

Firewalls

Objectives

Indispensable element in connecting a network domain

- Access control
- Flow control
- Content control

Centralized implementation of security policies

- Minimizes the impact of local vulnerabilities
 - Known or unknown
- Makes it easier to take more drastic positions
- Centralizes problem detection
 - and its treatment

Definition (Cheswick & Bellovin)

Link between networks

- of a protected perimeter (set of networks and machines)
- to an insecure network (Internet)

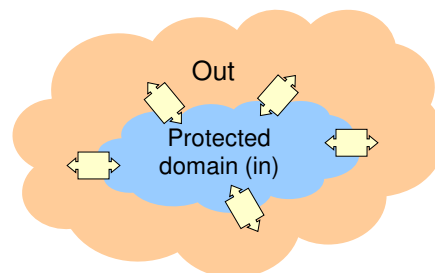
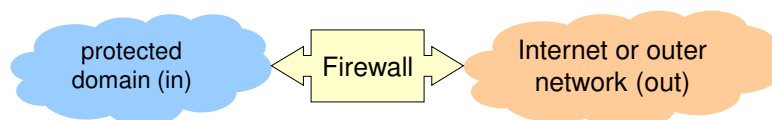
Component set

- Hardware and software

Properties

- In the path of all in \leftrightarrow out traffic
- Controls the traffic passing through it
- Immune to penetration (by definition)

Definition (Cheswick & Bellovin)



Functionalities

Supervision of all in ↔ out communication

- Control
 - The use of internal resources by external hosts/requests
 - The use of external resources by internal host/requests
- Defense from attacks
 - from outside the protected domain towards its resources
 - from the protected domain against external resources

Activation of gateway mechanisms

- To hide the structure from the protected perimeter
 - NAT (Network Address Translation)
 - Masquerading and Port Forwarding
- To extend the security perimeter
 - Secure tunneling (VPN)

Importance of Firewalls

Extreme!

Attacks on public systems are constant

- By specialized attackers
- By standalone applications

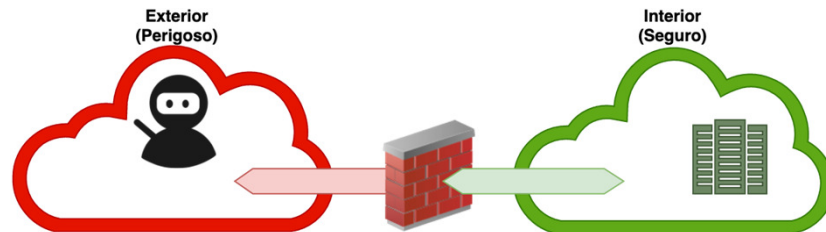
Systems do not always have adequate security mechanisms

- Blocking after too many incorrect attempts
- Validation of communications
- Access control

Necessary to apply mechanisms defined by the administrator, in accordance with domain policies

- An application programmer is not aware of these

Estrutura Genérica



Perimeter defense (of the domain)

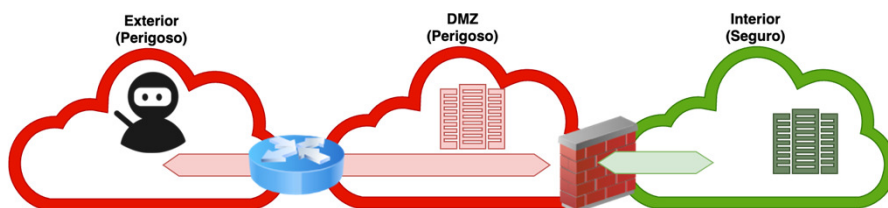
- Can be part of a defense in depth strategy

Consider an unsafe environment and a safe one

- Out: other domains or the Internet
- Inside: internal network

A single server: Bastion

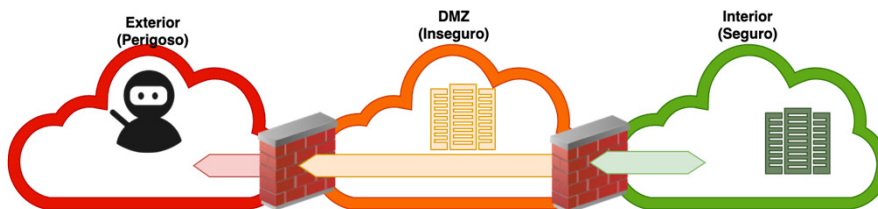
Estrutura Genérica



DMZ: DeMilitarized Network or Perimeter Network

- Insecure network
- Contains servers exposed to the world
- Sometimes necessary to use specific services/applications

Estrutura Genérica



DMZ may have some protection

- System of two Firewalls with different rules

External firewall: quite permissive

- Control access to all networks

Internal firewall: more restricted

- Control access to the internal network

Types: packet filters

Reject unauthorized interactions based on the content of IP datagrams

- IP addresses (source and/or destination)
- IP/transport header options
- Transport protocols and ports (origin and/or destination)
- Directions for creating virtual circuits
- Data sent via transport protocol
- Datagram size

Can analyze flow behavior

- Example: detect port scans (with nmap)

Typically supported by core OS components

- Example: iptables, ipfw, pf

Types: application gateways

Control interactions at the application level

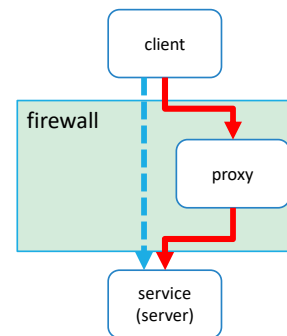
- But transparent to interacting applications
- There is usually a different firewall per protocol
 - proxy protocol

Client -> Proxy -> service (server)

- Proxies are servers

Aspects of operating a proxy

- User access control
- Analysis and modification of content
- Detailed logging
- Impersonation (proxying)
 - Transparent replacement of one of the interlocutors



Types: circuit gateways

Kind of application gateway

- Contacted directly by customers

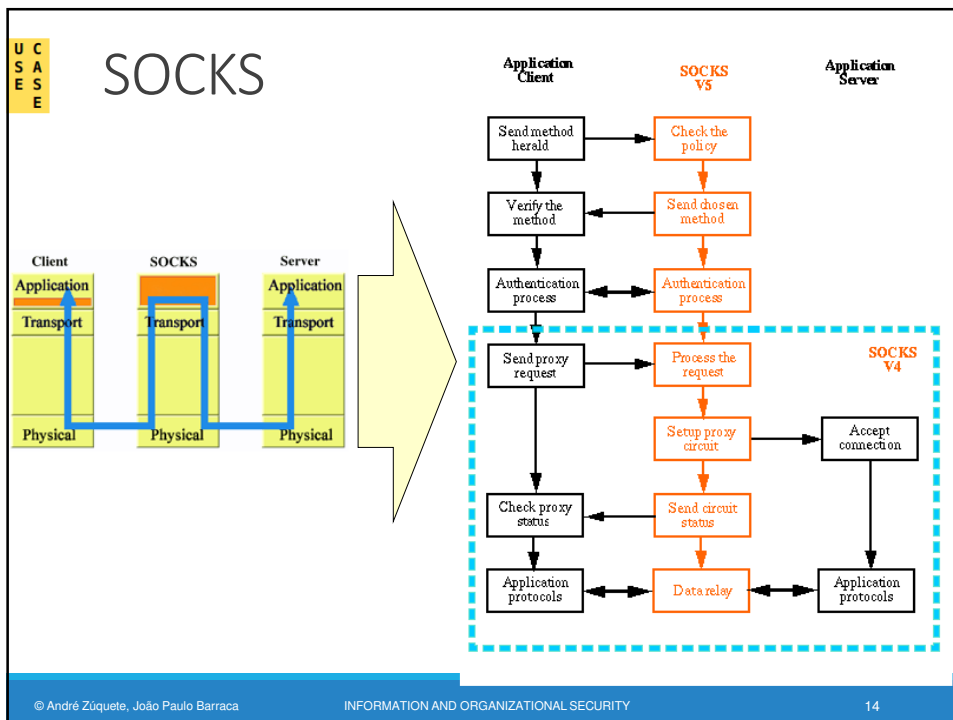
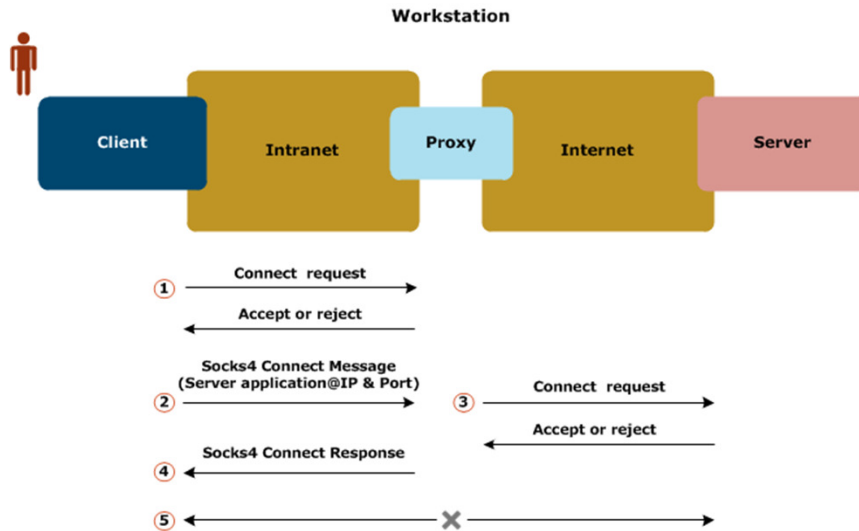
Non-transparent interposition

- For deploying specific authentication and authorization policies and mechanisms

Typically requires changing client applications

- Examples: SOCKS and HTTP Proxy

Types: SOCKS4 circuit gateways



Types: stateful packet filters

Dynamic (or context-sensitive) packet filter

- Sort of packet filter with historical context
- Context is key to certain decisions
- Common term: Stateful Packet Filter/Inspection (SPI)

Context examples:

- Decisions made for IP packet fragments
 - Defragmentation before filtering
- Established TCP virtual circuits
 - Circuit establishment requests are controlled
 - Established virtual circuits are allowed

Types: stateful packet filters

Context examples (cont.):

- Dynamic NAT tables
 - Creation of entries depending on observed traffic
- Request/response interactions over UDP
 - Dynamic authorization of responses to authorized requests
 - Example: DNS name resolution
- ICMP error messages
 - Related to previously sent TCP/UDP packets
- Identification of application protocols from data flows
 - To handle flows that use dynamic or “stolen” ports
 - Examples: FTP, RPC protocols, P2P protocols
 - Utility: filtering, transparent proxying, QoS

Bastion

Must run secure versions of operating systems

- With a secure configuration
- Only essential services are installed
- Telnet, DNS, FTP, SMTP and authentication proxies

Public servers should not perform in a bastion

- Examples: DNS, SMTP, HTTP, FTP, SSH, RAS, etc.
- Must run on isolated machines within DMZs
 - Preferably one per service
- Bastion only forwards traffic to the appropriate machines on a DMZ
 - And allows limited traffic from the DMZ

Bastion

It is often a platform for application gateways

- But the more proxies there are in the bastion, the lower its performance will be
- Proxies can run on specific machines
 - Security appliances
- Bastion only forwards traffic to and from the appliances

Secure execution of application gateways

- Independence
 - The compromise of one does not affect the rest
- No special privileges
 - Their compromise does not allow to affect the host

Topology: Dual-homed (w/ or w/o DMZ)

Architecture

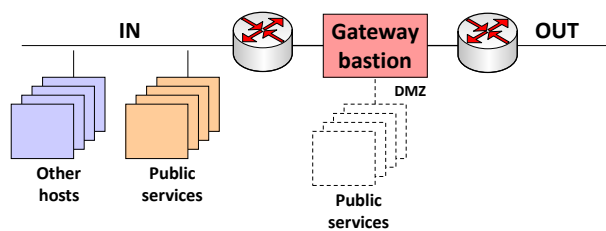
- A single machine
- Gateway bastion
- A pair of additional routers
 - To isolate the bastion of direct addressing
- Internal and public servers

Problems

- Bastion compromise disables firewall
- The firewall processing load is all on the bastion
- Public services are within the protected network

Benefits

- Simplicity
- Resource savings



Security services

Authorization

- From data streams (packet filters)
 - Transport or network level
- Users (application gateways / circuits)

Traffic Redirection

- For dedicated hosts
 - Local services (e.g., mail, www, ftp, etc.)
 - Proxies in security appliances
- Proxying
 - Explicit (e.g., circuit gateways)
 - Transparent (e.g., NAT address translations)

Security services

Application content processing

- Content analysis
 - Example: virus detection
- Changing high-level protocols
 - Example: virus removal

Secure communication

- Virtual Private Networks (VPNs)
 - Encryption and integrity control of data flows over public (insecure)
- Tunneling
 - IP domain extension to distant nodes
 - ex., PPTP, L2TP, IPSec

Security services

Defense against DoS attempts

- Attack detection
 - Abnormal traffic volumes, high volume, etc...
 - Filtering dangerous or malformed datagrams
 - ex. Land attack, Ping-of-Death
 - Activation of palliative measures
 - ex. SYN flooding relay/semi-gateway

Defense against information leaks

- Abnormal traffic detection
- Controlling behavior against known models

Limitations

They do not solve the problem of attackers within the internal network

- Unless the internal network is segmented into multiple subnets
- Switches typically do not support firewall operations
- VLANs provide minimal segregation (DMZ type)

Efficiency of control of all external connections

- Which can be done in parallel in countless ways:
 - PSTN & modems
 - Unregistered WLANs & Aps

Lack of control over camouflaged/hidden interactions

- Camouflaged interactions multiplexed by VPNs
- IP tunnels over HTTP, ICMP, DNS, etc.

Difficult to manage in environments with heterogeneous interests

- Universities, ISPs

Personal Firewalls

Adopted for the protection of individual / personal hosts

- Defense in depth vs. perimeter defense

Owners can set additional control policies

- Applications authorized to access the network
- The protocols that applications can use
- The hosts/networks that protocols/applications can interact with

Reduce the risk of compromise between hosts on a network

- Allows a machine to protect itself independently of the protection provided by its network
 - Do not make assumptions regarding other network protections
- Useful for machines that migrate between networks

Personal firewalls: issues

Normal users are not network security experts

- They don't normally understand how IP networks work
 - IP addresses, transport ports, transport protocols, etc.
- They do not know how to assess whether a given interaction is normal, acceptable, etc.
- They don't know the basic security policies they should apply

Blocking suspicious interactions may nullify functionality

- Network communication is currently commonplace
- Applications do not inform users of their communication needs

Personal firewalls: issues

Operational complexity

- Different operating environments → different policies
- Different network interfaces → different policies

The combination of operational scenarios, network interfaces and acceptable interactions for each case leads to a huge number of rules

- Confusion, incoherence → difficult to detect vulnerabilities

iptables

Packet filter (with context, or stateful)

- Integrated with Linux kernel TCP/IP
- Can be extended in several ways
 - New core modules
 - User mode applications

5 chains

- INPUT, OUTPUT, FORWARD
- PREROUTING, POSTROUTING

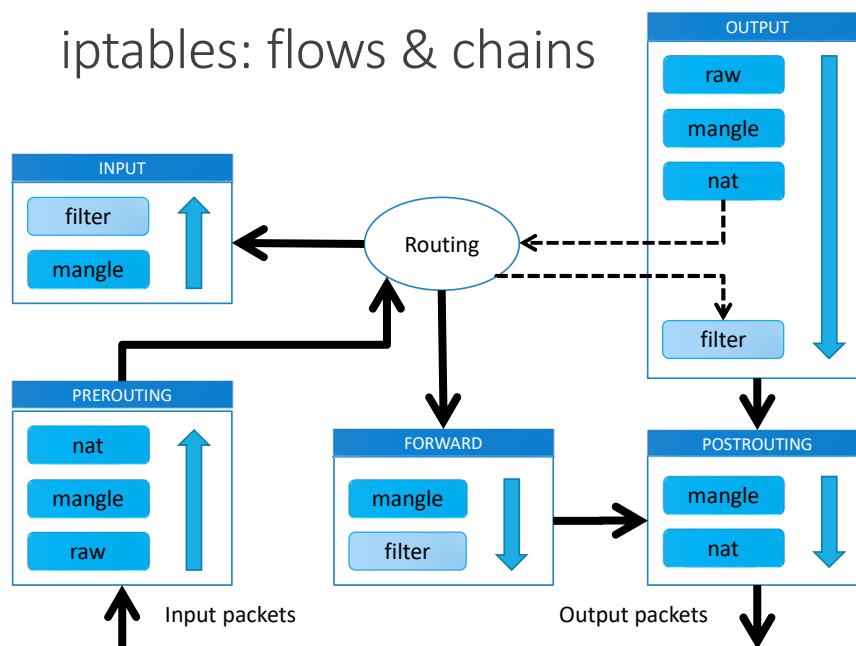
4 tables (per chain, but not for all)

- raw, mangle, nat, filter

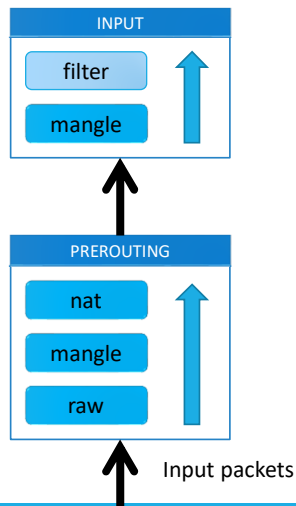
Various extra modules

- e.g., CONNTRACK (connection tracker, or flow follower)

iptables: flows & chains



iptables: traffic for the host

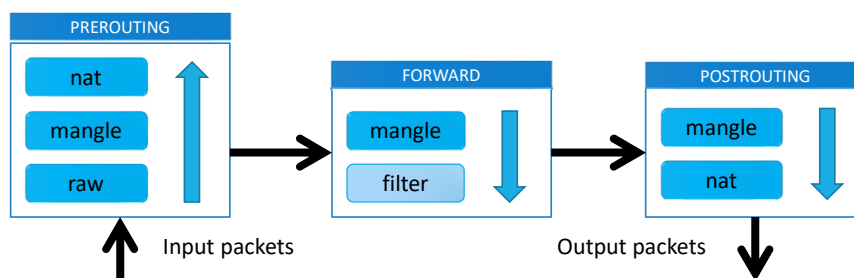


© André Zuquete, João Paulo Barraca

INFORMATION AND ORGANIZATIONAL SECURITY

29

iptables: routed traffic

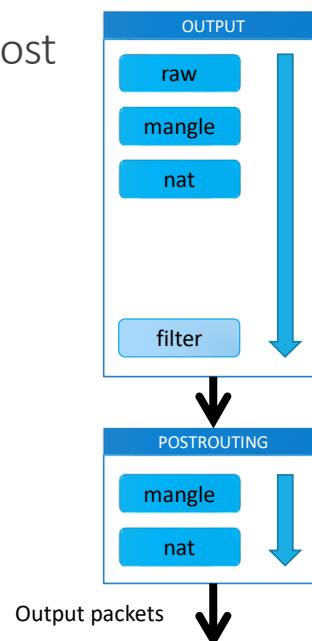


© André Zuquete, João Paulo Barraca

INFORMATION AND ORGANIZATIONAL SECURITY

30

iptables: traffic from the host



iptables: decisions

Basic decisions

- ACCEPT
 - Let the package continue
- DROP
 - Discard the package
- CONTINUES
 - Use decisions from other rules

Reusable Decisions

- New chains
- Jump to a new chain
 - The name of the chain is the decision
- RETURN
 - Leave the current chain

Other decisions

- LOG
- MARK
 - With internal label
 - Useful for making coherent decisions across different chains
- REJECT
 - Rejection with error message
- SNAT, MASQUERADE
 - Source NAT (masquerading)
- DNAT, REDIRECT
 - Destination NAT (port forwarding)
- Actions by applications
 - QUEUE

Iptables exploitation: fail2ban

Agent that observes records, comparing them with patterns

- Can prevent some DoS, brute force attacks (SSH), scans
- Reactive: Does not prevent the attack from starting
 - May not prevent attacks with few interactions
- Can be used with any service that creates records

Jail: a context composed of several rules

- Defines what to observe and what action to take
- Action: Implement a specific response
 - example: block communications on the firewall
 - Can use a local or remote firewall

Filter: a set of regexps that signal anomalous behavior

- Composed of expressions to consider and ignore (white list)

Iptables exploitation: fail2ban

“Anonymous” server, without content # of IPs blocked due to SSH access attempt

