TÉCNICO LISBOA

Firewalls and Intrusion Detection

Segurança Informática em Redes e Sistemas
2022/23

Miguel Pardal

Ack: Carlos Ribeiro, André Zúquete, Miguel P. Correia,
Ricardo Chaves

Roadmap

- Middleboxes
- Firewalls
- Intrusion Detection Systems
- SIEMs

Roadmap

- **Middleboxes**
- Firewalls
- Intrusion Detection Systems
- SIEMs

Middlebox

- Placed in the “middle” of communication path
  - Between source and destination hosts
- Definition:
  - *A network node 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

Middlebox examples

- Traffic Monitors
  - Logging of Internet usage
- Load Balancers (LB)
  - Provide one point of entry to a service, but forward traffic flows to one or more hosts that provide the service
- 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

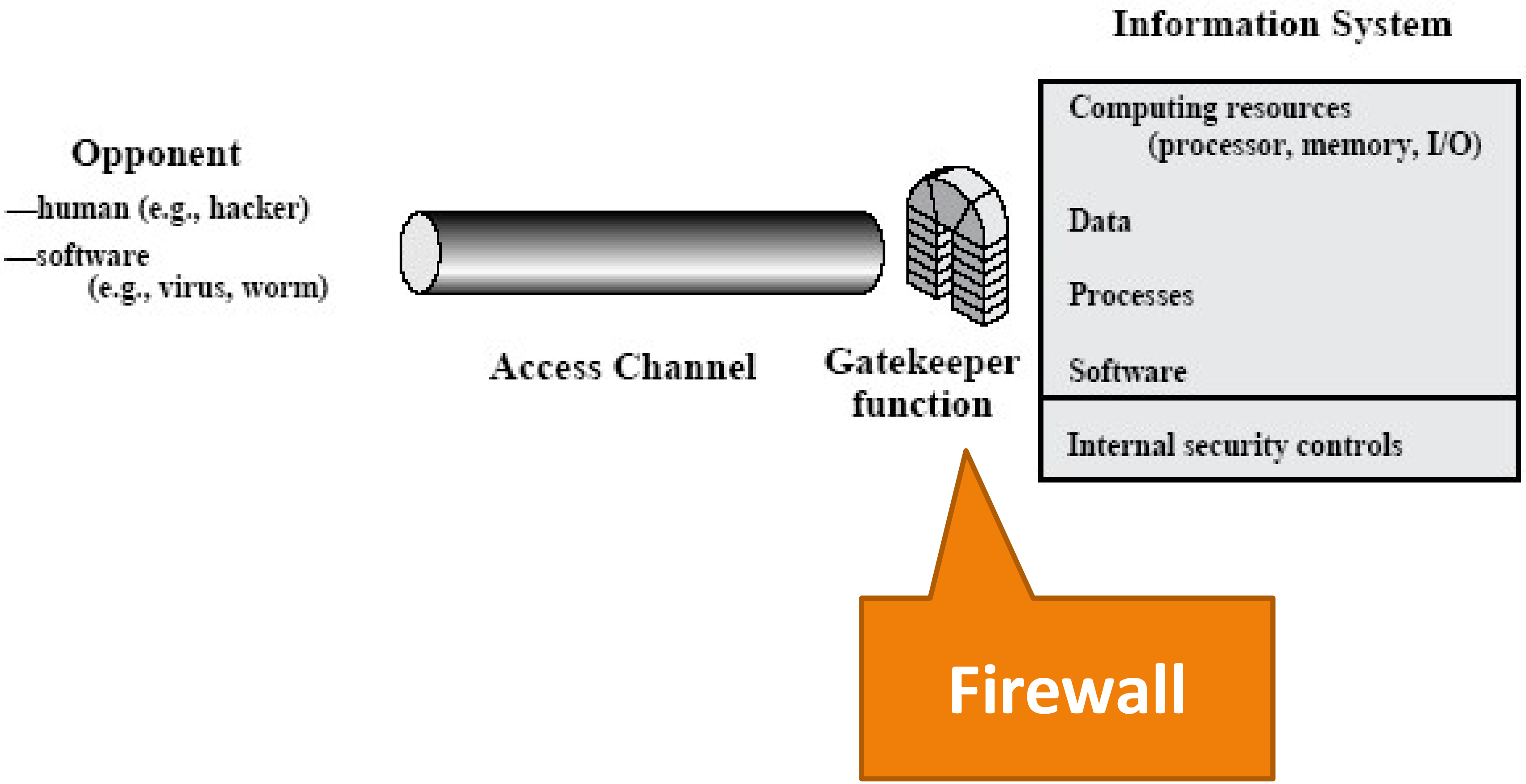
Security Middleboxes

- Firewalls
  - Filter traffic based on a set of pre-defined security rules defined by a network administrator
- Network Intrusion Detection Systems (NIDS)
  - Monitor traffic and collect data for (offline) analysis for security anomalies
  - Do more complex traffic inspection than Firewalls

Roadmap

- Middleboxes
- **Firewalls**
- Intrusion Detection Systems
- SIEMs

Gatekeeper for access control

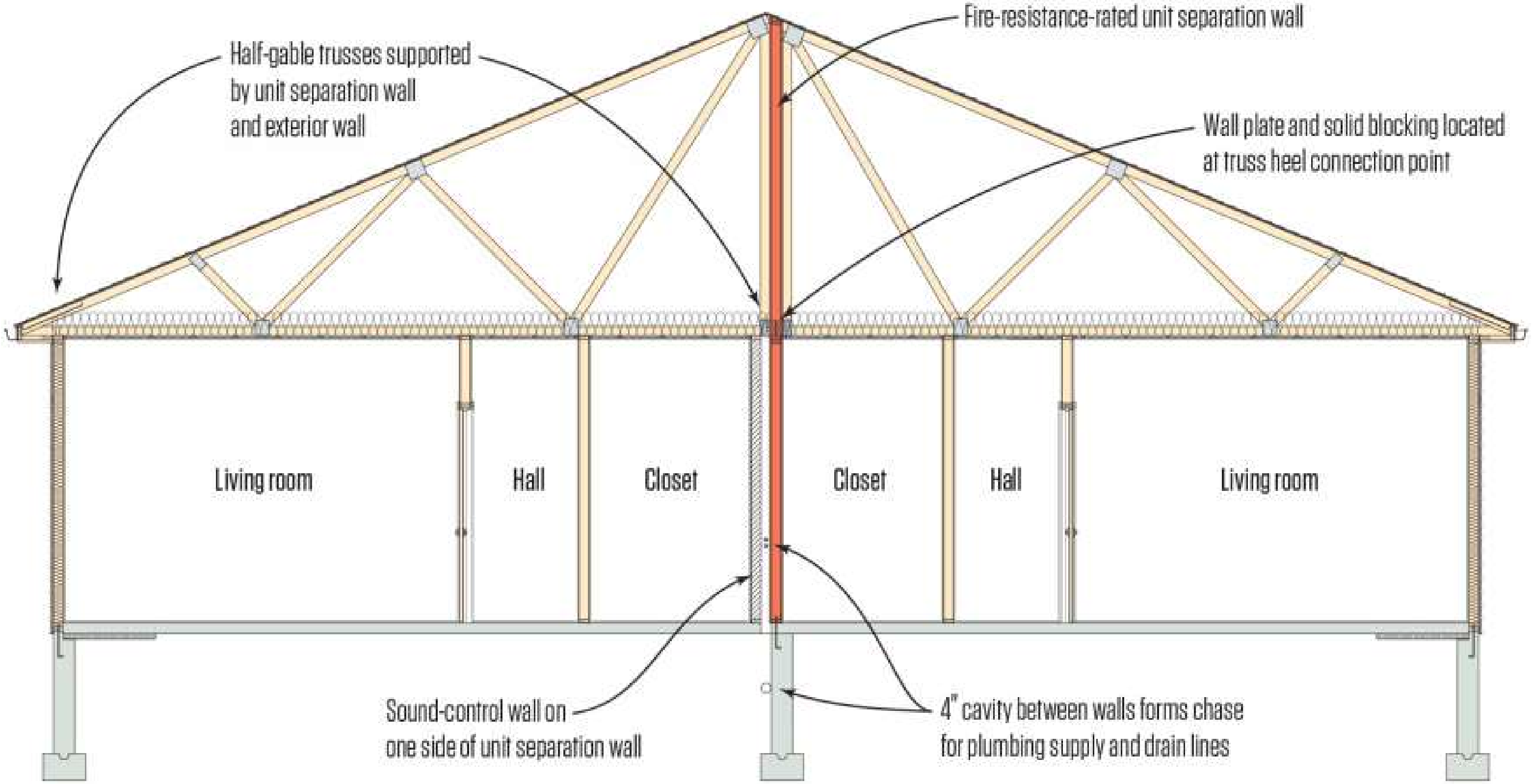


Roadmap

- Middleboxes
- **Firewalls**
  - **Concept**
- Intrusion Detection Systems
- SIEMs

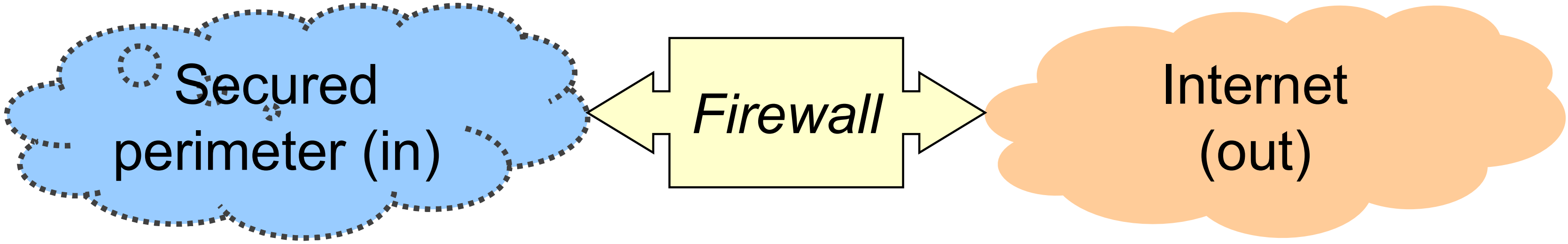
Firewall in building construction

- Wall that keeps a fire from spreading from one part of the building to another


Half-gable trusses supported by unit separation wall and exterior wall
Fire-resistance-rated unit separation wall
Wall plate and solid blocking located at truss heel connection point
Living room
Hall
Closet
Closet
Hall
Living room
Sound-control wall on one side of unit separation wall
4" cavity between walls forms chase for plumbing supply and drain lines

Firewall

- A Firewall is a means of protecting a local system or network of systems from network threats
  - Creates a **perimeter of defense**
  - Allow only authorized access to inside network
    - Set of authenticated users/hosts
  - Prevents illegal modification/access of internal data
  - Mitigates denial-of-service attacks



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 Firewall

- Connection of protected networks to the Internet
  - Each machine accessible from the Internet is a potential target of attacks
- Enforce access control policies
  - In a simple, scalable way
  - Authentication
  - Authorization

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

What does a firewall do?

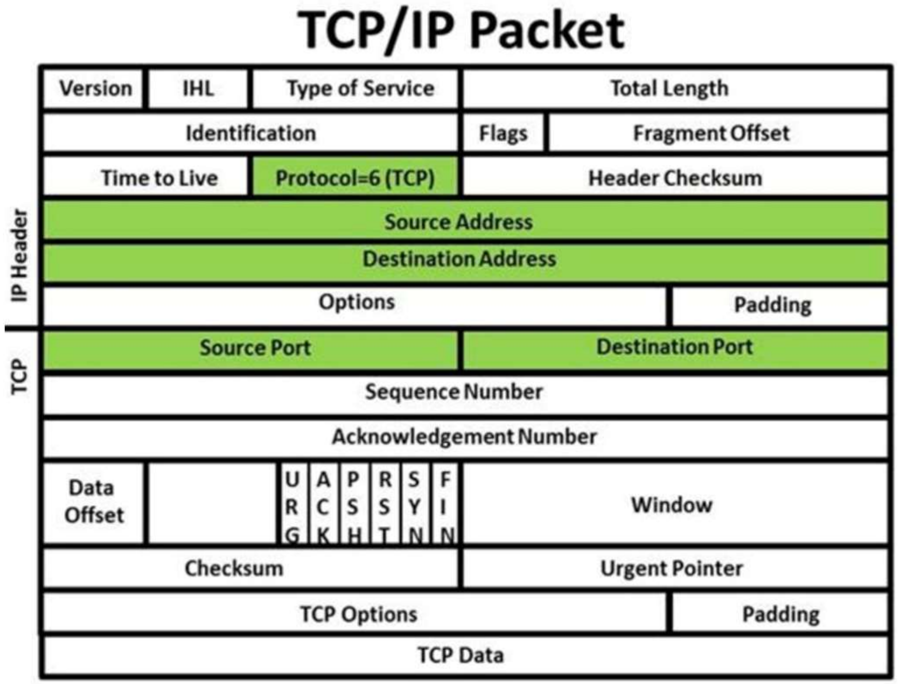
- By default, nothing
  - It needs to be configured
- Strategies:
  - Blacklisting: default is **allow**
    - *"Everything not explicitly forbidden is permitted"*
    - Less user complaints
  - Whitelisting: default is **deny**
    - *"Everything not explicitly permitted is forbidden"*
    - Increased security
    - **This is the best practice**

Roadmap

- Middleboxes
- **Firewalls**
  - **Example: packet filter on local network**
- Intrusion Detection Systems
- SIEMs

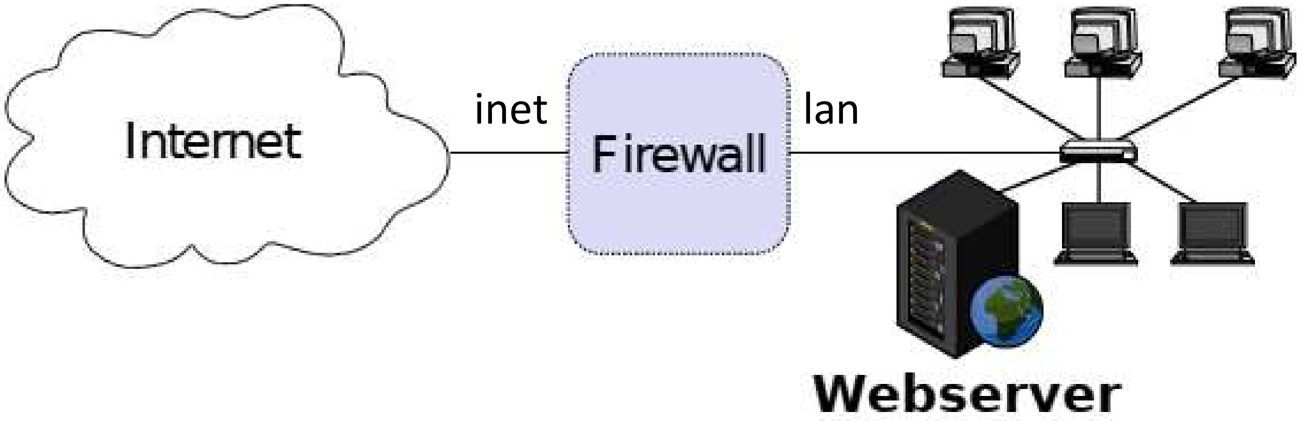
Packet filter

- Reject packets depending on the IP and transport layer headers:
  - IP addresses (origins and/or destinations)
  - Options in the IP header
  - Transport ports and protocols
  - Options in the headers of transport protocols
  - Direction in which virtual circuits are being created
  - Data sent via transport protocols
  - Type of the ICMP message
  - Datagram size
  - Network interface in which the data is sent/received



Example: small business LAN with Web Server

- Security policy
  - Allow HTTP traffic initiated by external hosts to webserver
  - Allow internal hosts to initiate HTTP and DNS
  - Do not allow other communication
    - No communication initiated by external hosts to the local hosts other than the webserver



Firewall rules table

- Example of creating rules for the firewall
- Rules are in an informal format:

Rule number

Source interface: LAN or Internet

Transport Protocol: UDP, TCP, ICMP

Destination IP address

Accept, Drop

Rule	Itf.	Source IP	Source Port	Transp. Proto.	Dest. IP	Dest. Port	State	Action
1	*	*	*	*	*	*	Establ.	

wildcard

Connection already established / New connection

Example: LAN with Web Server (1)

Rule	Itf.	Source IP	Source Port	Transp. Proto.	Dest. IP	Dest. Port	State	Action
1	*	*	*	*	*	*	Establ.	Accept

Rule 1: accept packets for already established connections

Example: LAN with Web Server (2)

Rule	Itf.	Source IP	Source Port	Transp. Proto.	Dest. IP	Dest. Port	State	Action
1	*	*	*	*	*	*	Establ.	Accept
2	inet	external	> 1023	TCP	webserver	80	New	Accept

Rule 2: Allow HTTP traffic initiated by external hosts to web server

To fill-in this rule, we needed to know that HTTP uses TCP on port 80.

The rationale for requiring source port bigger than 1023 is because system ports should not be used by regular processes.

Example: LAN with Web Server (3)

Rule	Itf.	Source IP	Source Port	Transp. Proto.	Dest. IP	Dest. Port	State	Action
1	*	*	*	*	*	*	Establ.	Accept
2	inet	external	> 1023	TCP	webserver	80	New	Accept
3	lan	internal	> 1023	TCP	external	80	New	Accept

Rule 3: Allow internal hosts to initiate HTTP requests to the outside

Example: LAN with Web Server (4)

Rule	Itf.	Source IP	Source Port	Transp. Proto.	Dest. IP	Dest. Port	State	Action
1	*	*	*	*	*	*	Establ.	Accept
2	inet	external	> 1023	TCP	webserver	80	New	Accept
3	lan	internal	> 1023	TCP	external	80	New	Accept
4	lan	internal	> 1023	UDP	external	53	New	Accept

Rule 4: Allow internal hosts to initiate DNS queries to the outside

To fill-in this rule, we needed to know that DNS uses UDP on port 53

Example: LAN with Web Server (5)

Rule	Itf.	Source IP	Source Port	Transp. Proto.	Dest. IP	Dest. Port	State	Action
1	*	*	*	*	*	*	Establ.	Accept
2	inet	external	> 1023	TCP	webserver	80	New	Accept
3	lan	internal	> 1023	TCP	external	80	New	Accept
4	lan	internal	> 1023	UDP	external	53	New	Accept
5	*	*	*	*	*	*	*	Drop

Final rule: drop all other packets

(rules are executed from top to bottom)

Complete example: LAN with Web Server

Rule	Itf.	Source IP	Source Port	Transp. Proto.	Dest. IP	Dest. Port	State	Action
1	*	*	*	*	*	*	Establ.	Accept
2	inet	external	> 1023	TCP	webserver	80	New	Accept
3	lan	internal	> 1023	TCP	external	80	New	Accept
4	lan	internal	> 1023	UDP	external	53	New	Accept
5	*	*	*	*	*	*	*	Drop

Common configuration errors 1/2

- How is your firewall management interface reachable?
  - From the Internet? From the complete internal network?
  - Via telnet? Via UPnP?

- What is allowed over the Internet?
  - NetBIOS? NFS? RPC? Telnet?
  - Other ICMP than Unreachable, Fragmentation Needed, TTL Exceeded, Ping?
  - IP header options?

Common configuration errors 2/2

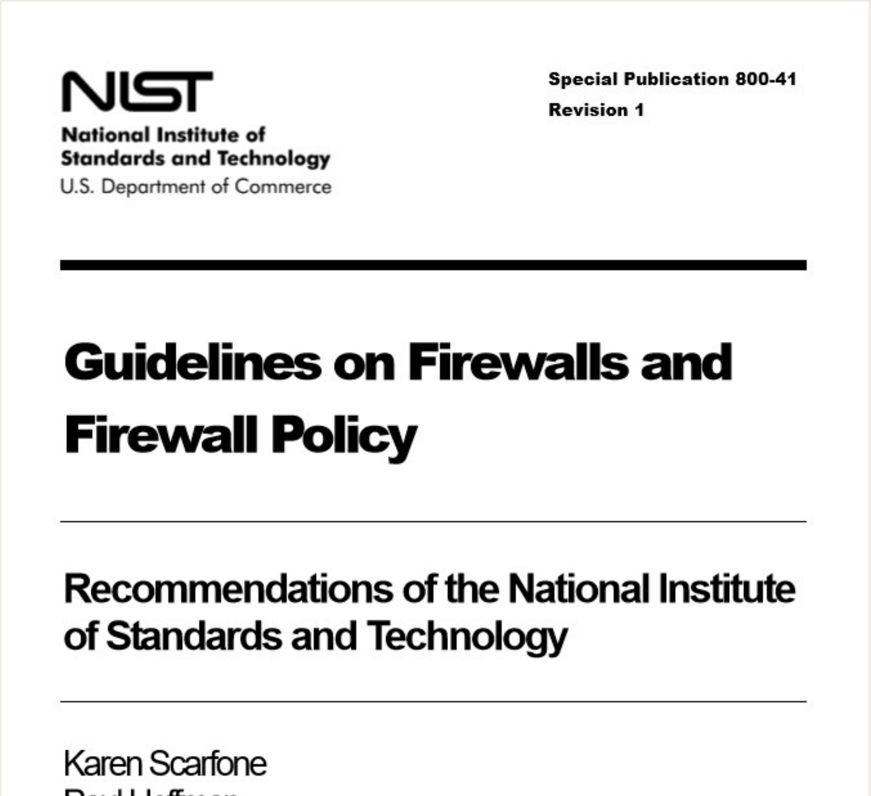
- IPv4 and IPv6?
  - Are the rule sets compliant?
- Outbound rule ANY?
  - Even private IP ranges or IP ranges that do not belong to you?
- Policy vs. Firewalls understanding of Inbound and Outbound?
  - If eth0 is your internal interface and the firewall says inbound on eth0, policy might say outbound.

Firewall rules for TCP and UDP

- Use deny by default policies for incoming TCP and UDP traffic
  - Use less stringent policies for outgoing TCP and UDP traffic
  - Most organizations permit their users to access a wide range of external applications
- Block/report malformed UDP and TCP traffic
  - Frequently used to scan for hosts
  - May also be used in certain types of attacks

Guidance for defining rules

- Defining firewall rules / policy
  - What rules should be included?
- NIST SP 800-41 document
  - Guidelines on Firewalls and Firewall Policy
  - General principles



NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Special Publication 800-41
Revision 1

Guidelines on Firewalls and Firewall Policy

Recommendations of the National Institute of Standards and Technology

Karen Scarfone

Roadmap

- Middleboxes
- **Firewalls**
  - **Types of firewall**
- Intrusion Detection Systems
- SIEMs

Firewall types

- **Packet Filter** – what we call **firewall by default**
- Circuit-Level Gateway
- Application-Level Gateway

Firewall type: Packet Filter

- Reject non-authorized interactions according to the content of the datagrams:
  - Network interface in which the data is sent/received
  - IP addresses (origins and/or destinations)
    - Options in the IP header
  - Transport ports and protocols
    - Options in the headers of transport protocols
    - Direction in which virtual circuits are being created
    - Data sent via transport protocols
  - Type of the UDP or ICMP message
    - Datagram size

Connection state

- TCP connections are explicit
  - Established with "SYN, SYN-ACK, ACK“ and ended with a "FIN, FIN-ACK, ACK"
- UDP and ICMP are connectionless
  - But a “connection” can be approximately tracked through addresses and ports of packets source and destination

Stateless vs stateful packet filters

- Packet filters can be stateful or stateless
  - **Stateful**: stores state based on packets observed; packet verification depends on the state
    - States of a connection:
      - NEW – packet for a new connection
      - ESTABLISHED – packet for a previously seen connection
  - **Stateless**: each packet is verified independently
    - No connection state is kept in memory
    - Rely on packet contents and flags

Stateless vs stateful tradeoffs

- Keeping state needs fast memory
  - Expensive
- Performance depends on the number of rules
  - Less rules leads to better performance
  - With simple policies, only a few rules are necessary
    - Stateless is usually faster
  - With complex policies, many more rules are required
    - Stateful is more expressive, and requires less rules, so it can be faster
  - Best choice for performance will depend
    - Compare and evaluate!
- Stateless firewalls typically require more rules
  - Which makes configuration errors more likely…

Circuit-Level Gateway

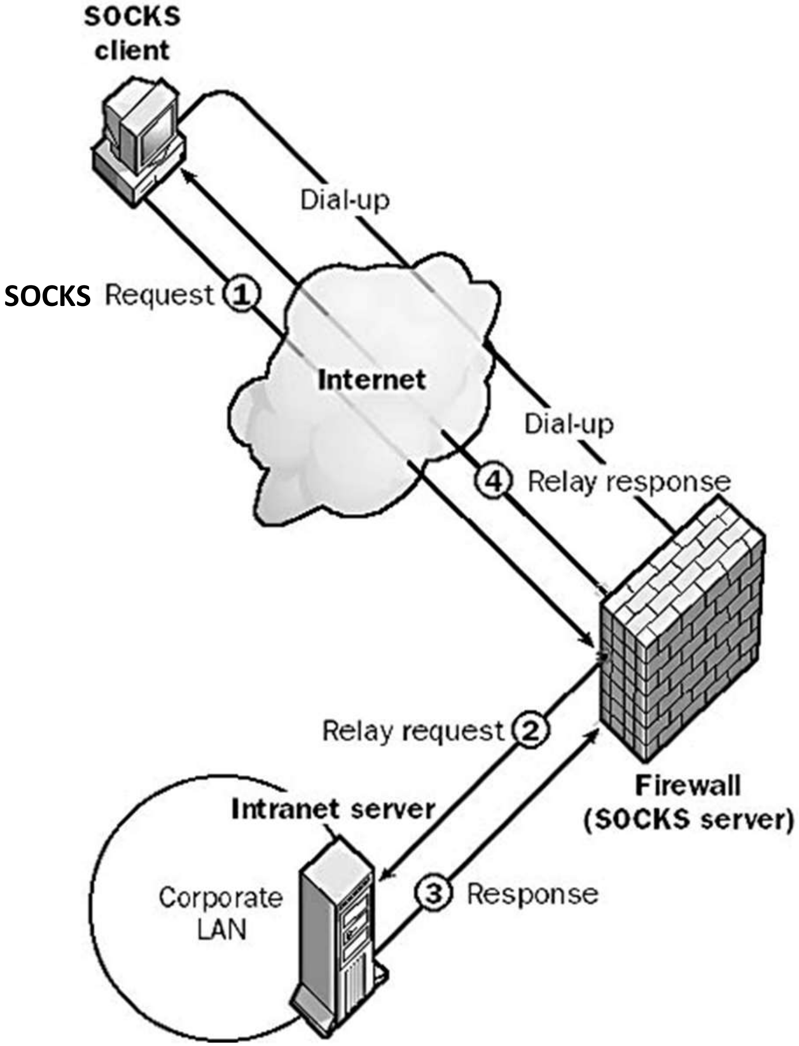
- Directly contacted by the clients at the gateway
  - Works at *transport layer* (typically TCP)
- Non-transparent interposition
  - Applications are aware of the gateway
  - Usually requires changes to the client application
    - Addition of extra redirections protocols:
      - ex. SOCKS

SOCKS

- SOCKS (**SOCK**et **S**ecure)
  - *de facto* standard for circuit gateways
  - RFC 1928 defines version 5
- Components:
  - SOCKS server
    - Often runs on a Unix-based firewall
  - SOCKS client library
    - Runs on host protected by the firewall
  - SOCKS-ified versions of client programs
    - FTP, TELNET, …

SOCKS operation

- Client opens a TCP connection to the appropriate SOCKS port on the SOCKS server
  - Typically TCP port 1080
- Client negotiates authentication method and authenticates
- Client sends a relay request
  - SOCKS server either establishes the connection or denies it



Firewall type: Application-Level Gateway

- Controls the iterations at the application layer
- Typically there is a specific proxy for each protocol
- Proxy operation characteristics:
  - User-oriented access control
  - Packet content analysis and modification
  - Detailed logging
    - Operations performed, at the application level
  - Proxying
    - Acts as an intermediary, representing other machines/services
  - Caching
    - Keep copies of frequently requested data

Summary of firewall types

- **Packet Filter** – what we call **firewall by default**
  - Reject packets depending on the IP and transport layer headers
  - Stateful vs Stateless
- Circuit-Level Gateway
  - Control iterations at the transport layer (typically TCP “circuit”)
  - Otherwise similar to Application-Level Gateways
- Application-Level Gateway
  - Control iterations at the application layer
  - Protocol-specific proxy

Comparison of firewall types

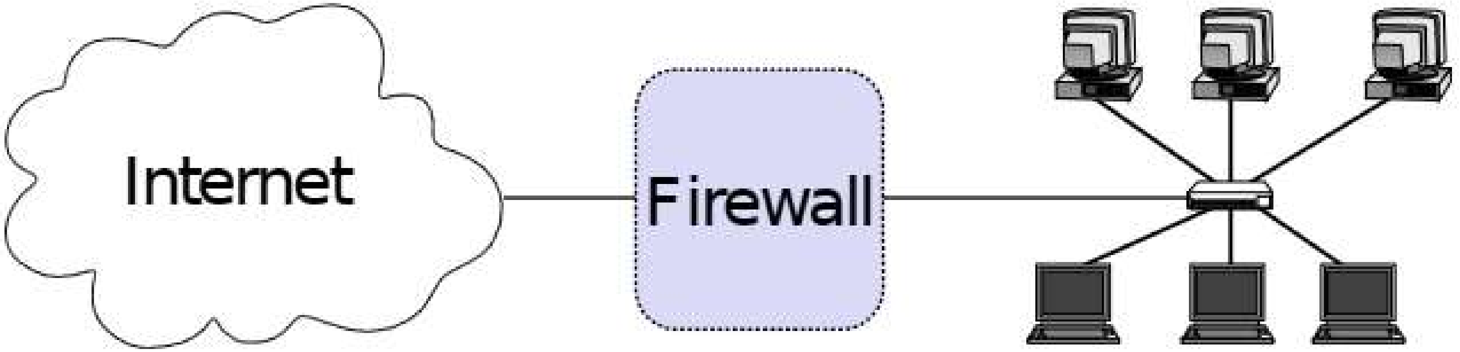
- Packet Filters
  - Faster but harder to configure
  - Unable to protect against “misbehaving” protocols
    - ex.: ftp, portmapper
  - Current/previous state is not always considered
- Application-level gateways
  - Slower but easier to configure
    - Individually for each protocol/application
  -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

Roadmap

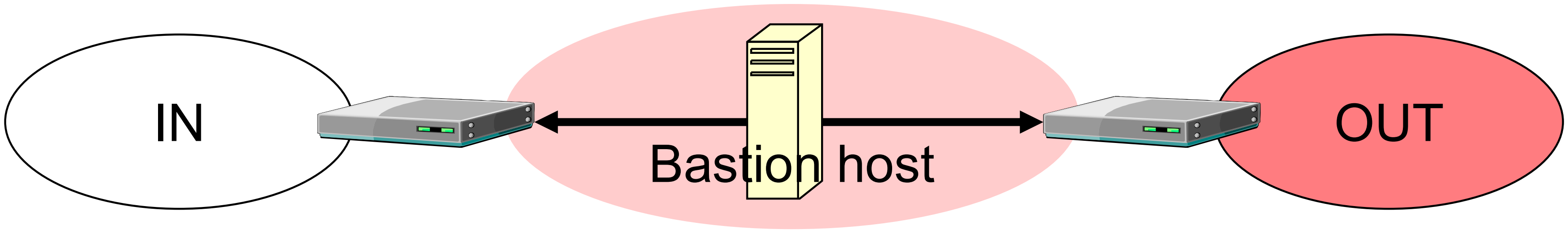
- Middleboxes
- **Firewalls**
  - **Placement (topologies)**
- Intrusion Detection Systems
- SIEMs

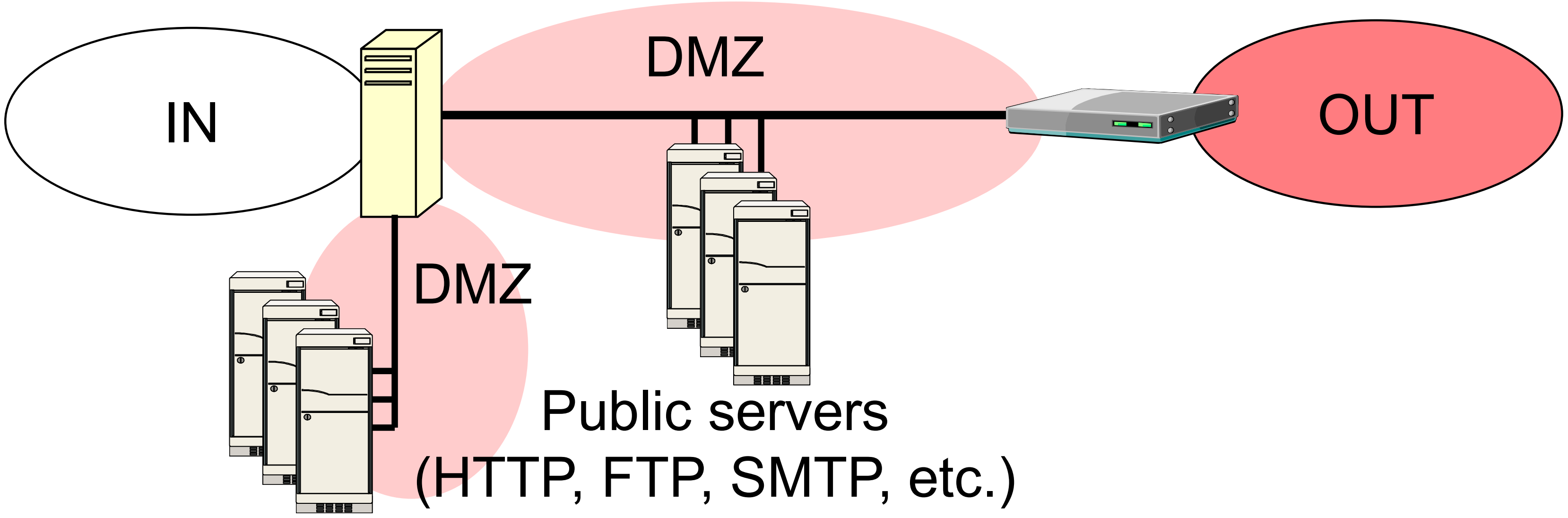
Placement of Firewalls

- Install where a protected subnetwork is connected to a less trusted network
  - If not specified otherwise, we assume Firewall is placed between Internet and local network



Firewalls: core topologies and variations





DMZ

- DeMilitarized Zone

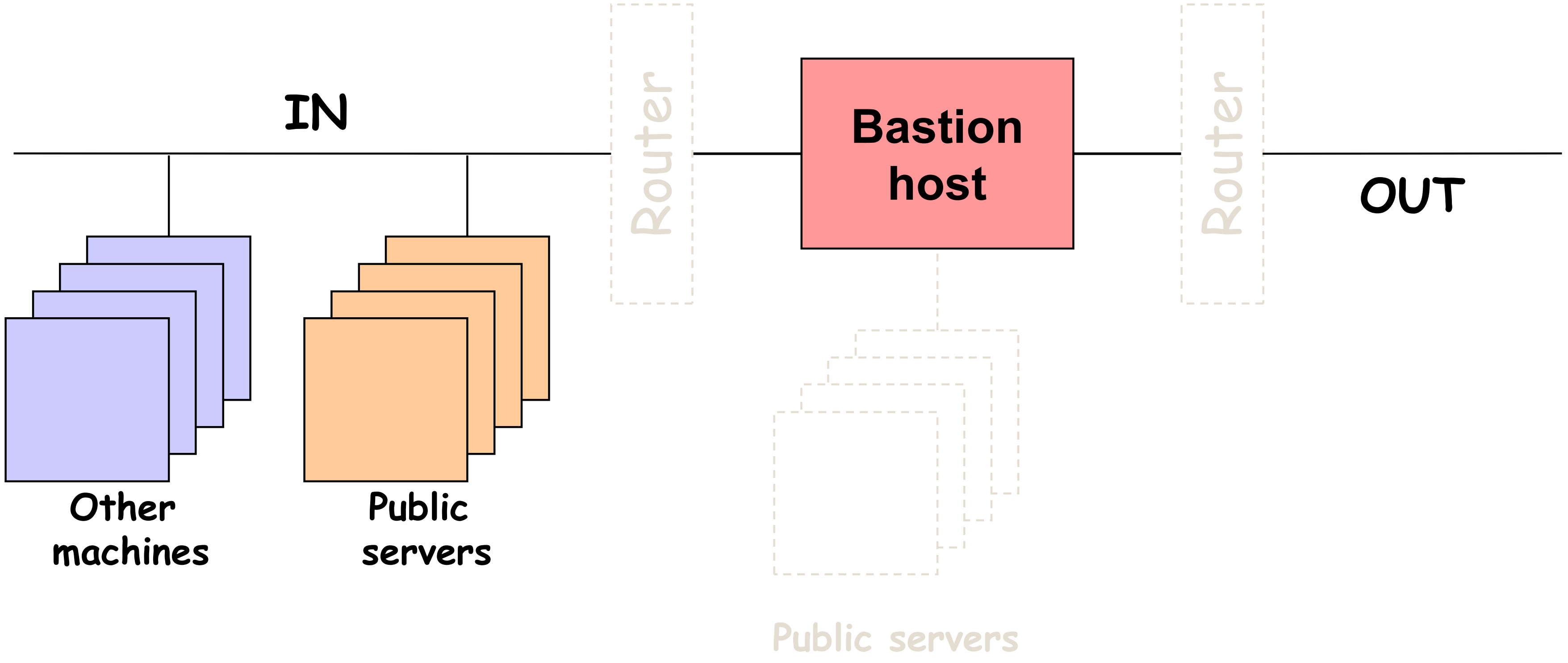
- Network Security use:
  - Not part of the protected perimeter
  - Not part of the outside because it is controlled

Firewall: core topologies

- Dual-Homed Host – Bastion Host
- Screened Host
- Screened Subnet– DMZ

Dual-homed host firewall

- Firewall / bastion has 2 home networks: IN, OUT



Core topologies:
Dual-homed host

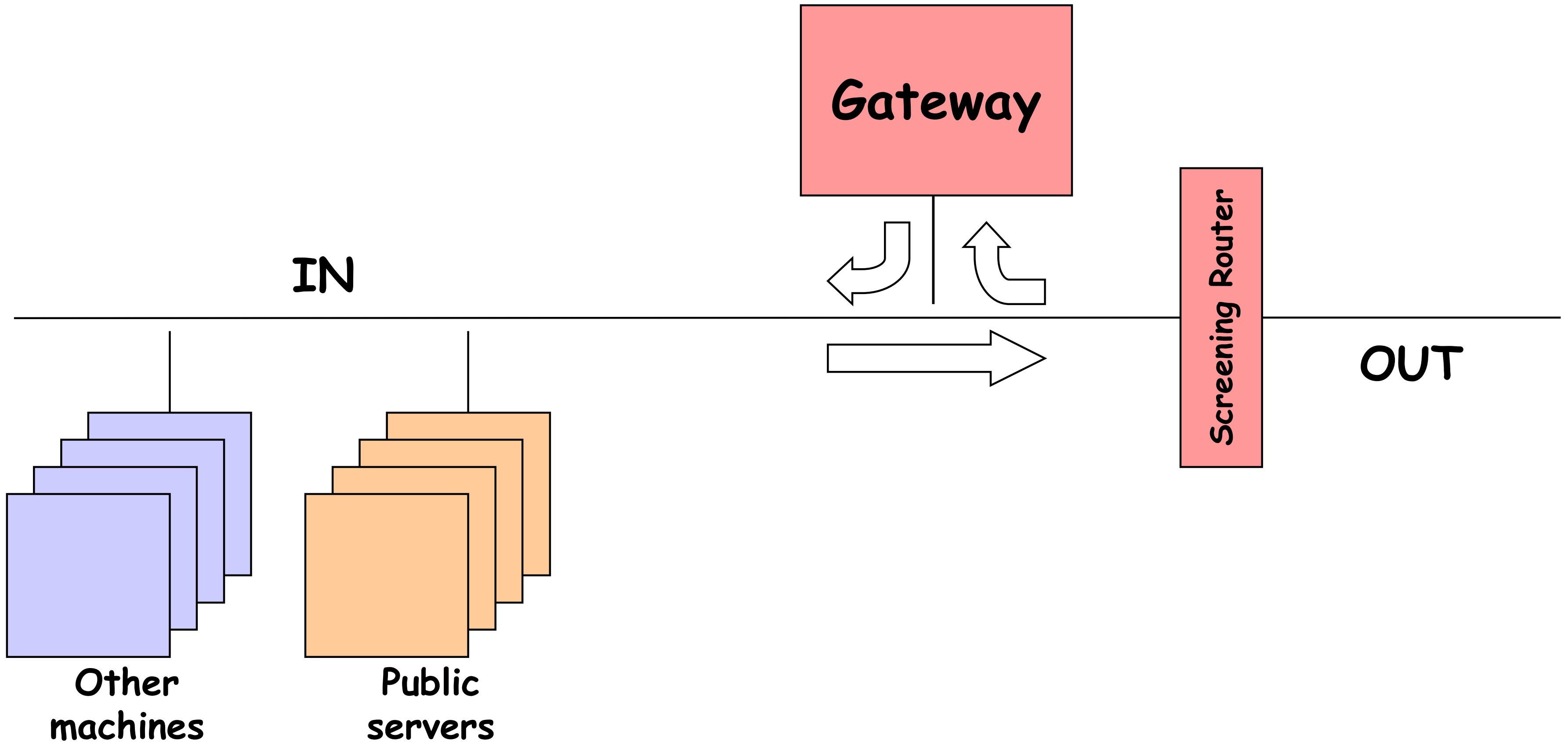
- Architecture
  - Single box (bastion host)

- Advantages
  - Simplicity and resource economy

- Disadvantages
  - Compromising the machine deactivates the firewall
  - All the processing load of the firewall in a single machine
  - Public servers are within the protected network

Screened host firewall

- Screening router – a router that works as a firewall
  - Gateway in the figure is optional

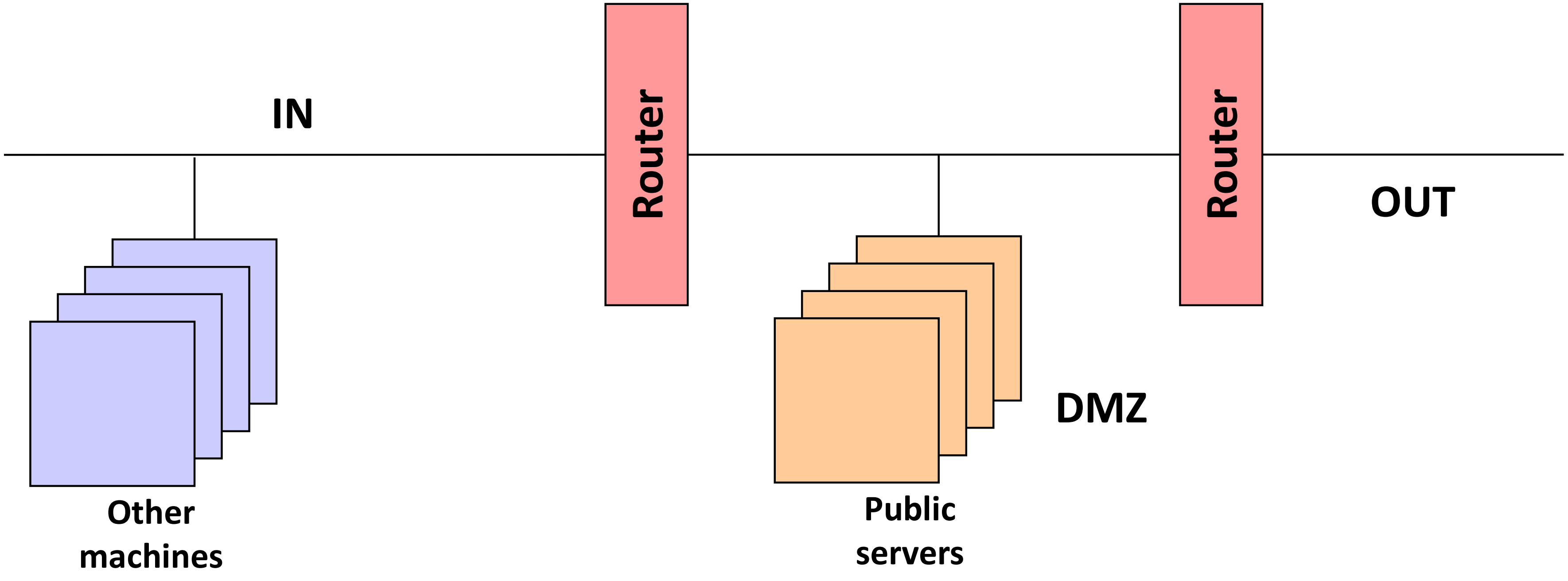


Core topologies: Screened host

- Operation with gateway
  - Router sends all *out →in data flow* to the gateway
    - Gateway has a fine-grained control over that data flow
    - Gateways forwards authorized data to the internal nodes
  - All the *in →out data flow* is filtered by the router
    - Optionally goes through gateway (e.g., for trusted connections)
- Advantages
  - Balances workload between the router and the gateway
- Disadvantages
  - Public services are within the protected network

Screened subnet

- Two internal subnets: IN and DMZ
  - Routers are packet filters

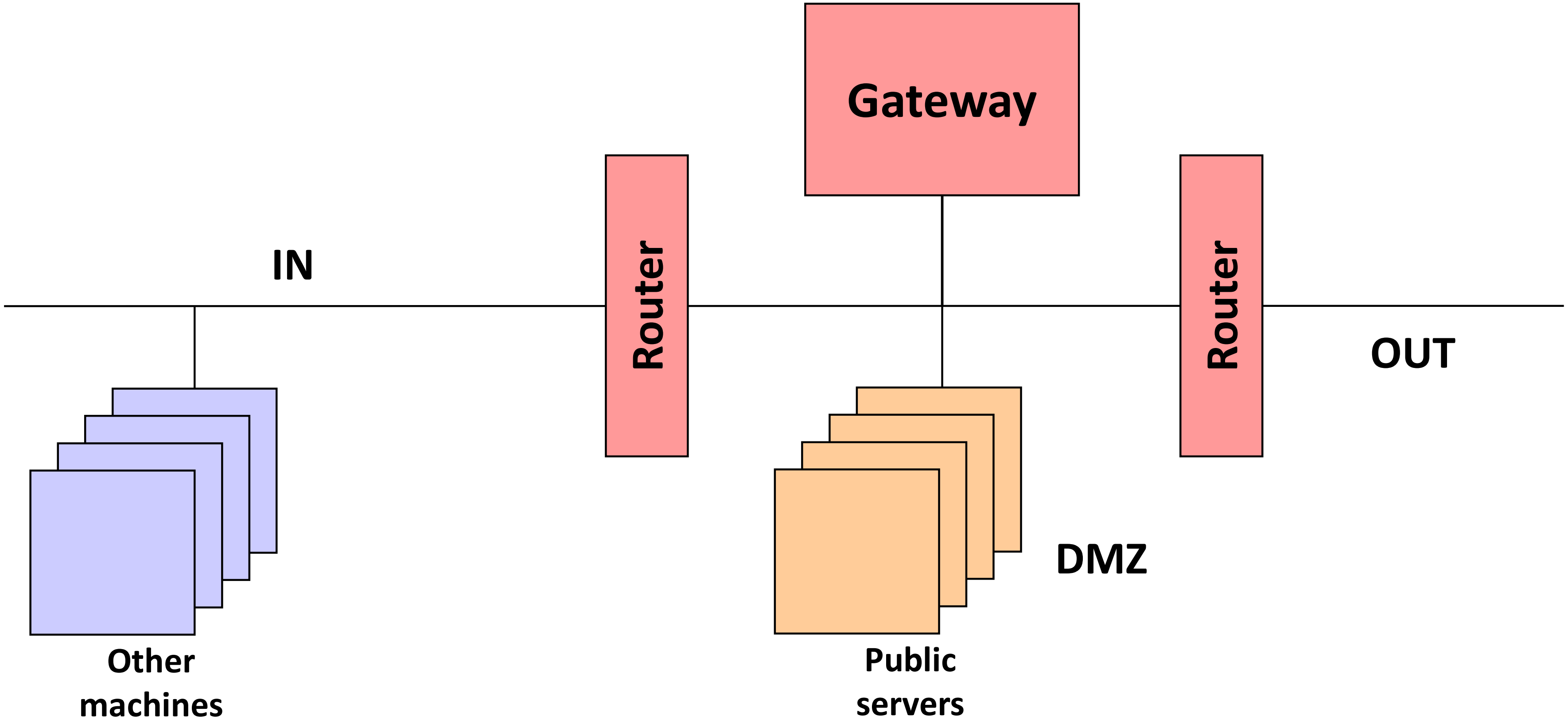


Core topologies:
Screened subnet

- Architecture
  - 2 routers, 1 DMZ
  - The public services are placed in the DMZ
- Advantages
  - Lower risk regarding the public services
  - Lower risk regarding a firewall being compromised
- Disadvantages
  - Lower control over the activities going on in the DMZ machines

Screened subnet (v2)

- Optional architecture w/ single-homed gateway (application-level or circuit-level)



Roadmap

- Middleboxes
- **Firewalls**
  - **iptables**
- Intrusion Detection Systems
- SIEMs

Firewall implementation on Linux

iptables / netfilter

- **netfilter** – a packet filtering framework for Linux
  - module of the Linux kernel that supports packet filtering, NAT,…

- **iptables** – program that configures netfilter’s rules

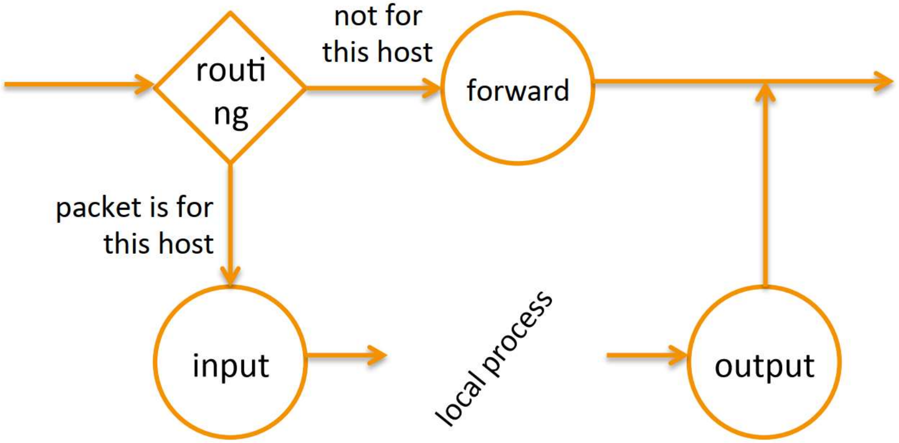
- 3 important concepts:
  - Tables
  - Chains
  - Rules

Tables contain Chains

Chains contain Rules

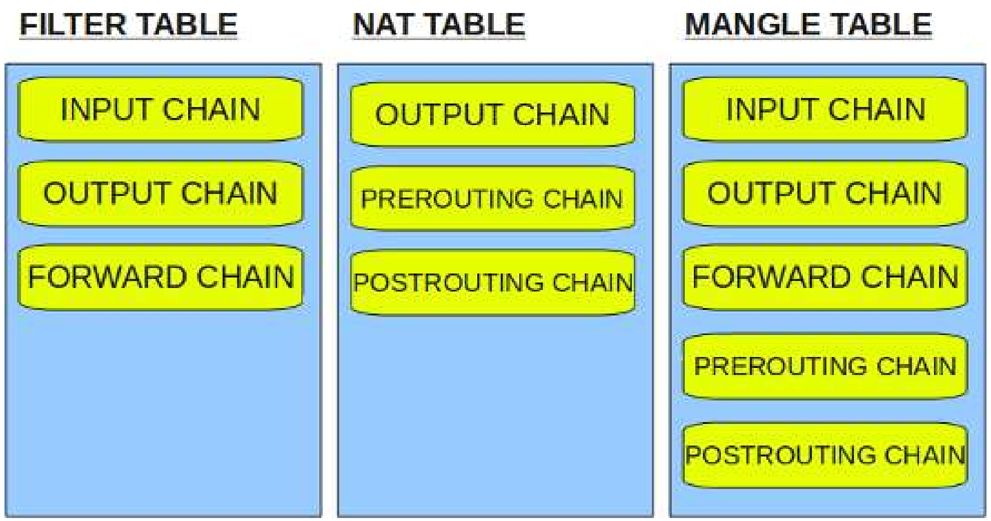
iptables

- **Filter table** has 3 chains (lists of rules): *input, output, forward*
  - When a packet reaches a chain, the chain's rules decide the packet's fate: drop (throw it away) or accept (continue)
    - Input – applied to incoming packet destined to the host
    - Output – applied to packet sent by a process at the host
    - Forward – applied to incoming packet to be forwarded

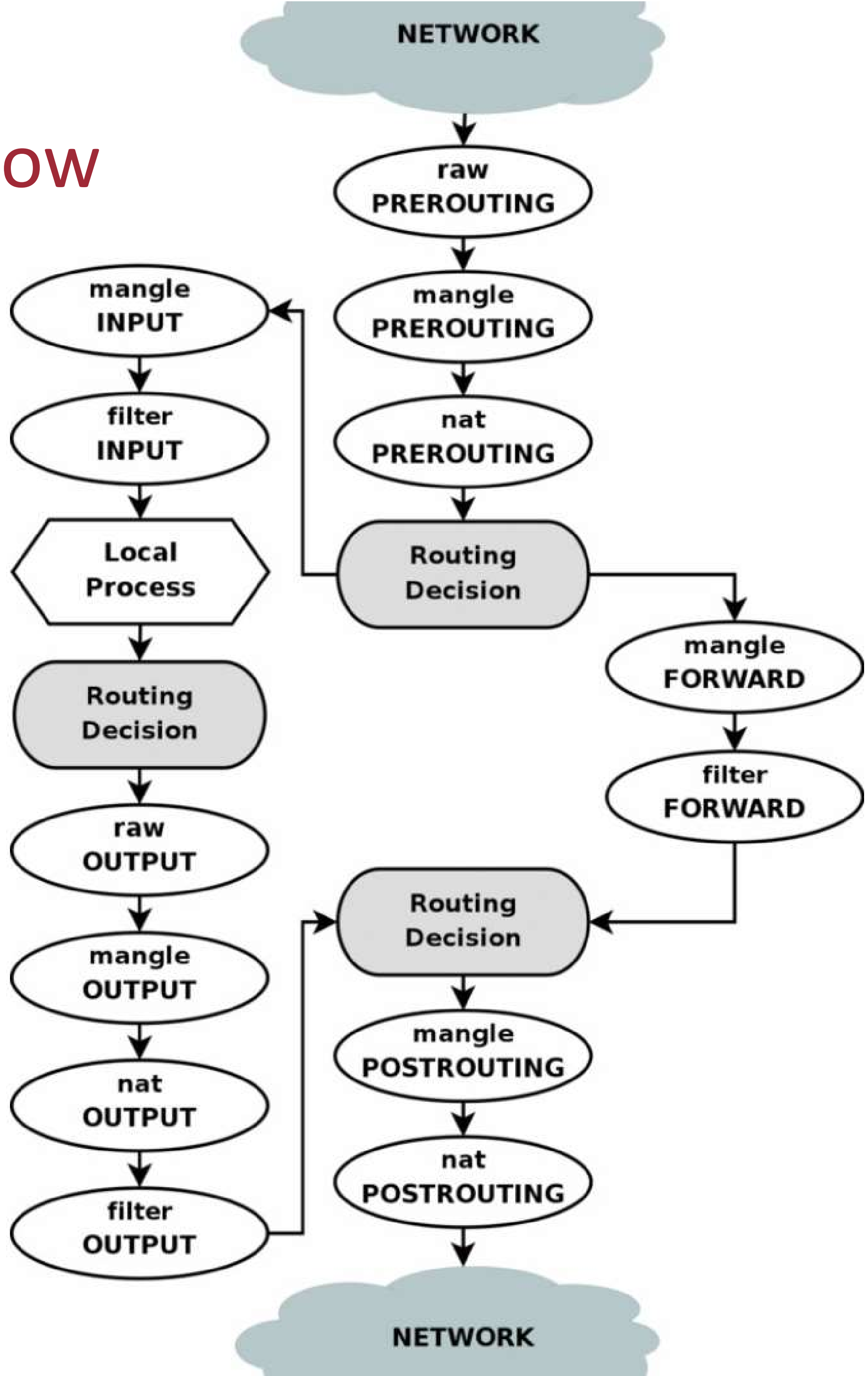


Iptables' tables and chains

- Tables:
  - **Filter** – (the only one) used for packet filtering
  - NAT – used to implement NAT rules
  - Mangle – used to modify packets arbitrarily



Overview of packet flow on iptables chains



iptables – a simple rule

- Command to drop ICMP packets from 10.0.0.1 passing through this host (default is *accept*):
- iptables -A FORWARD -s 10.0.0.1 -p icmp -j DROP
  - append (-A) to chain FORWARD a rule that says that:
  - packets from source (-s) 10.0.0.1
  - with protocol (-p) ICMP
  - should be dropped (-j DROP)

- Packets to be filtered are specified using -s and -p but there is more
- *man iptables* for more info

Roadmap

- Middleboxes
- **Firewalls**
  - **Open issues**
- Intrusion Detection Systems
- SIEMs

Open issues with firewalls

- Attacks can come in through the IP/ports the firewall does not close
  - e.g., currently many attacks come through port 80 (HTTP) that is almost always open
  - IP spoofing: firewall cannot know if packet really comes from claimed source
  - If multiple applications need special treatment, each one has to have its own gateway
  - Tradeoff: degree of communication with outside world, level of security

Open issues with firewalls (cont.)

- The firewall cannot protect against attacks that bypass it
  - Dial-up link, wireless, cellular router,…
- The firewall does not protect against insider threats / authorized users
  - A laptop, tablet, smartphone, or portable storage device may be used and infected outside the corporate network, and then attached and used internally
    - This is the BYOD (Bring Your Own Device) security problem

Roadmap

- Middleboxes
- Firewalls
- **Intrusion Detection Systems**
- SIEMs

IDS definitions

- Intrusion (or attack)
  - 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

Motivation for IDS

- All systems have vulnerabilities
  - Known or unknown
  - Can be used to carry out attacks
- Attacks can be detected by:
  - Becoming 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 preliminary phases (probes)
  - Attack accesses from the outside
  - Attacks from the inside

IDS complement firewalls

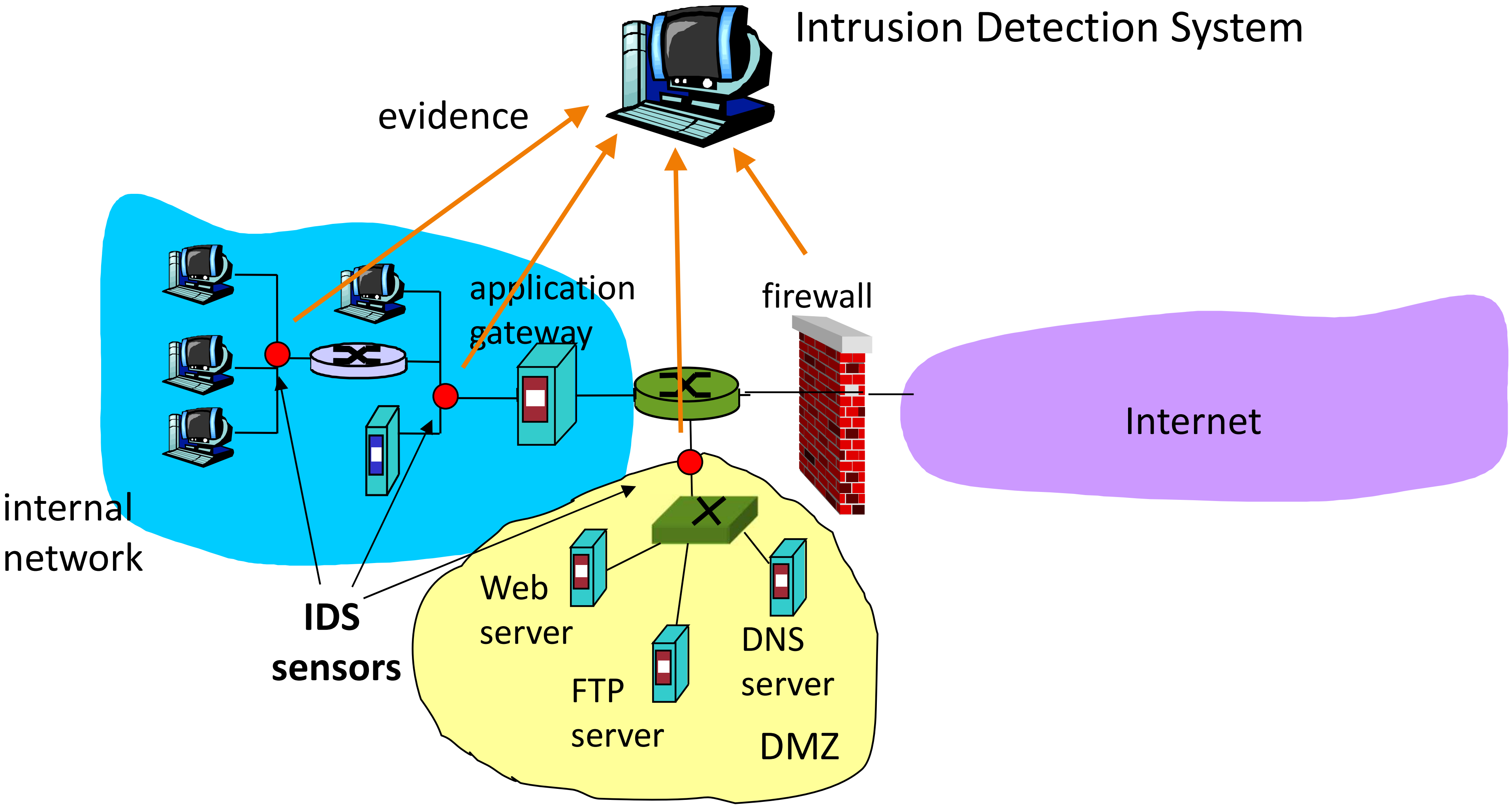
- *Firewalls (packet filters)*
  - Operate on TCP/UDP/IP/ICMP headers only +
  - Do not do correlation among packets or sessions

- *Intrusion Detection Systems (IDSs)*
  - **Deep packet inspection (DPI)**
    - Look at packet contents
      - e.g., check character strings in packet against database of known virus, attack strings
  - **Examine correlation among multiple packets**
    - Can detect attacks like port scanning, network mapping, DDoS
    - Not only network-based but also host-based

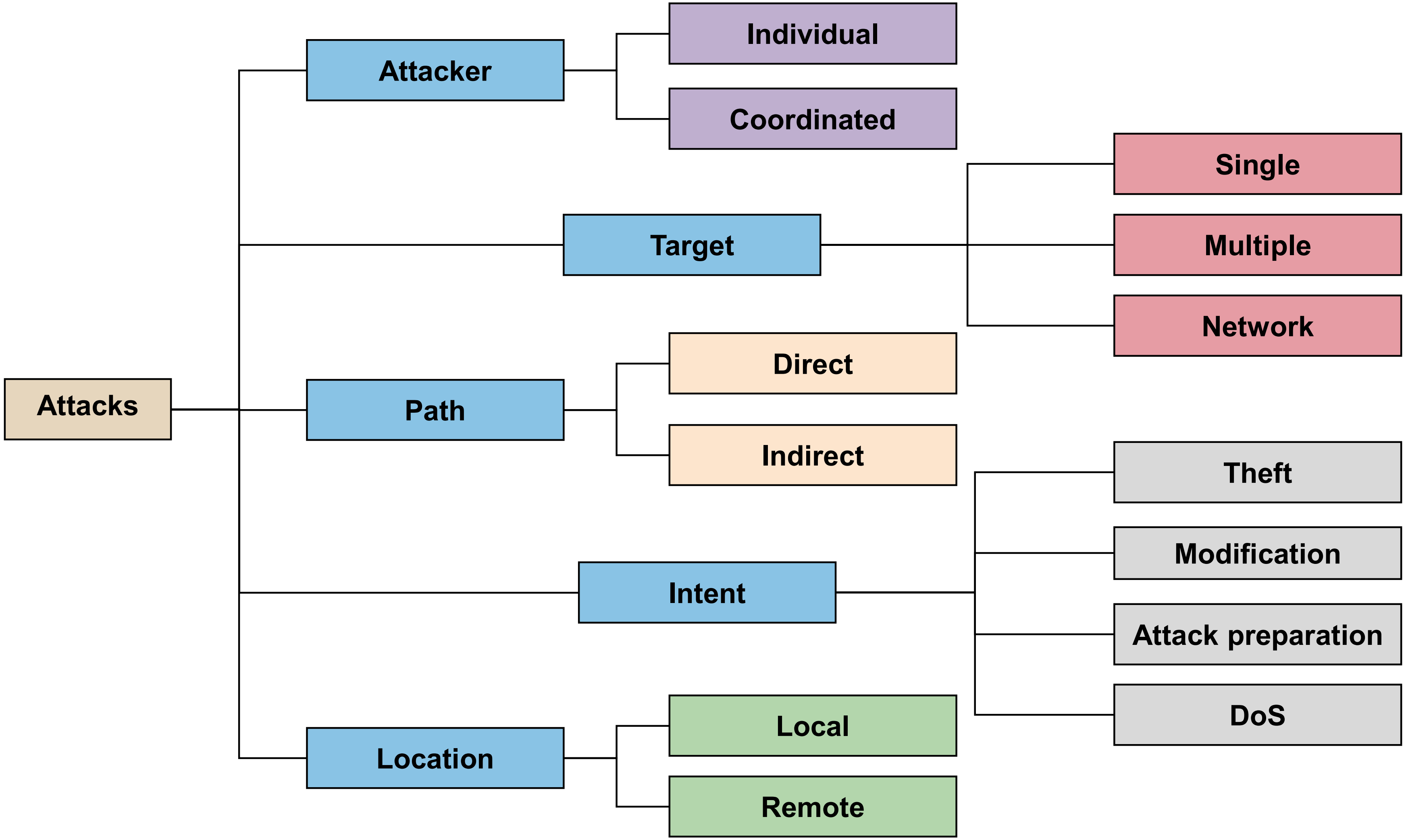
Intrusion detection – Why ?

- When prevention does not work
  - Detecting intrusion access (external ones)
  - Detecting intrusion preambles (probes)
  - Detecting abusive behaviors (internal ones)
    - Particularly effective in these cases
    - Given the more relaxed preventive measures for the internal users
      - e.g.: malicious staff, email, 802.11b, laptops and mobile devices, …
  - Gather intrusion information for later use
  - To document existing threats for the organization
  - Verify the effectiveness of the prevention mechanisms

Intrusion detection – How ?



Attack classification



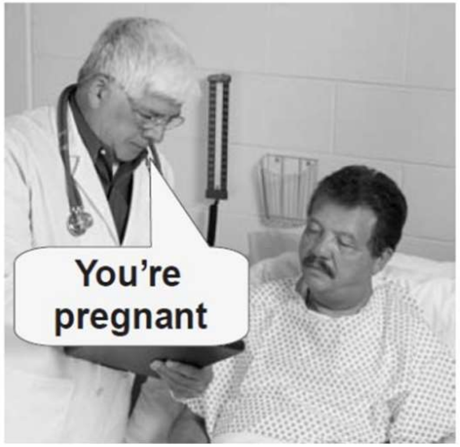
Attack detection

- IDSs generate alarms
- There are detection errors
  - False positive (false alarm)
  - False negative (missing alarm)
    - Tradeoff: configuring the IDS for less false negatives usually leads to more false positives
    - False positives also very bad in practice
  - Can be used for subversion
    - E.g. change IDS behavior by forcing too many alarms
- Correlation
  - Detecting patterns in sets of atomic events
    - Requires temporary storage of state
- Data merging
  - Uniformly analyzing events from heterogeneous sources

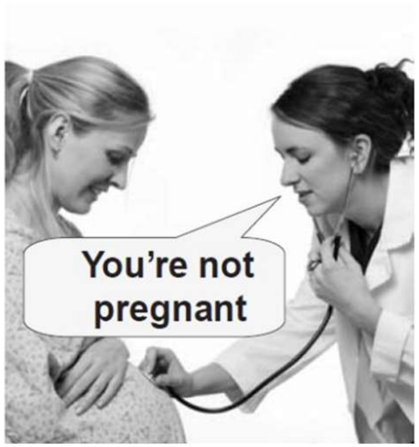
True/False Positive/Negative

- True/false
  - First word indicates the **reality**
- Positive/negative
  - Second word indicates the **prediction**

(false positive)



(false negative)



Honeypots

- Vulnerable system created for **deception**
- Focus attacker's attention on an apparently weaker and valuable system:
  - Deflect the attack from the real system
  - Detect and learn about new attacks
  - Gather forensic information
- Example implementation:
  - https://opencanary.org
- Problem?
  - Can be used as an attack origin

IDS classification

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

IDS classification

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

Misuse Detection / Knowledge-based Detection

- System activity analysis in search of known attack patterns (attack signatures)
  - A match raises an alarm

- Advantages:
  - Efficient detection
  - Reduced amount of false positives
- Disadvantages:
  - Only detects known attacks
    - Useless with unknown attacks
  - May generate a large amount of false negatives

Anomaly Detection / Behavior-based Detection

- Matches observed behavior with a model of normal behavior
  - Using statistical heuristics (thresholds) or Machine Learning
  - No match raises an alarm
    - *“this is not normal…”*
- Advantages:
  - Able to detect new attacks
  - Can be used to collect data to define new attack signatures
- Disadvantages:
  - Needs a large amount of training data without attacks
    - If training set contains attacks, they are considered “normal”
  - Difficult to define adequate threshold values
    - Large amount of false positives

IDS classification

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

NIDS: Network-Based IDS

- Capture and do traffic analysis on network data (e.g., packets)

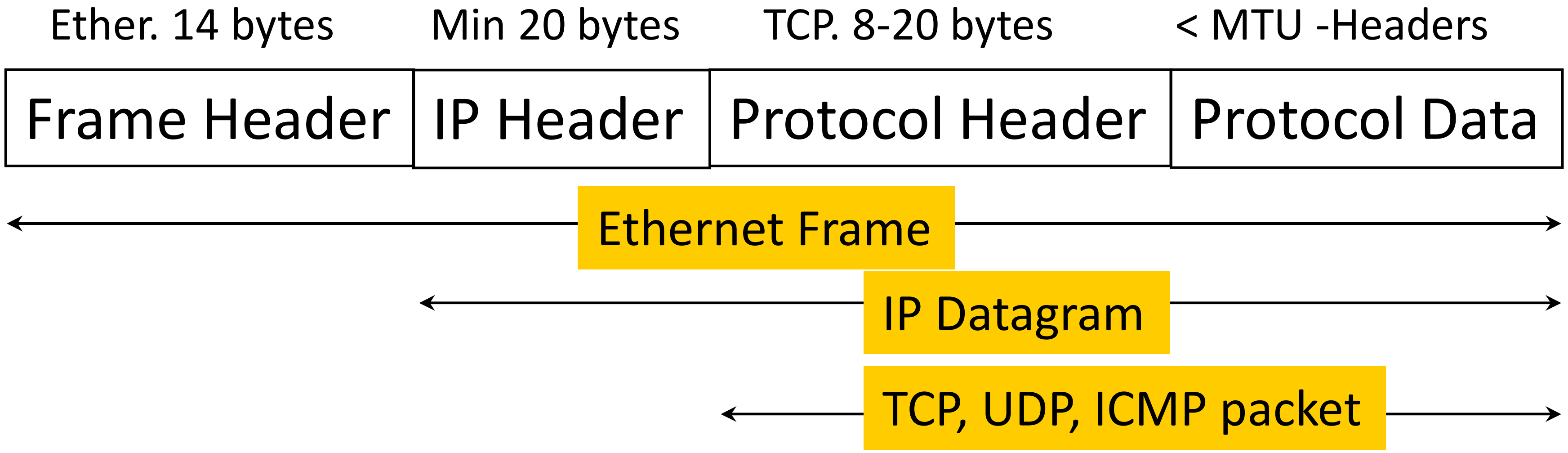
- Advantages:
  - Small amount of sensors can monitor a large network
  - Little to no impact in the network performance
  - Can be invisible to attackers
- Disadvantages:
  - Hard to process large amounts of data flowing through the network
  - Difficult to install in networks that are not shared
  - 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
- Brute-force attacks, e.g., to get passwords
- Abuse of bandwidth resources
- Denial of Services (DoS)
  - Improperly formatted packets
  - Abnormally high data/packet flow
  - Distributed DoS

NIDS – Attack signature

- Packet content
  - More powerful
  - Ineffective in ciphered channels
- Packet header
  - Less powerful
  - Not affected by ciphered contents



NIDS example: SNORT

- Misuse detection (has signatures)
- SNORT can be used as a:
  - Packet sniffer - live analysis
  - Packet logger - *a posteriori* analysis
- Advantages
  - Open-source
  - Stable
  - Flexible - allows custom rules
  - There is an active community
    - Keeping attack signatures up-to-date
  - Also a company – SourceFire
    - provides rules immediately for subscribers, and free after 30 days

https://www.snort.org/

HIDS: Host-Based IDS

- Capture and do analysis on host data
  - Can look at processes running in the computer, their CPU and memory usage, I/O behavior, etc.; look at logs, registry, etc.

- Advantages:
  - Able to observe/detect attacks that cannot be seen by a NIDS
  - Able to function in environments with ciphered data
  - Not affected by network isolation (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 (external) staff
- User account usurpation:
  - Old employees
  - Created by misbehaving administrators
- Inadvertently assigned privileges
- Access and modification of critical information
  - Browsing critical information
  - Modification of configuration files
  - Modification of Web site
- Information leakage

HIDS example: OSSEC

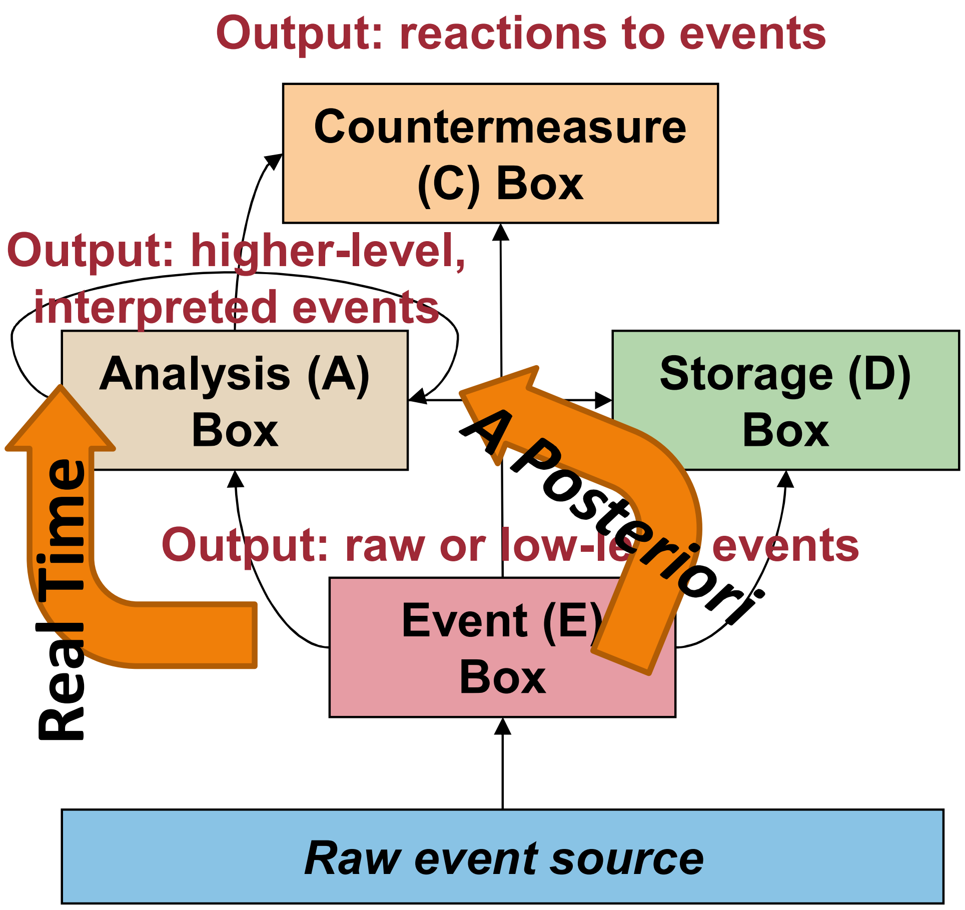
- OSSEC has:
  - Correlation and analysis engine
  - Log analysis
  - File integrity checking
  - Centralized policy enforcement
  - Rootkit detection
  - Alerting
  - Active response – e.g. black list IP addresses
  - Optional web-based graphical monitoring interface
- Advantages
  - Open-source
  -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

https://ossec.github.io/

IDS classification

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

Functional architecture



- Event Box
  - Sensors that capture events
- Analysis Box
  - Performs analysis of low-level events and generates higher-level events
- Data Box
  - Information storage module
- Countermeasure Box
  - Reaction modules: execution of predetermined actions / methods as a response to events

Based on the Common Intrusion Detection Framework (CIDF), an old IETF proposal for IDS interoperability

IDS classification

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

How to react to attacks?

- Passive
  - Only detect and report the detection results:
    - Alarms and notifications
    - Logging and report creation
- Active
  - Respond to the attacks:
    - Close connections: TCP RST
    - Perform system/operational modifications
    - Reconfiguration of routers/firewalls, etc.
  - Counterstrike
    - Typically, illegal
    - Be careful not to start a cyberwar…
- Active IDSs also known as:
  intrusion prevention systems (IPSs) or
  intrusion detection and prevention systems (IDPSs)

Attack reaction

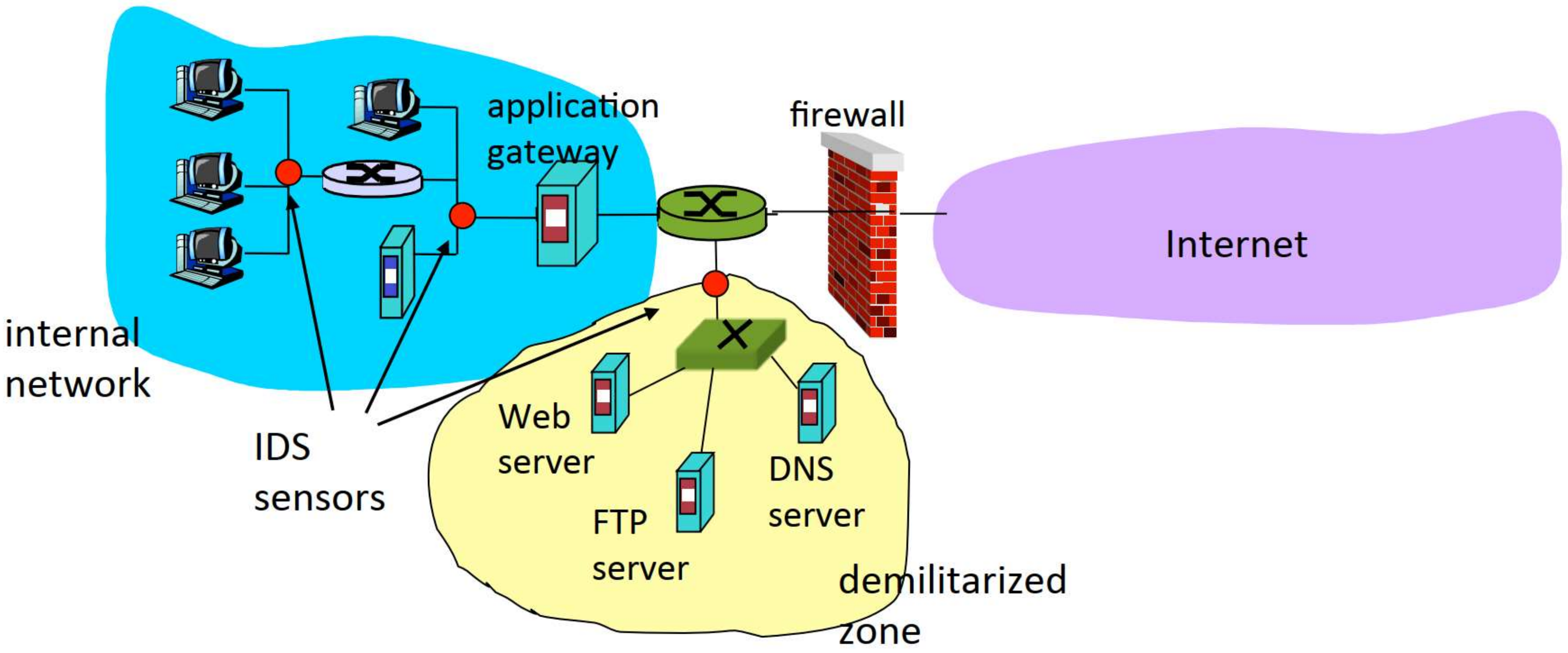
- Block malicious traffic
  - Closer to firewalls, but with deep packet inspection and correlation
  - Blocking mechanisms
  - Ending TCP connections
  - Dropping packets (like packet filters)
  - Throttling bandwidth usage
  - Sanitizing traffic (e.g., dropping malicious mail attachment)
  - Reconfiguring other network devices (firewalls, routers,…)
  - Running third-party program or script
- False positives are even more dangerous in this case
  - The reaction might be intentionally caused by the attacker
    - e.g., mislead you to block a range of IPs

IDS classification

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

Cooperative IDS

- Not necessarily centralized as a firewall
  - Multiple IDSs: different types of checking at different locations



IDS classification

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

Roadmap

- Middleboxes
- Firewalls
- Intrusion Detection Systems
- **SIEMs**

SIEM

- Security Information and Event Management
  - SIEMs are security management platforms
  - SIEMS are cooperative IDSs with storage capacity
  - Many are commercial products from major vendors
    - Symantec, McAfee, IBM, EMC-RSA, …
  - Others are open
    - OSSIM
    - But, with more complete version commercialized AlienVault, now AT&T Cybersecurity

SIEM main objectives

- Detect attacks and intrusions on the whole infrastructure of the organization
- Collect audit logs for security and compliance
- Provide evidence to conduct forensic investigations

Security Operations Center (SOC)

- SOC – organizational unit that manages security, i.e., that does SecOps (security operations)
  - Composed of systems and people
  - Major cybersecurity component is a **SIEM**

Context enrichment

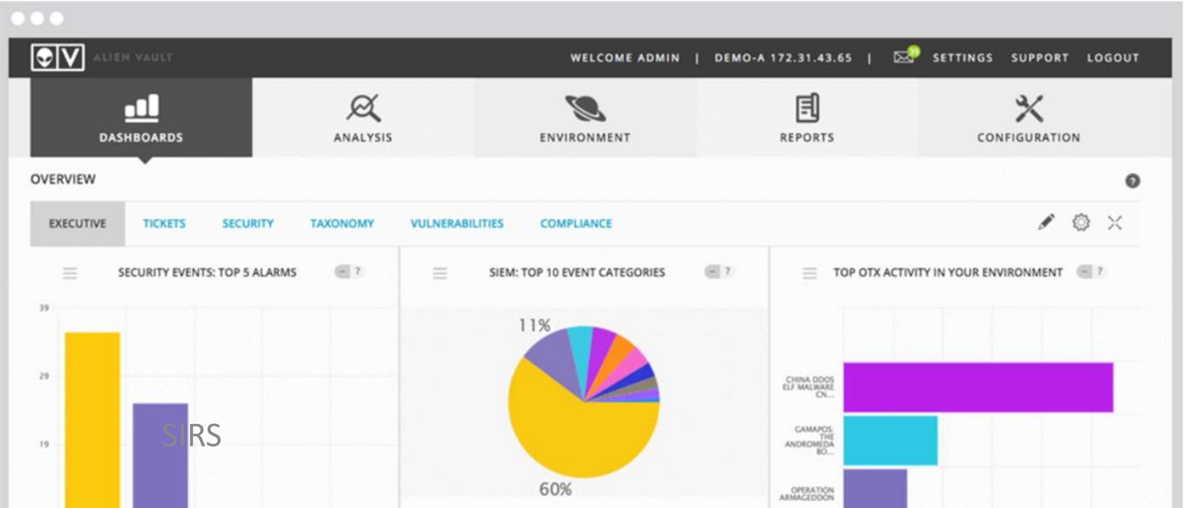
- Data shall be added with context to help using it for security analysis
- Examples of context
  - Geo-location data (e.g. country of origin)
  - DNS and WHOIS data
  - User details (name, job title, location, etc.)

SIEM main features (1)

- Log/event collection
  - Important metric: Events generated Per Second (EPS)
- User activity monitoring
  - Allow identifying which user did what
  - Important form: Privileged User Monitoring and Audit (PUMA)
- Reporting
  - Real-time event correlation
  - Data aggregation/correlation from several sensors+logs
- Log retention
  - Long term archival in a normalized format
  - Should be tamper proof and have time stamps

SIEM main features (2)

- IT compliance reports
  - – Ability to generate reports for that purpose; example formats: GDPR (EU), PCI DSS, FISMA, HIPAA, SOX,… (standards/US laws)
- File integrity monitoring
  - – Track and report changes to files (e.g., OS files in servers)
- Log forensics
  - – Tools to support investigation and collection of proofs related to a certain event, possibly to present in court of justice
- Dashboard – graphical interface
  - – Alarms, charts,…


ALIEN VAULT
WELCOME ADMIN | DEMO-A 172.31.43.65 |
SETTINGS
SUPPORT
LOGOUT
DASHBOARDS
ANALYSIS
ENVIRONMENT
REPORTS
CONFIGURATION
OVERVIEW
EXECUTIVE
TICKETS
SECURITY
TAXONOMY
VULNERABILITIES
COMPLIANCE
SECURITY EVENTS: TOP 5 ALARMS
39
29
19
SIEM: TOP 10 EVENT CATEGORIES
11%
60%
TOP OTX ACTIVITY IN YOUR ENVIRONMENT
CHINA DDOS ELF MALWARE CN…
GAMAPOS: THE ANDROMEDA BO…
OPERATION ARMAGEDDON

Summary

- Middleboxes
- Firewalls
- Intrusion Detection Systems
- SIEMs

Conclusion

- Firewalls and IDS are important security mechanisms that can enforce security policies
  - Firewalls control accesses
  - IDS monitor activities
  - Both can and should be combined
  - Several configurations and solutions exist
- SIEMs are the authoritative security information repository for many organizations