Network Security - Week 9

Manuel E. Correia

DCC/FCUP

2025

Firewall Location

- Firewalls can only filter traffic going through it
- **Q:** where to put, e.g. a mail server?

Firewall Location

- Firewalls can only filter traffic going through it
- **Q:** where to put, e.g. a mail server?

- Requires external access to receive mail from the Internet
  - Should be on the inside of the firewall

Firewall Location

- Firewalls can only filter traffic going through it
- **Q:** where to put, e.g. a mail server?

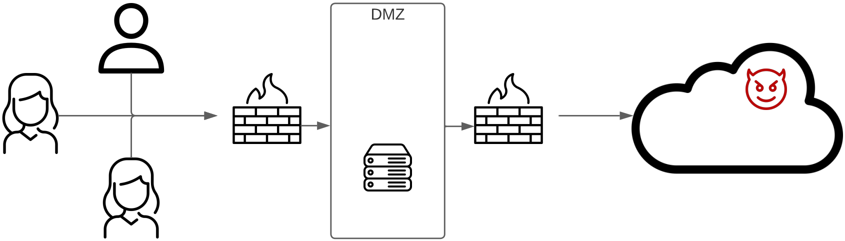
- Requires external access to receive mail from the Internet
  - Should be on the inside of the firewall

- Requires internal access to receive mail from the internal network
  - Should be on the outside of the firewall

Firewall Location

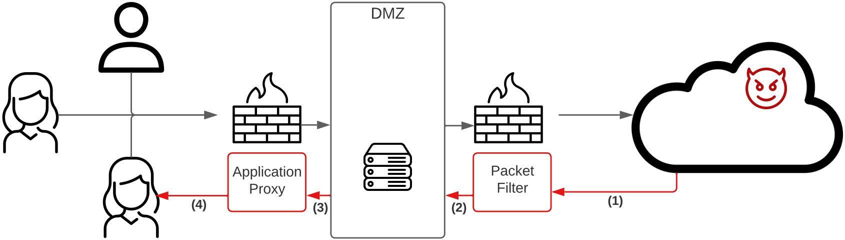
- Firewalls can only filter traffic going through it
- **Q:** where to put, e.g. a mail server?
- Requires external access to receive mail from the Internet
  - Should be on the inside of the firewall
- Requires internal access to receive mail from the internal network
  - Should be on the outside of the firewall
- **R:** “perimeter network” (a.k.a. DMZ)

Demilitarized Zone (DMZ)



- Demilitarized Zone is used for servers that require (selective) access from both inside and outside the firewall
- Very unique position security-wisely

Defence in Depth



- If one layer is breached, there are more layers
- Carlos may breach one layer
  - But breaking other layers may require a different skillset
  - And it takes additional time to go from (1) to (4)
- Useful to detect an attack in progress

Firewall Basing

There are several option for locating firewalls

- I - Bastion host
- II - Host-based individual firewall
- III - Personal firewall

I -Bastion Hosts

- Critical strongpoint in the network
- Host application/circuit-level gateways
- Common characteristics:
  - Runs secure O/S, only essential services
  - May require user auth to access proxy or host
  - Each proxy can restrict features, hosts accessed
  - Small, simple proxies, security-checked
  - Limited disk use, read-only code

II -Host-Based Firewalls

- Used to secure an *individual* host
- Available in/add-on for many O/Ss
- Filter packet flows
- Often used on server

II -Host-Based Firewalls

- Used to secure an *individual* host
- Available in/add-on for many O/Ss
- Filter packet flows
- Often used on server

Advantages

- Tailored filter rules for specific host needs
- Protection from both internal/external attacks
- Additional layer of protection to org firewall

III - Personal Firewalls

- Controls traffic flow to/from PC
- For both home and corporate usage
- Can be a software module on a PC
- Or in a DSL router/gateway

III - Personal Firewalls

- Controls traffic flow to/from PC
- For both home and corporate usage
- Can be a software module on a PC
- Or in a DSL router/gateway

Characteristics

- Typically much less complex than its counterparts
- Primary role to deny unauthorized access
- May also monitor outgoing traffic to detect/block malware activity

Tools: Firewalk

Scan open ports through firewall

- Attacker knows IP address of firewall
- An an IP address of one system inside firewall

Tools: Firewalk

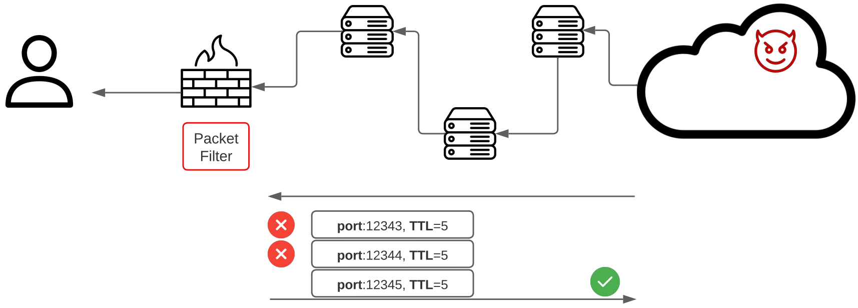
Scan open ports through firewall

- Attacker knows IP address of firewall
- An an IP address of one system inside firewall

Method (test port *N*):

- Set TTL to 1 more than the number of hops to firewall
- Set destination port to *N*
- If firewall allows data port *N*, get TIME EXCEEDED error message
- Otherwise, no reply
- More info here

Firewalk and Proxy Firewall



- Not feasible through an application proxy
- The application creates a new packet
- Which rewrites old TTL

Tables: Context of applying rules

- Filter: packet filtering/firewalling
- Nat: network address translation
- Mangle: modification of packets

IPTables: Firewalls in Linux

Terminology

Tables: Context of applying rules

- Filter: packet filtering/firewalling
- Nat: network address translation
- Mangle: modification of packets

Chains: Place/stage of packet processing

- Input: at system entrance (before being sent to apps)
- Output: at system exit (before being sent for routing)
- Forward: for systems operating as routers

IPTables: Firewalls in Linux

Terminology

Tables: Context of applying rules

- Filter: packet filtering/firewalling
- Nat: network address translation
- Mangle: modification of packets

Chains: Place/stage of packet processing

- Input: at system entrance (before being sent to apps)
- Output: at system exit (before being sent for routing)
- Forward: for systems operating as routers

Targets: Destination to give to packet

- Drop, Accept, Reject, Log, Return, Queue

IPTables: Firewalls in Linux

Methodology

- Add rules to TABLES specifying the CHAINS there in.

IPTables: Firewalls in Linux

Methodology

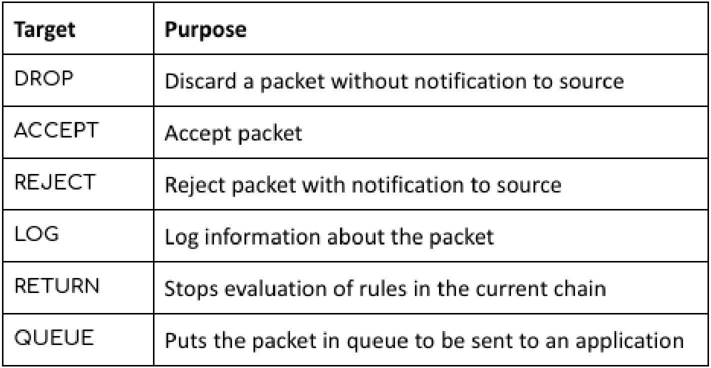
- Add rules to TABLES specifying the CHAINS there in.
- When a packet matches a rule, its TARGET is selected
  - TARGETS vary according to TABLES
    - Filter Table: DROP, ACCEPT
    - NAT Table: DNAT, SNAT, MASQUERADE, REDIRECT

IPTables: Firewalls in Linux

Methodology

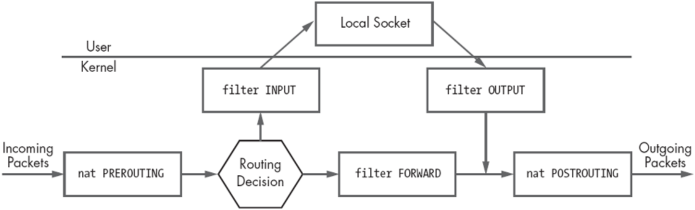
- Add rules to TABLES specifying the CHAINS there in.
- When a packet matches a rule, its TARGET is selected
  - TARGETS vary according to TABLES
    - Filter Table: DROP, ACCEPT
    - NAT Table: DNAT, SNAT, MASQUERADE, REDIRECT
- New CHAINS may be created by the user
- These can then be set as TARGETS of rules

IPTables: Filter Targets



Target	Purpose
DROP	Discard a packet without notification to source
ACCEPT	Accept packet
REJECT	Reject packet with notification to source
LOG	Log information about the packet
RETURN	Stops evaluation of rules in the current chain
QUEUE	Puts the packet in queue to be sent to an application

IPTables: Incoming/Outgoing Packets



IPTables: Examples

Accept ICMP echo-request pks with source address 10.1.0.1

```
iptables -A INPUT -S 10.1.0.1 -p icmp --icmp-type
echo-request -j ACCEPT
```

Accept at server exit TCP pks in interface eth1 with dest. port 22 and dest. address in network 10.5.0.0/24

```
iptables -A OUTPUT -d 10.5.0.0/24 -p tcp --dport 22
-o eth1 -j ACCEPT
```

Set DROP policy to all packets that are not authorized by previous policies

```
iptables -P INPUT DROP
```

More examples here

Wrap up

Firewalls as the first line of defence

- Establish the criteria under which packets come in/go out
- Can be deployed in a variety of ways
  - Packet filter - network
  - Stateful packet filter - transport layer
  - Application proxy - application layer
- No clear-cut “best" practice.
- Depends on security requirements

Wrap up

Firewalls as the first line of defence

- Establish the criteria under which packets come in/go out
- Can be deployed in a variety of ways
  - Packet filter - network
  - Stateful packet filter - transport layer
  - Application proxy - application layer
- No clear-cut “best" practice.
- Depends on security requirements

Firewall deployment/configuration

- Firewall efforts can be done in multiple ways
  - Bastion hosts; Host-based firewalls; Personal firewalls
- Firewalking vulnerability
- IPTables to establish access rules

Proactive vs Reactive

Previously...

- We want to keep bad guys out
    - Authentication prevents intrusions
    - Firewalls are a form of intrusion prevention
    - Virus defenses aimed at avoiding intrusions
    - Locking the door on your car

Proactive vs Reactive

Previously...

- We want to keep bad guys out
  - Authentication prevents intrusions
  - Firewalls are a form of intrusion prevention
  - Virus defenses aimed at avoiding intrusions
  - Locking the door on your car

Intrusion Detection Systems

- What to do if they get in?
- Detect attacks in progress
- Look for *unusual* or *suspicious* activity
- IDS evolved from log file analysis

Classes of Intruders - Cyber Criminals

- Individuals or members of an organized crime group, with the goal of financial reward
- Activities include, but are not limited to
  - Identity theft
  - Theft of financial credentials
  - Corporate espionage
  - Data theft
  - Data ransoming

- Information exchanged in underground forums to trade tips/data and coordinate attacks
- Anonymous networks (Tor et. al.) are very good for this

Classes of Intruders - State-Sponsored Organizations

- Groups of hackers sponsored by governments to conduct espionage or sabotage activities

- Also known as Advanced Persistent Threats
- Covert nature
- Persistence over extended periods

- Widespread nature and scope by a wide range of countries (China, Russia, USA, UK, and intelligence allies)

Classes of Intruders - Activists

- Individuals motivated by social or political causes
  - Working as insiders
  - Members of a larger group
- Also known as hacktivists
- Skill level often not high
- Goal is to promote and publicize their cause, typically through:
  - Website defacement
  - Denial-of-service attacks
  - Theft and distribution of data, resulting in negative publicity or compromise of their targets

Classes of Intruders - Others

- Hackers with motivations other than previously listed

- Include classic hackers/crackers
- Motivated by technical challenge or peer-group esteem and reputation
- Many responsible for discover new vulnerabilities

- Given the wide availability of attack toolkits, there is a pool of “hobby hackers” exploring system and network security challenges

Insider attacks

- Among most difficult to detect and prevent
- Employees have access & systems knowledge

Motivation is key

- Revenge or entitlement
- Employment terminated
- Stealing customer data for competitor

IDS may help, but also...

- Least privilege configuration
- Monitor logs
- Strong authentication
- Termination to block access

Network Security - Week 9

Manuel E. Correia

DCC/FCUP

2025