily access the outside world

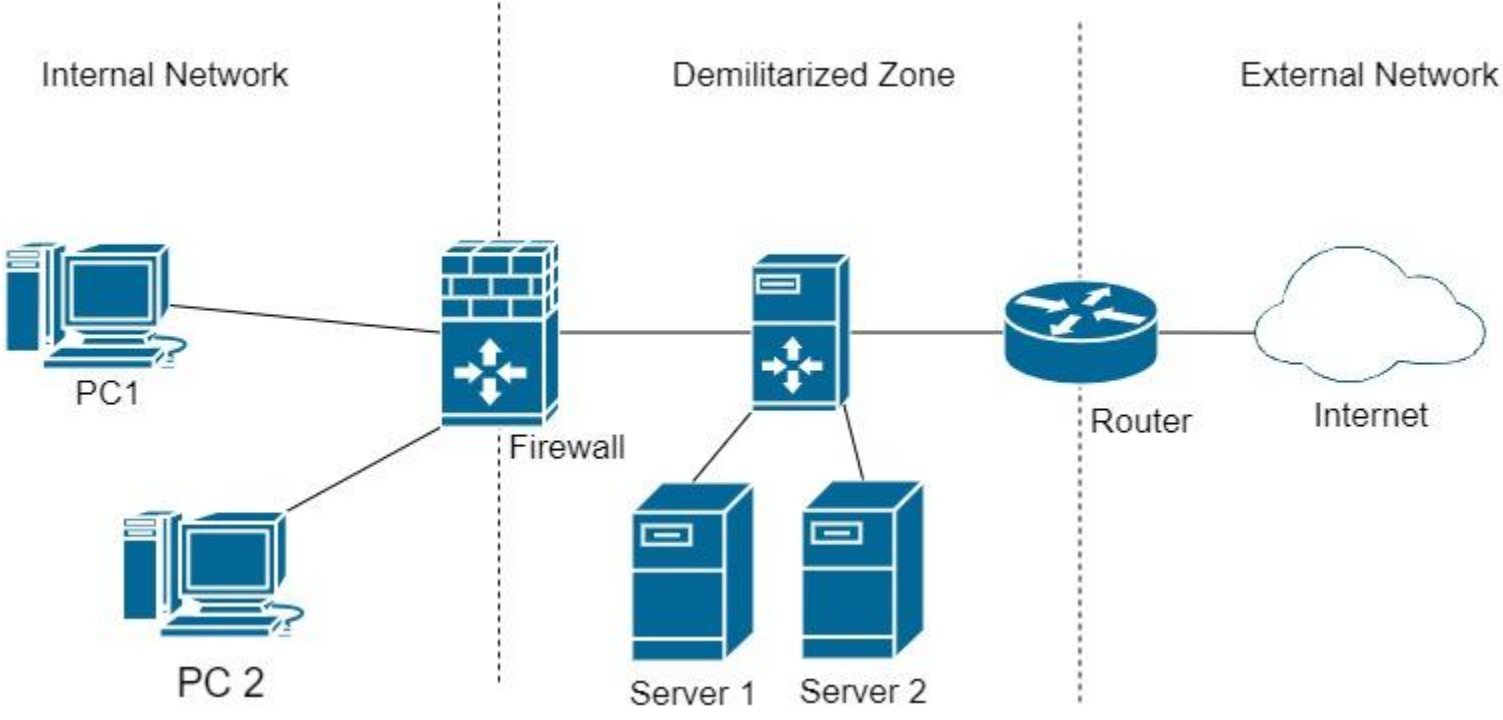
Design Goals

- All traffic flowing from inside to outside and vice-versa must pass through the firewall, achieved via physical connections
- Firewalls implement security policies to decide which type of traffic is authorized
- Should be immune to penetration, therefore implemented on trusted computing platforms with secure operating systems

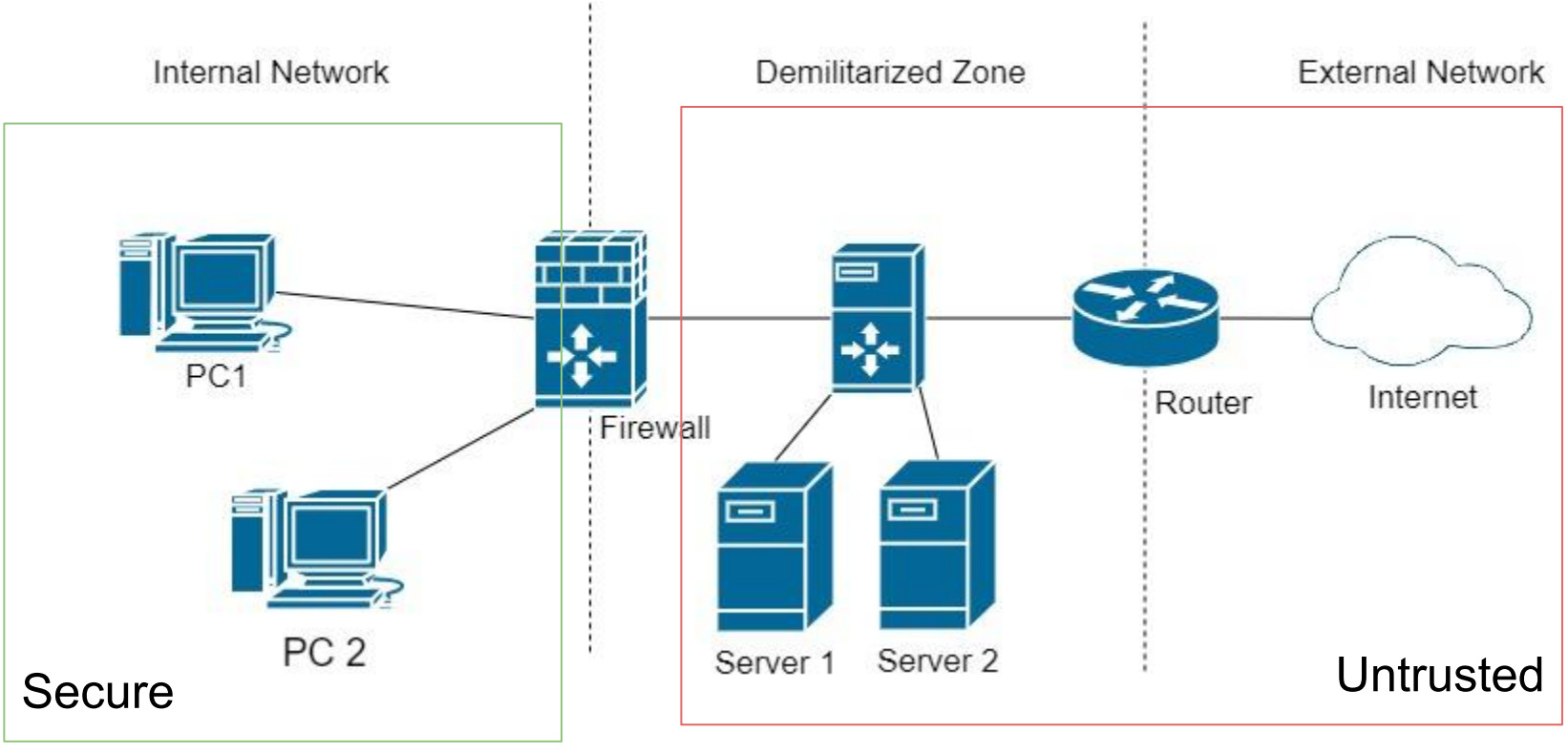
Capabilities of a Firewall

- Defines a single choke point that attempts to keep unauthorized users out of the protected network, prohibit potentially vulnerable services from entering or leaving the network, and provide protection from various kinds of IP spoofing and routing attacks
- Audits and alarms can be implemented on the firewall system
- Convenient platform for several Internet functions that are not security related

Firewalls


Internal Network
Demilitarized Zone
External Network
PC1
Firewall
Router
Internet
PC 2
Server 1
Server 2

Firewalls


Internal Network
Demilitarized Zone
External Network
PC1
PC 2
Firewall
Server 1
Server 2
Router
Internet
Secure
Untrusted

Firewall Packet Filtering

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- Inspect each and every incoming and outgoing packet
- The network administrator defines rules for valid packets
- Non conforming packets are discarded
- Rules usually include addresses or ports that are or not allowed
- Filtering is usually organized in tables

Firewall Policy

- A firewall defines a set of rules having control over
  - **Users**: based on the role of who is trying to access data
  - **Service**: access granted based on the type of service offered by the host being protected by the firewall
  - **Direction**: based on the direction of requests passing through the firewall
- A firewall has three responses:
  - Accepted
  - Denied
  - Rejected

Types of Firewall

- Firewalls can inspect the network packets from the lowest level (network packets) up to application protocols details
- The firewall “level” depends on the specific network needs
- Depending on the type, it might inspect a single packet, multiple packets, or the pattern generated by a sequence of packets

Characteristics for Filtering

- **IP address and protocol value:** based on the source or destination addresses and port numbers, direction of flow being inbound or outbound, and other network and transport layer characteristics
- **Application protocols:** filtering is used by an application-level gateway that relays and monitors the exchange of information for specific application protocols
- **User Identity:** typically in conjunction with IPSec
- **Network Activity:** based on considerations such as the time or request

Packet Filtering Firewall

- Applies a set of rules to each IP packet
- Decides whether to forward or discard specific packets
- Filtering is based on information typically contained in packets:
  - Source IP address
  - Destination IP address
  - Source and destination transport level address
  - IP protocol field
  - Interface

Packet Filtering Firewall

- Packet filtering is usually implemented via a set of rules
- If, for an incoming packet we have a match, than we apply the rule
- If nomatch, we select a default policy
  - Default discard = that which is not permitted is prohibited
  - Default forward = that which is not prohibited is permitted

Example of Packet Filtering: SMTP

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

Rule	Direction	Src address	Dest addresss	Protocol	Dest port	Action
1	In	External	Internal	TCP	25	Permit
2	Out	Internal	External	TCP	>1023	Permit
3	Out	Internal	External	TCP	25	Permit
4	In	External	Internal	TCP	>1023	Permit
5	Either	Any	Any	Any	Any	Deny

- Goal: allow in and out email traffic, and bock all the rest
- Allow both mail and SMTP packets
- Default discard

The Previous Example is Not Secure

- Rules exploiting port numbers above 1023 may cause malicious connections to be open (e.g., to web proxy server on 8080)
  - Countermeasure: add source port related to SMTP
- Still, an attacker may send packets with source port 25
  - Add an “ACK” Flag field to rule 4 (we only expect acknowledgements)

Attacks to Packet Filtering Firewalls

SPRITZ
SECURITY & PRIVACY
RESEARCH GROUP

UNIVERSITÀ
DEGLI STUDI
DI PADOVA

- **IP address spoofing:** the (external) attacker spoofs an IP address of an internal host, hoping to have easy access to resources
  - Solution: block incoming packets with internal addresses
- **Source Routing Attacks:** the attacker specifies the route a packet should undertake, hoping to bypass security measures
  - Countermeasure: discard packets with this option
- **Tiny Fragments Attack:** the attacker uses IP fragment option to create very small packets to separate the TCP header from the rest of the packet and prevent blocking based on header content
  - Enforce each packet to have a small portion of transport header