Network Security
IN2101

Prof. Dr.-Ing. Georg Carle
Dr. Heiko Niedermayer
Dr. Miguel Pardal
Dipl.-Ing. Univ. Quirin Scheitle

Chair for Network Architectures and Services
Department of Computer Science
Technische Universität München
http://www.net.in.tum.de

Outline

- Network Middleboxes
- Firewalls
  - Topologies
- Intrusion Detection Systems
  - Detection methods
  - Data sources
  - Reaction

Network Middleboxes

Middleboxes

- Definition:
  - *“any intermediary box performing functions apart from normal, standard functions of an IP router on the data path between a source host and destination host”*
  - Transforms, inspects, filters, or otherwise manipulates traffic for purposes other than packet forwarding

Middleboxes

- RFC 3234 defines classification facets:
  - Protocol layer
  - Explicit vs implicit
  - Single-hop vs multi-hop
  - In-line vs call-out
  - Functional vs optimizing
  - Routing vs Processing
  - Soft-state vs Hard-state
  - Failover vs Restart

Types of middleboxes

- Firewalls (FW)
  - Filter traffic based on a set of pre-defined security rules defined by a network administrator
- Intrusion Detection Systems (IDS)
  - Monitor traffic and collect data for (offline) analysis for security anomalies
  - Capable of more complex inspection than Firewalls
- Network Address Translators (NAT)
  - Replace the source and/or destination IP addresses of packets that traverse them
  - Allow multiple (private) hosts to share a single (public) IP address
- Load Balancers (LB)
  - Provide one point of entry to a service, but forward traffic flows to one or more hosts that actually provide the service

Security Middleboxes

- Firewalls (FW)
  - Combined with Network Address Translators (NAT)
- Intrusion Detection Systems (IDS)

Firewalls

The history of Firewalls

- Term comes from *Building Construction*
  - Wall that keeps a fire from spreading from one part of the building to another

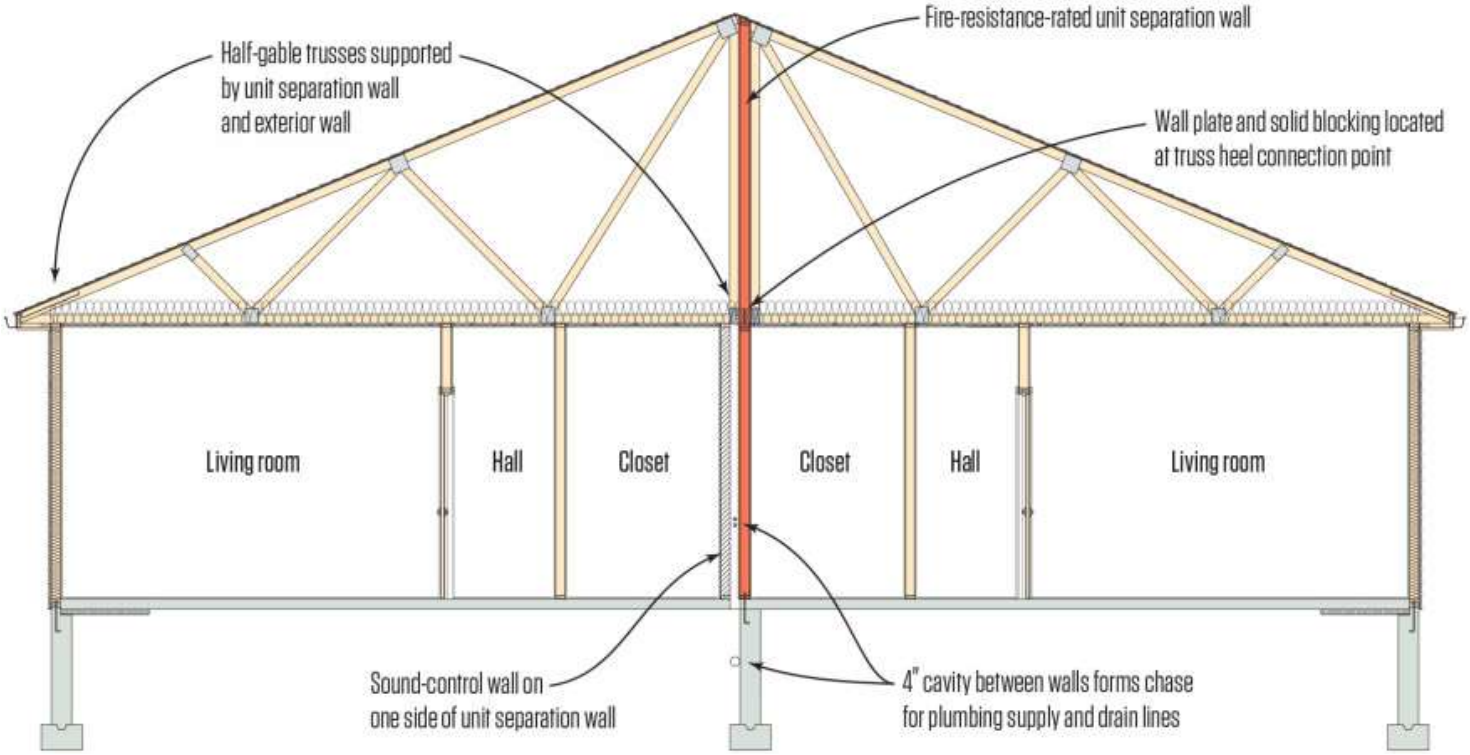
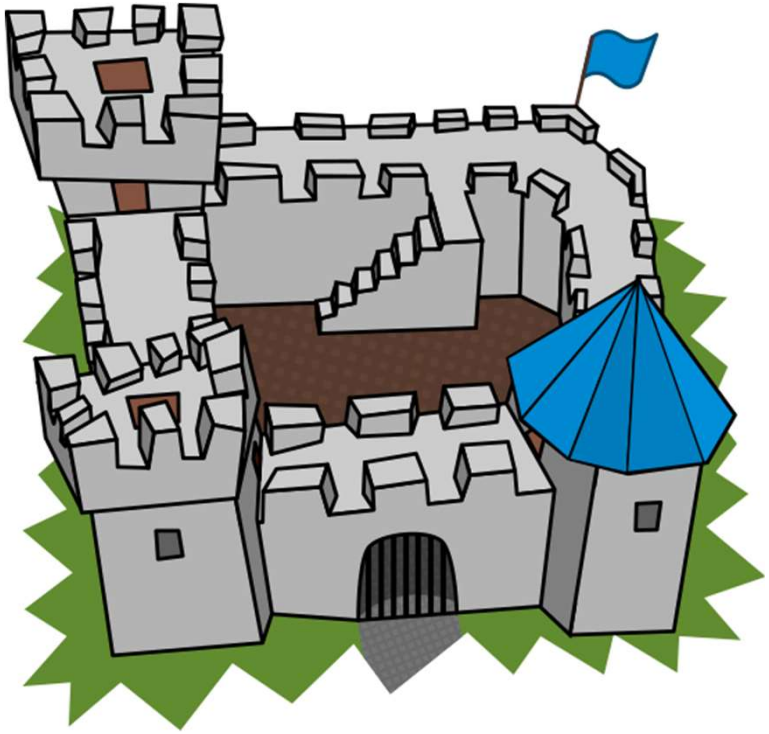


Image credits: sbcmag.info

Firewall analogy

- Better compared to a *moat* of a medieval castle
  - Prevents attackers from getting close to other defenses
  - Restricts people to **enter** at one carefully controlled point
  - Restricts people to **leave** at one carefully controlled point



Problems addressed by Firewalls

- Connect protected networks to the Internet
  - Each machine accessible from the Internet is a potential source of vulnerabilities
- Enforce access control policies
  - In a simple, scalable way
- Provide control to services
  - Authentication
  - Authorization

- Firewall allows the enforcement and implementation of security policies in a **centralized** manner

Firewall assumptions

1. Firewall can intercept all the data flows
2. Firewall can control the data flows passing through it
3. Firewall is immune to penetration attacks

Firewall functionality

- **Supervise all communication**

- **Extend reach of protected network**
  - Tunnel for Virtual Private Network (VPN)
    - e.g. PPTP, IPsec tunneling

- **Conceal internal structure of protected network**
  - Network Address Translation (NAT)
    - Source NAT – *Masquerading*
      - Hide the source address in outgoing packets and replace with the gateway address
    - Destination NAT – *Port Forwarding*
      - Allow packets addressed to the gateway to be redirected to an internal server

Firewall types

- **Packet Filter**
  - Reject non authorized interactions according to the content of the IP datagrams
- **Application-Level Gateway**
  - Controls the iterations at the application layer
  - Provides caching for frequently requested data
  - Typically there is a specific **proxy** for each protocol
- **Circuit Gateways**
  - Similar to *Application Gateways*
    - But with **non-transparent interposition**
  - Applications are aware of the gateway and can contact it to request passage
  - Usually implies changes to the clients applications
    - ex. SOCKS proxies

Comparison of firewall types

- *Packet Filters*
  - Faster
  - Harder to configure
  - Unable to protect against “misbehaved” protocols
    - ex.: ftp, portmapper
  - Current/previous state is not always considered
- *Application-level gateways*
  - Slower
  - Easier to configure
    - Individually for each protocol/application
  - Allow authentication mechanisms
  - Allow more fine-grained control
    - ex.: deny “put” in FTP, deny “delete” in HTTP
  - Less adaptable to new protocols

Firewall example: Linux iptables

- Manage packet filtering and NAT rules
  - Available on all Linux distributions
- Tables -> Chains -> Rules
- Built-in tables:

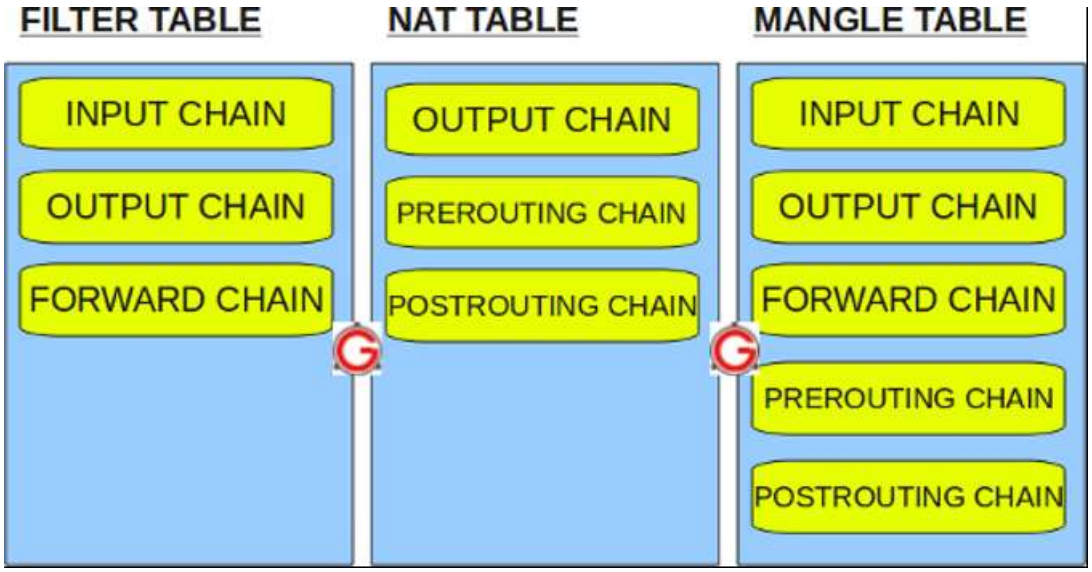
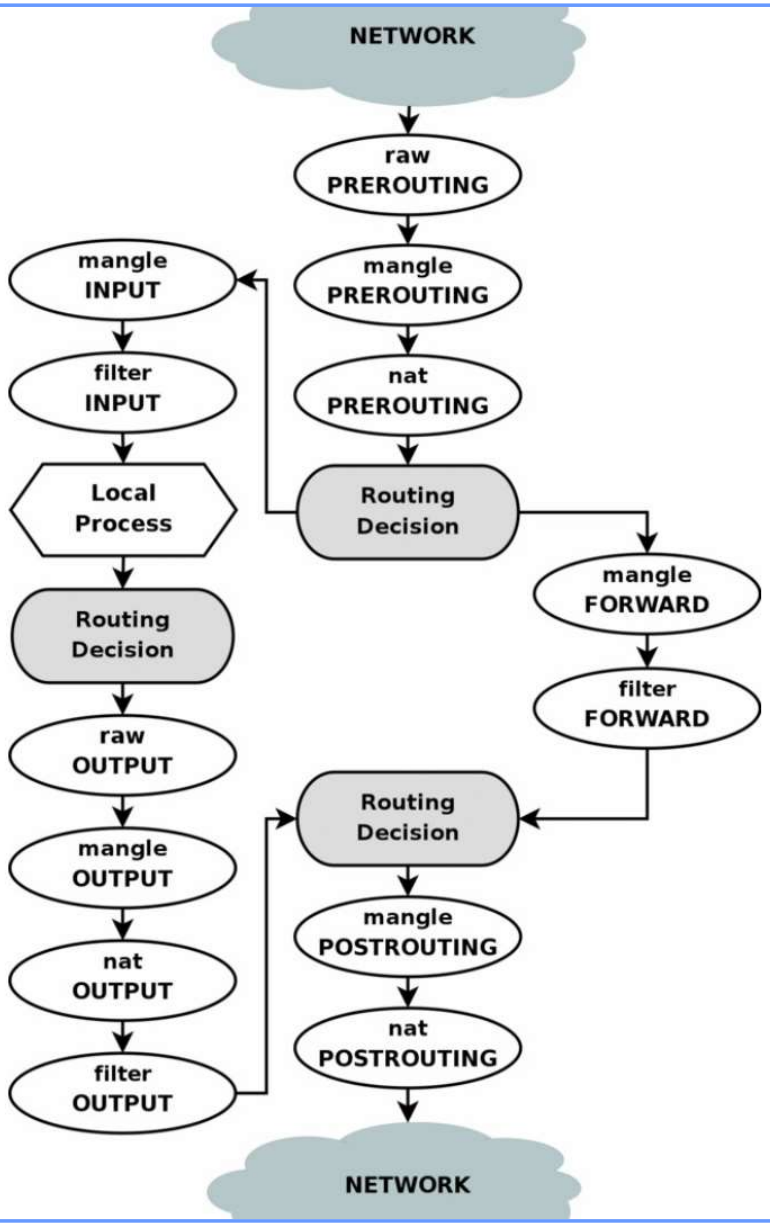


Image credits: Ramesh Natarajan

Overview of packet flow on iptables chains



iptables rules

- Chains define lists of rules
- Rules contain **criteria** and **target**
  - If criteria is matched, executes target
  - If the criteria is not matched, moves on to the next rule
- Target values:
  - ACCEPT – Firewall will accept the packet
  - DROP – Firewall will drop the packet
  - REJECT – Firewall will send back a reject packet
  - …

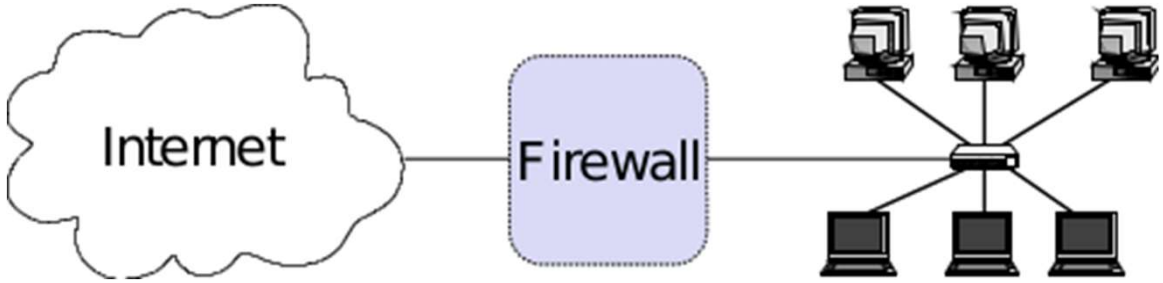
iptables command example

```
$ iptables -t filter -L

Chain INPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere
tcp dpt:ssh state NEW,ESTABLISHED

Chain FORWARD (policy DROP)
target     prot opt source               destination

Chain OUTPUT (policy DROP)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             anywhere
tcp spt:ssh state ESTABLISHED

$ man iptables # for more information
```

Firewall topologies

Firewall placement

- **Controlled access** at the network level
- Install the Firewall where
  a less trusted network is connected to a protected subnetwork
  - Typically, firewall is placed between
    the Internet and a local network

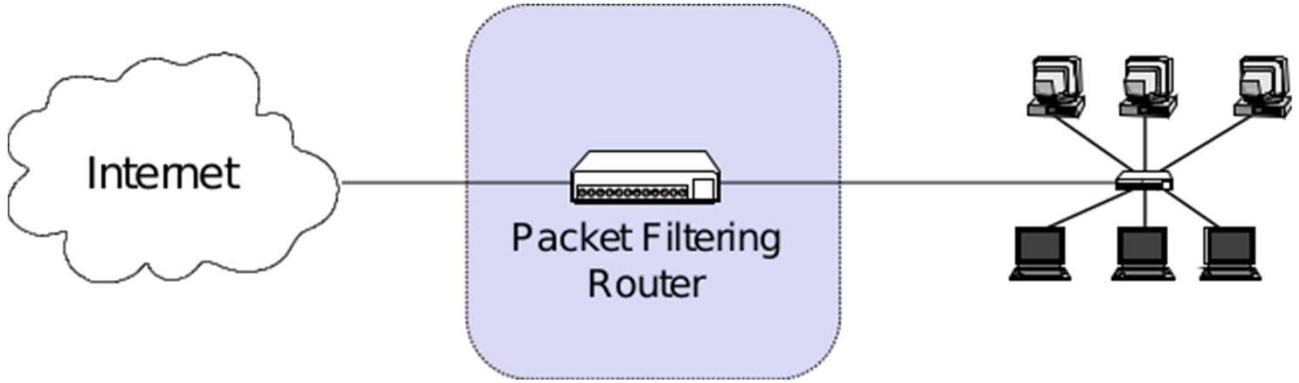


Firewall topologies

- Simple packet filter
- Dual-homed host
- Screened hosts
- Screened subnet

Simple packet filter topology

- A packet filtering router with two interfaces

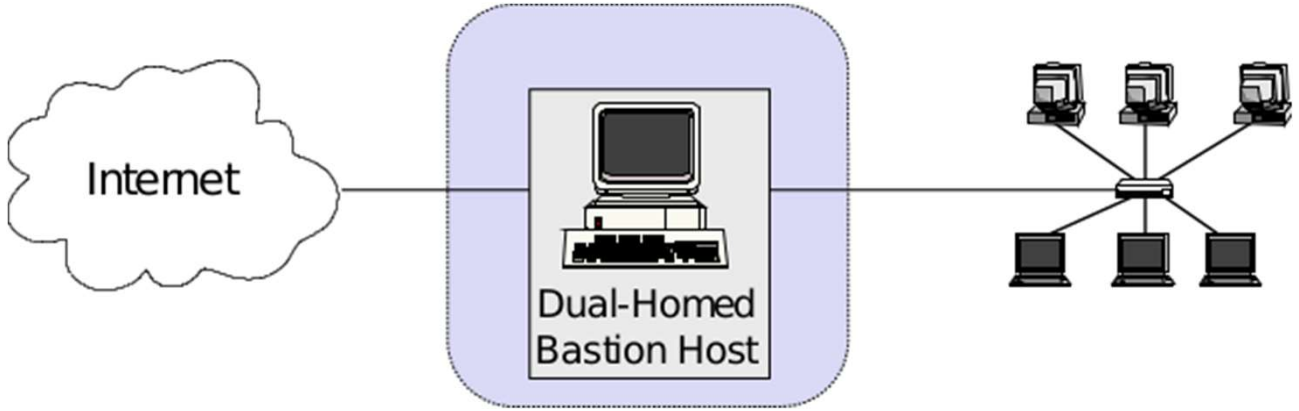


Bastion Host

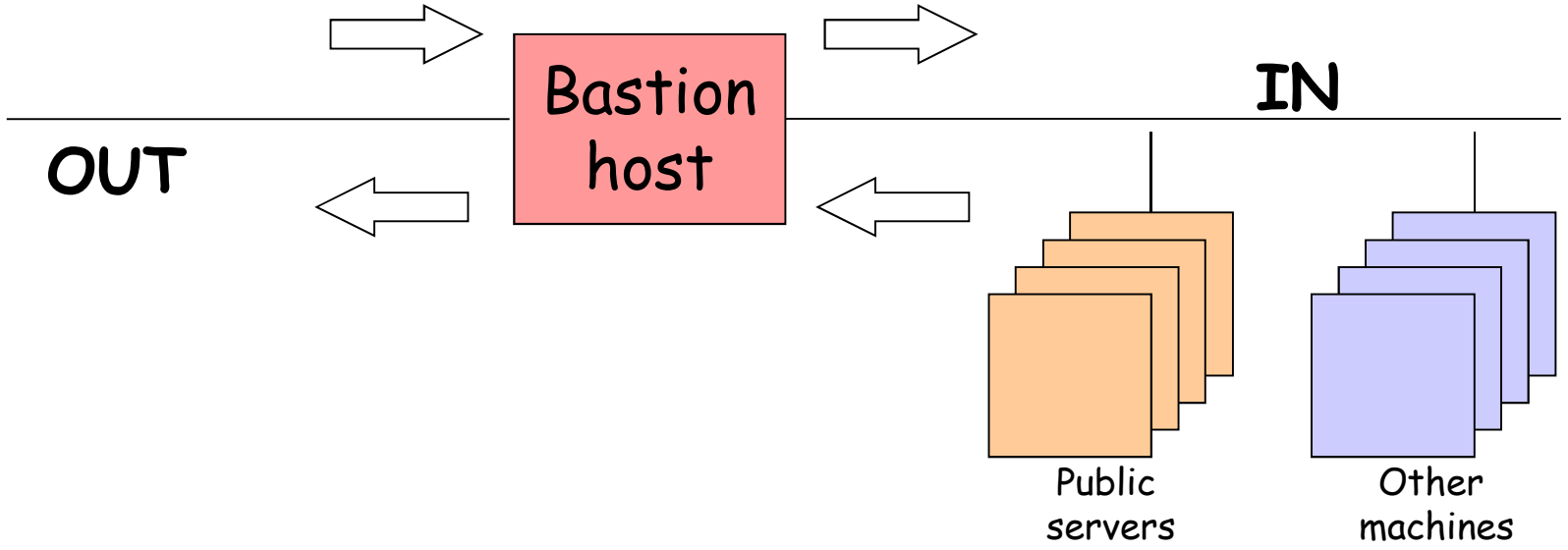
- Definition:
  - *“A bastion host is a host that is more exposed to the hosts of an external network than the other hosts of the network it protects.”*
- A bastion host may serve for different purposes:
  - Packet filtering
  - Providing proxy services
  - Usually a combination of both

Dual-Homed Host topology

- Dual-Homed: Host is part of two networks (has two NICs)
- Bastion Host is Firewall + Application Proxy



Dual-homed host



Analysis of Dual-homed topology

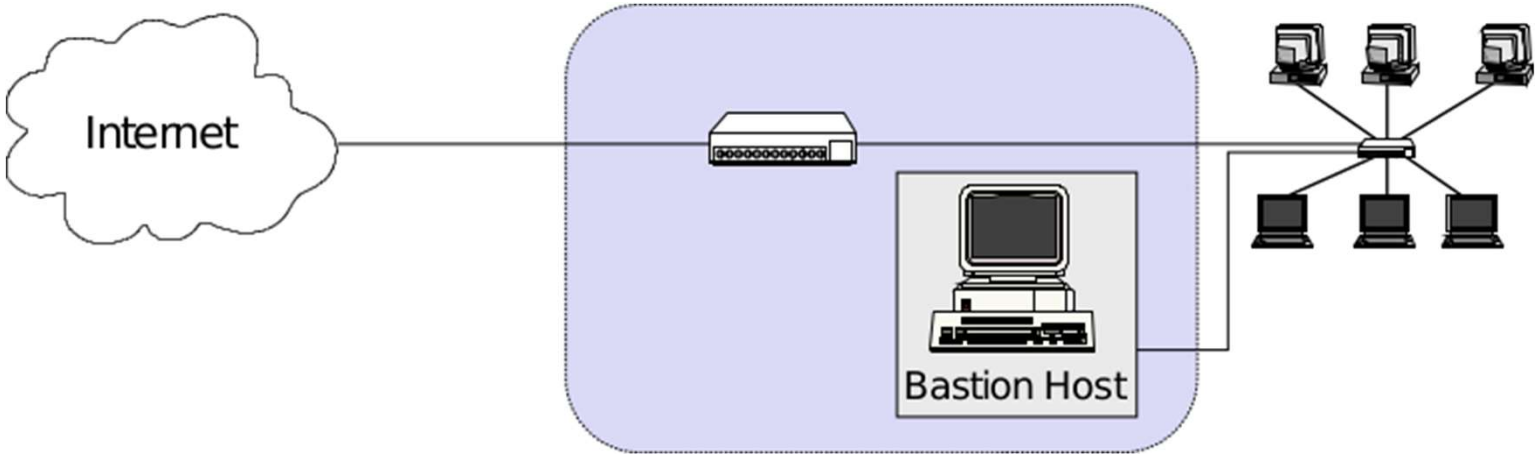
- Dual-homed
  - Single box (Bastion Host)
- Advantages
  - Single machine: simplicity and resource economy
- Problems
  - Public servers are within the protected network
    - If they are compromised, they can attack other hosts directly
  - Bastion Host is bottleneck: all the processing load is on the firewall in a single machine
  - Compromising the Bastion Host deactivates the firewall
    - **Worst-case scenario**

Securing Bastion Hosts

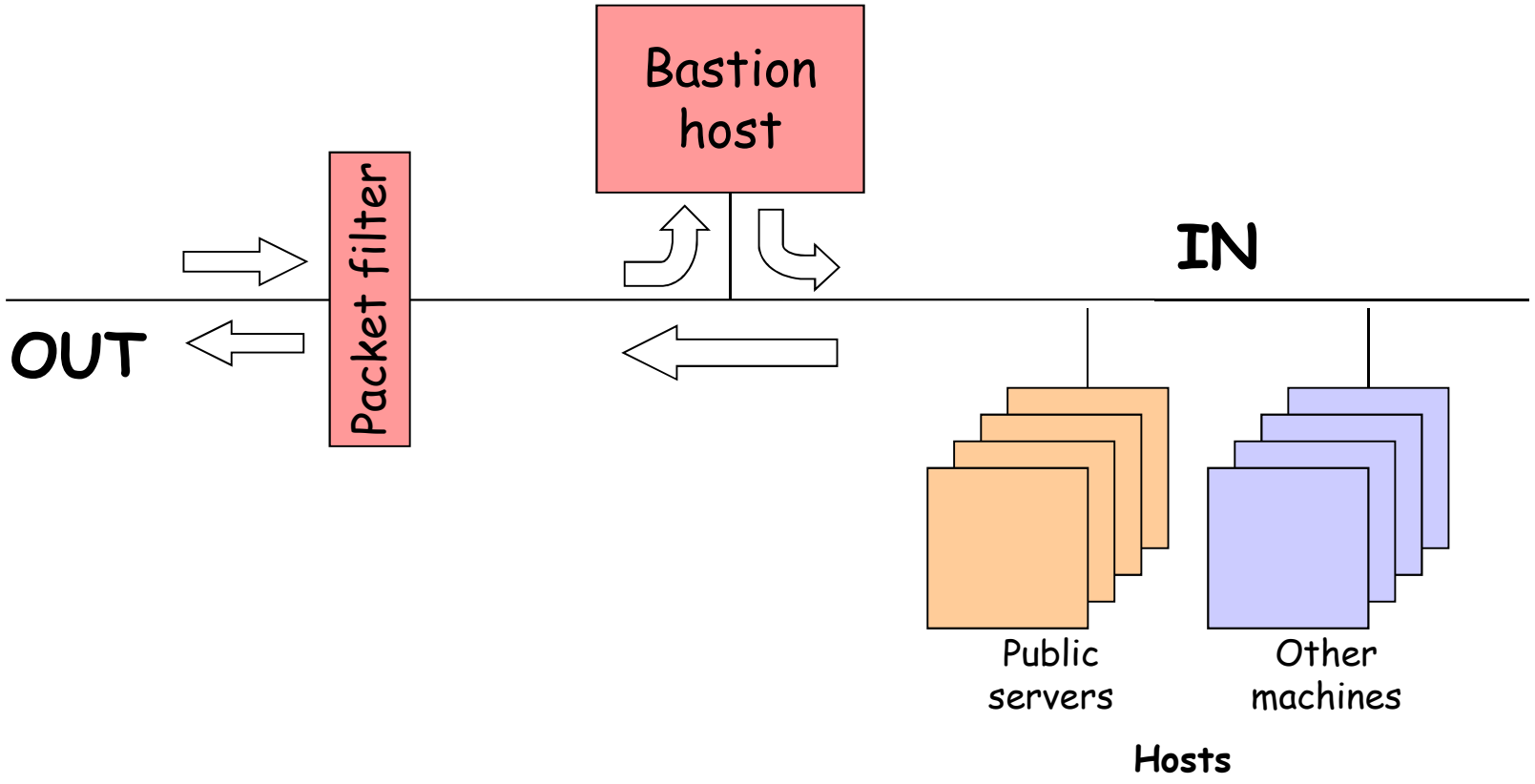
- Prepare for the bastion host to be compromised
- Connect in such a way that it cannot sniff internal traffic
- Extensive and tamper-resistant logging
- Reliable hardware configuration and physically secure location
- Disable ssh password login (only public key login)
- Disable user accounts
- Monitor the machine closely
  - Reboots, usage / load patterns, etc.
- Perform regular backups

Screened Host topology

- Packet filter protects network and Bastion Host
- Bastion Host is Proxy (may be accessible from the Internet)
  - Compromised Bastion Host compromises the internal network



Screened hosts



Analysis of Screened Hosts topology

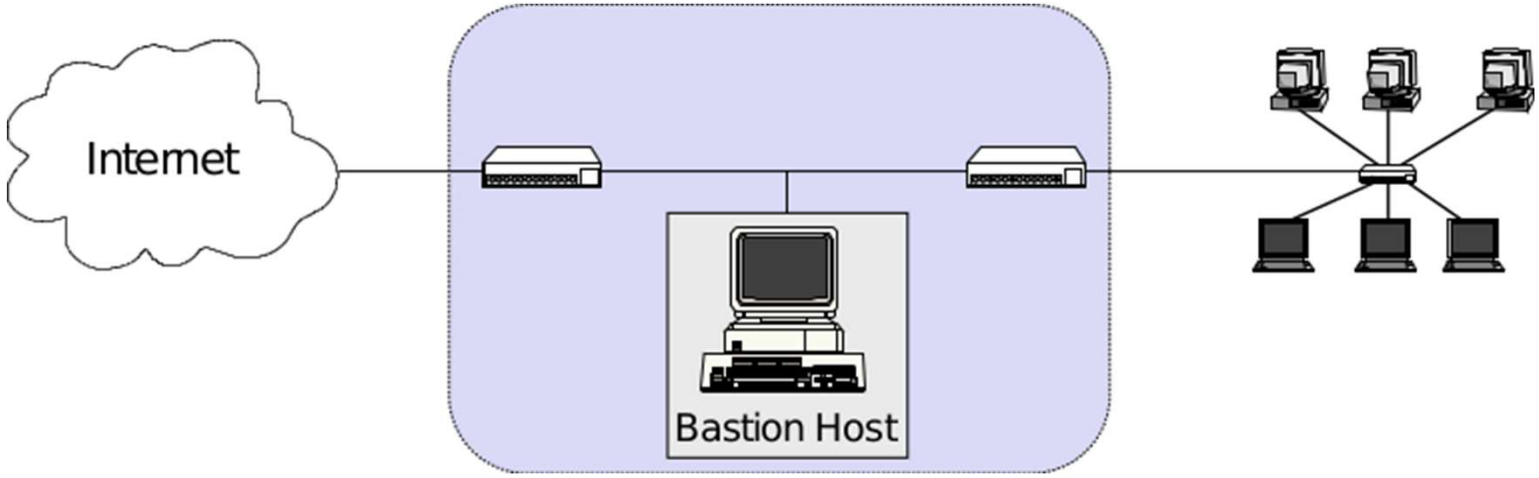
- Screened hosts
  - Packet filter for external access
  - Bastion host is gateway to the inner network
    - Has more fine grained control over the data flow
    - Forwards authorized flows to internal nodes
- Advantages
  - Balances the workload between the router and the gateway
- Disadvantages
  - Public services are still in the protected network

DMZ – DeMilitarized Zone

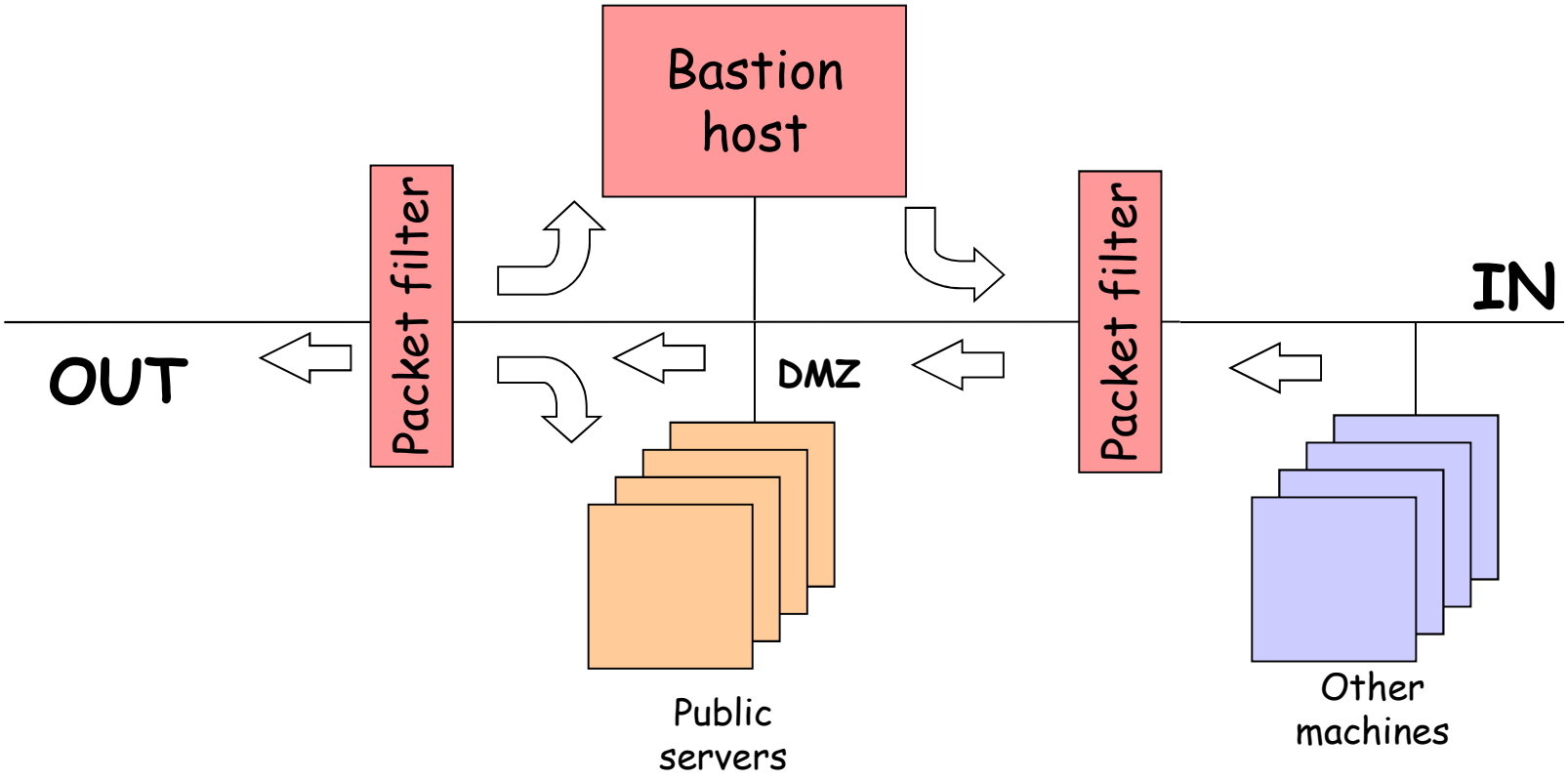
- Network Security use:
  - Not part of the protected perimeter
  - Not part of the outside because it is controlled
- Real world example:

Screened Subnet topology - DMZ

- Demilitarized Zone (DMZ): perimeter network
- Hosts Bastion Host (Proxy) and publicly accessible servers
- Second packet filter in case they are compromised
  - Protection for the internal network
- Requires two firewalls



Screened subnet



Analysis of Screened Subnet topology

- Screened subnet
  - One packet filter for controlling external access
  - One packet filter for controlling internal access
  - One Bastion Host and a DMZ between the two routers
    - The public services are placed in the DMZ
  - All the data flows allowed by the external router is sent to the gateway or to the public services in the DMZ
  - The gateway performs a more fine grained control over the data flow allowed by the router for the protected network
- Advantages
  - Workload balancing
  - Marginal risks regarding the public services
- Disadvantages
  - Low control over the activities going on in the DMZ machines

Intrusion Detection Systems

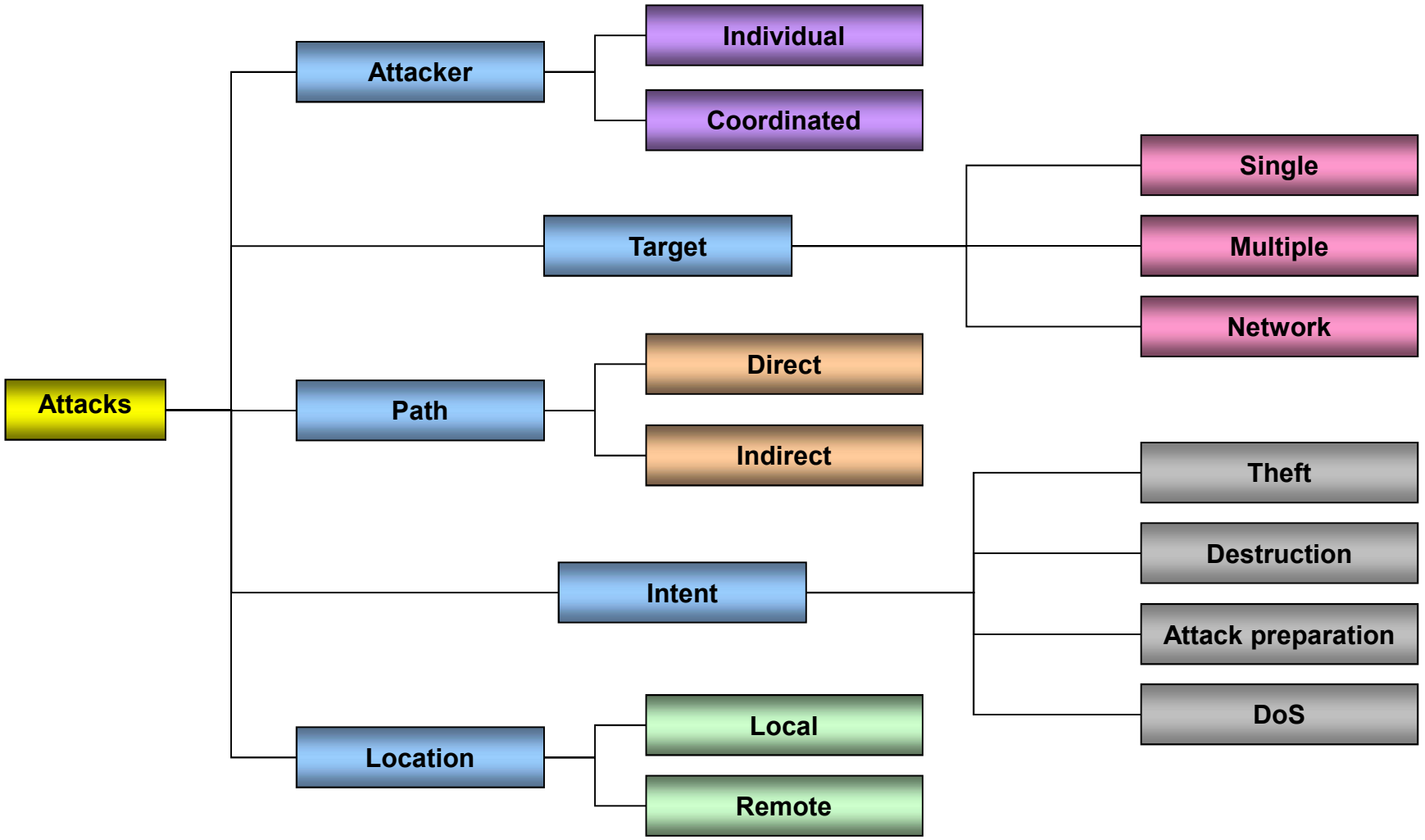
Motivation for IDS

- All systems have **vulnerabilities**
  - Known or unknown
  - Can be used to carry out attacks

- Attacks can be detected by:
  - Being aware of / seeking unusual or suspicious actions
  - Searching for unusual or suspicious alterations in the information stored in the system

- What do we want to detect?
  - Intrusion preambles (probes)
  - Intrusion accesses from the outside
  - Abusive behaviors from the inside

Attack classification



Definitions

- **Intrusion**
  - Any set of actions with the intent of compromising the Confidentiality, Integrity, or Availability (CIA) of a resource

- **Intrusion Detection System (IDS)**
  - Software that has the function to detect, identify, and respond to unauthorized or abnormal activities in the targeted system

Honeypots

- *Deception systems*
  - Vulnerable system created with the goal of focusing the attackers attention to an apparently weaker system:
  - Ability to gather forensic information
  - Deflect the attack form the real system
  - Detect and learn about new attacks
  - Problem: can be used as an attack origin

IDS classification

Detection method	Misuse detection	
	Anomaly detection	
Data source	Network-based	Hybrid
	Host-based	
Detection delay	Real-time	
	A posteriori	
Reaction	Passive	
	Active	
Analysis	Individual	
	Cooperative	

Detection method

Misuse Detection

- *Knowledge-driven*
- System activity analysis in search of known attack patterns (**attack signatures**)
- Advantages:
  - Very efficient detection
  - Reduced amount of false positives
- Disadvantages:
  - Only detects known attacks
  - May generate a large amount of false negatives

Anomaly Detection

- *Behavior-driven*
- Uses statistical heuristics (threshold values) or Machine Learning and other Artificial Intelligence techniques
- Advantages:
  - Able to detect new attacks
  - Can be used to collect data to define new attack signatures
- Disadvantages:
  - Typically needs a large amount of training data sets to learn attacks
  - Extremely difficult to define adequate threshold values
  - Large amount of false positives

Data source

NIDS

- **N**etwork-Based **IDS**
  - Capture and performs traffic analysis on the network (packets)
- Advantages:
  - Small amount of sensors are able to monitor a large network
  - Little to no impact in the network performance
  - Can become invisible to attackers
- Disadvantages:
  - Hard to process large amounts of data flowing through the network
  - Difficult to install in networks that are not shared
  - Cannot analyze *ciphered* data
  - Cannot assess with certainty if an attack was successful
  - Difficult to be aware of the connection state

Attacks targeted by NIDS

- Unauthorized access to the internal network
- Base/bridge to other attacks
- Theft of information in the network
- Password stealing
  - E.g. brute-force attempts
- Abuse of bandwidth resources
- Denial of Services (DoS)
  - Improperly formatted packets
  - Abnormally high data/packet flow
  - Distributed DoS

NIDS example: SNORT

- Open-source
- SNORT can be used as a:
  - Packet sniffer
    - Live analysis
  - Packet logger
    - *A posteriori* analysis
- Stable
- Flexible
  - Allows custom rules
  - There is an active community keeping attack signatures up-to-date

https://www.snort.org/

HIDS

- **H**ost-Based **IDS**
- Works over information collected from individual systems
- Advantages:
  - Able to observe/detect attacks that cannot be perceived by the NIDS
  - Able to function in environments with *ciphered* data
  - Not affected by commuted networks (virtual channels)
- Disadvantages:
  - Hard to manage
  - Can be attacked and deactivated
  - Unable to detect scans
  - Degrades the performance of the systems

Attacks targeted by HIDS

- Abuse of privileges
  - Employees, Administrators
  - Sub-contracted staff
- User accounts usurpation:
  - Old employees
  - Created by misbehaving administrators
- Inadvertently assigned privileges
- Access and modification of critical information
  - Browsing critical information
- Information leakage
- Modification of configuration files
- Modification of Web site

HIDS example: OSSEC

- Open-source
- OSSEC has:
  - Correlation and analysis engine
  - Log analysis
  - File integrity checking
  - Centralized policy enforcement
  - Rootkit detection
  - Alerting
  - Active response
    - E.g. black list IP addresses
  - Optional web-based graphical monitoring interface
- Runs on most operating systems
  - Linux, OpenBSD, FreeBSD, MacOS, Solaris and Windows

https://ossec.github.io/

Detection delay

Detection delay

- “Real”-time
  - Intercepts data and control flows
  - Interferes with performance

- *A posteriori*
  - Log analysis
  - Can be more easily parallelized

Reaction

Attack reaction

- **Passive**
  - Only detect and report the detection results:
    - Alarms and notifications
    - SNMP Traps
    - Logging and report creation

- **Active**
  - Provides response mechanisms to the attacks:
    - Close connections: TCP RST
    - Perform system/operational modifications
    - Reconfiguration of routers/firewalls, etc.
  - Counterstrike
    - Careful… you can start a **Cyberwar**
      - Best left for military

Analysis

- **Individual**
  - IDS works on its own
    - Configuration
    - Receives periodic updates
- **Cooperative**
  - IDS collaborates with other IDS
    - Threat sharing communities
      - "Social" IDS
    - Receives updates, but also uploads information

Summary: IDS classification

Detection method	Misuse detection	
	Anomaly detection	
Data source	Network-based	Hybrid
	Host-based	
Detection delay	Real-time	
	A posteriori	
Reaction	Passive	
	Active	
Analysis	Individual	
	Cooperative	

Summary

- Network Middleboxes
  - Firewalls
    - Different topologies
      - Performance/Security trade-offs
  - Intrusion Detection Systems
    - Detection methods
      - Attacks signatures vs anomalies
    - Data sources
      - Host IDS, Network IDS, combined

- Both FW and IDS are important security **mechanisms** that can enforce security **policies**