Fundamentos de Segurança Informática

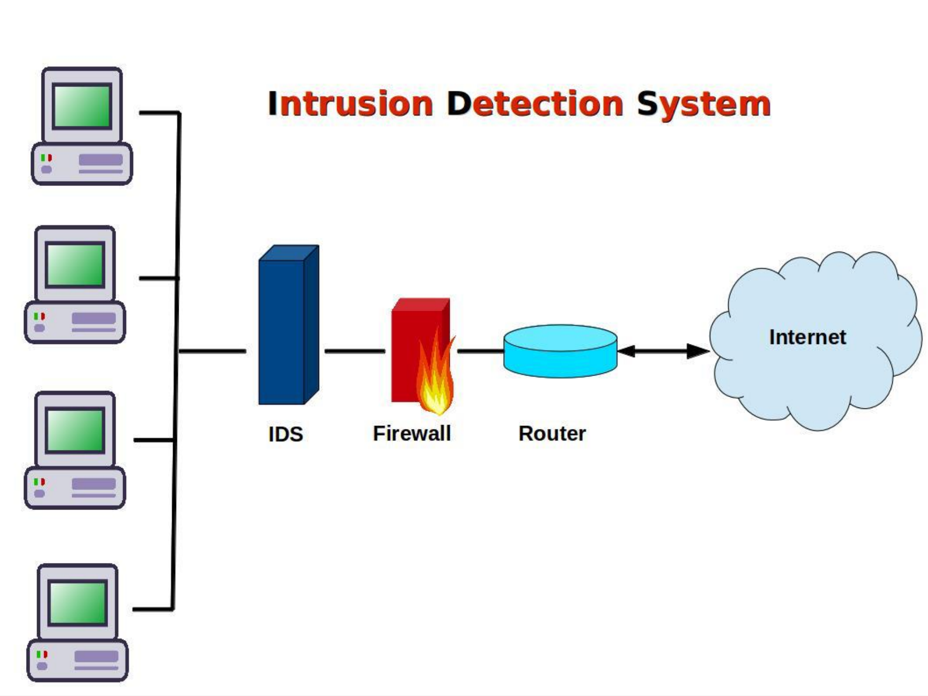
LEI

2025/2026

T2 – Access Control: Firewalls and Intrusion detection

Access control

- Firewalls
- Intrusion detection systems



Access control policies and mechanisms

- Access Policy
  - ✓ One of the main goals of the Security Policy
  - ✓ Defined before implementing Access Control mechanisms
- Access Control
  - ✓ Implements and enforces the Access Policy
  - ✓ Usually implemented side-by-side with authentication
- Access Control mechanisms
  - ✓ Physical Barriers
    - Walls, doors, closets, etc.
  - ✓ Logical Barriers
    - Permissions, access rules, etc.
  - ✓ Firewalls

Usual elements in Access Control

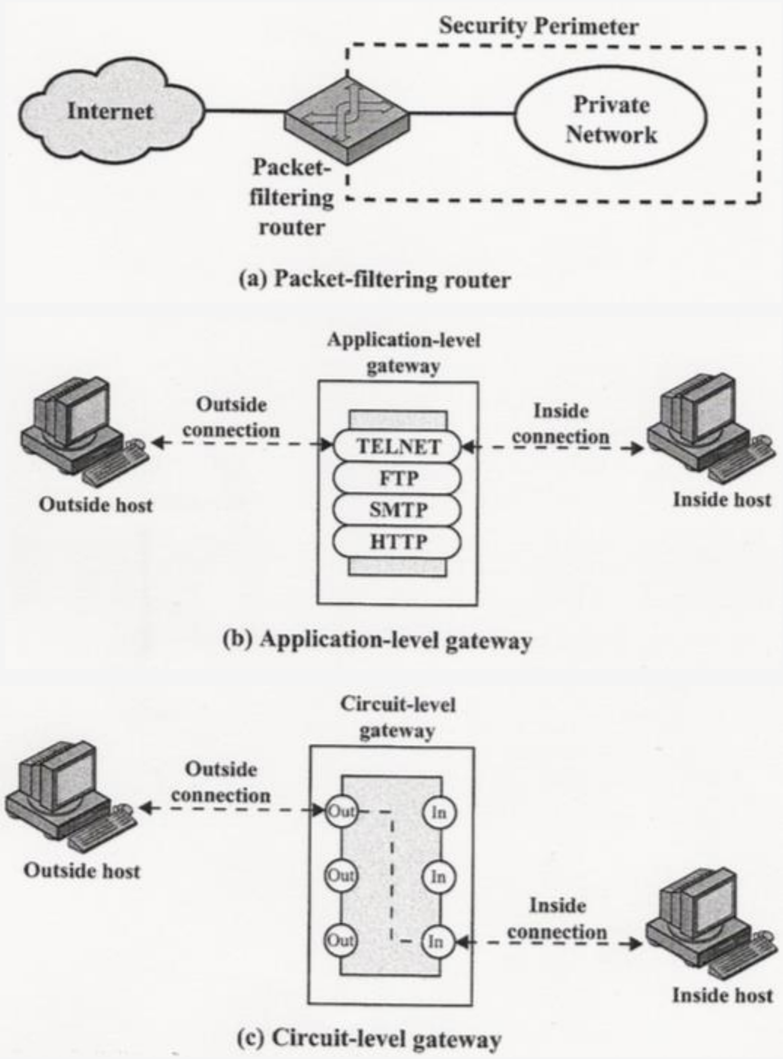
- Network Traffic direction:
  - Input or Output
- Service:
  - HTTP, FTP, SMTP, etc.
- Host:
  - Origin or destination
- User:
  - Identification, role, etc.
- Time:
  - Hour of the day, day of the week, month, etc.
- Type of connection:
  - Public or private
- Quality of Service (QoS):
  - Throughput, delay, etc.

Firewalls

- A **system** or **group of systems** that enforces an access policy
- Firewall usage scenarios
  - Internet access
  - Remote access (via 3G/4G, Wi-Fi, ..)
  - Connections with networks of related organizations (clients, partners, ..)
- Controlling the "Security Perimeter"
  - Accesses to services
    - By IP address, destination or source port, ..
  - Controlling network traffic direction
    - Input and output
  - Controlling users
    - Local, remote users
  - Controlling behaviour
    - Content of applications, application-layer attacks, ..

Types of Firewalls

- Packet filters (static, dynamic)
- Application-level gateways
- Circuit-level gateways



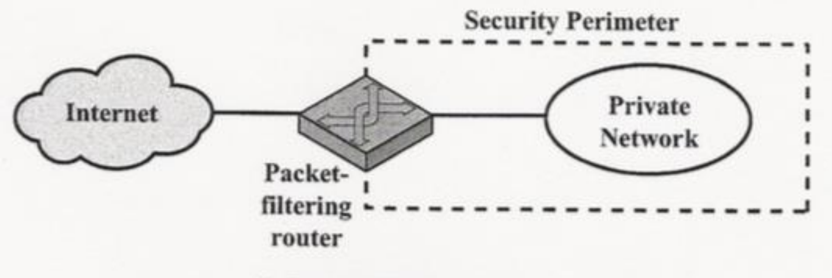
(a) Packet-filtering router

(b) Application-level gateway

(c) Circuit-level gateway

Types of Firewalls: Packet filters

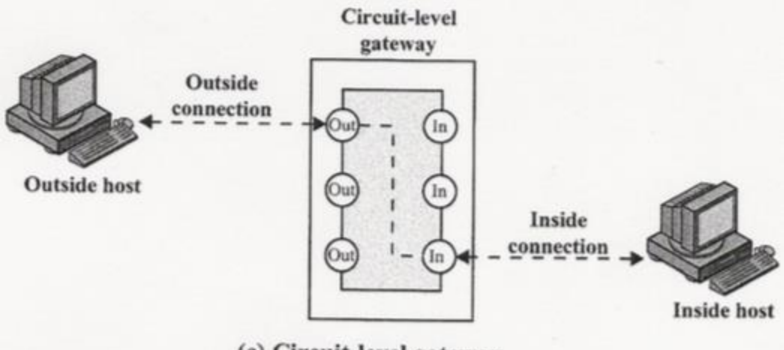
- Operate at the network level
  - ✓ Usually implemented in a router
  - ✓ Using Access Control Lists (Cisco ACL, Linux IPTables, IPFW, ..)
- Filtering rules are built based on:
  - ✓ Origin IP address
  - ✓ Transport protocol (UDP, TCP)
  - ✓ Origin and destination port
  - ✓ Optionally using NAT (Network Address Translation)
- Packet filtering strategies
  - ✓ Static filtering
  - ✓ Dynamic filtering (support of services that use dynamic ports)



(a) Packet-filtering router

Types of Firewalls: Circuit-level gateways

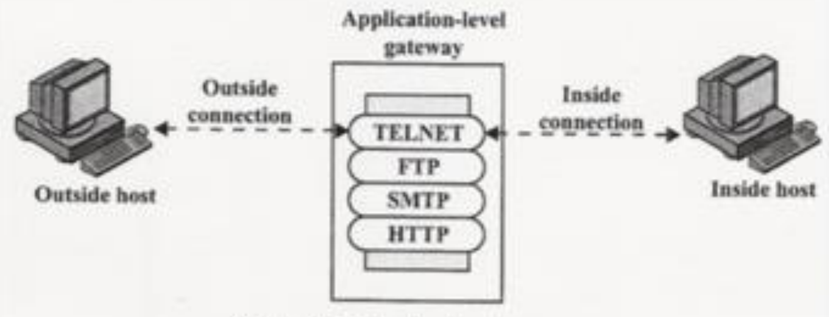
- Operate at the transport level (example: SOCKS, RFC 1928)
- Operation:
  - ✓ Intercepts UDP or TCP communications
  - ✓ Verify user permissions
  - ✓ Establish new TCP or UDP communications with the requested destination
  - ✓ Concatenate the two connections
- Usage
  - ✓ Internet access by hosts with private IP addresses
  - ✓ Support “real-time” network traffic for applications unable to use application-level proxies



(c) Circuit-level gateway

Types of Firewalls: Application-level gateways

- Operate at the application level
- Examples: "SQUID" for HTTP, "ftpgw" for FTP, "TIS" for Telnet, ..
- Operation:
  - ✓ Application proxies
  - ✓ Serve requests from applications according to user permissions
  - ✓ Forward information between clients and remote servers
  - ✓ May cache requests
- Usage
  - ✓ Internet access by hosts using private IP addresses
  - ✓ Promote resource (e.g. bandwidth) usage



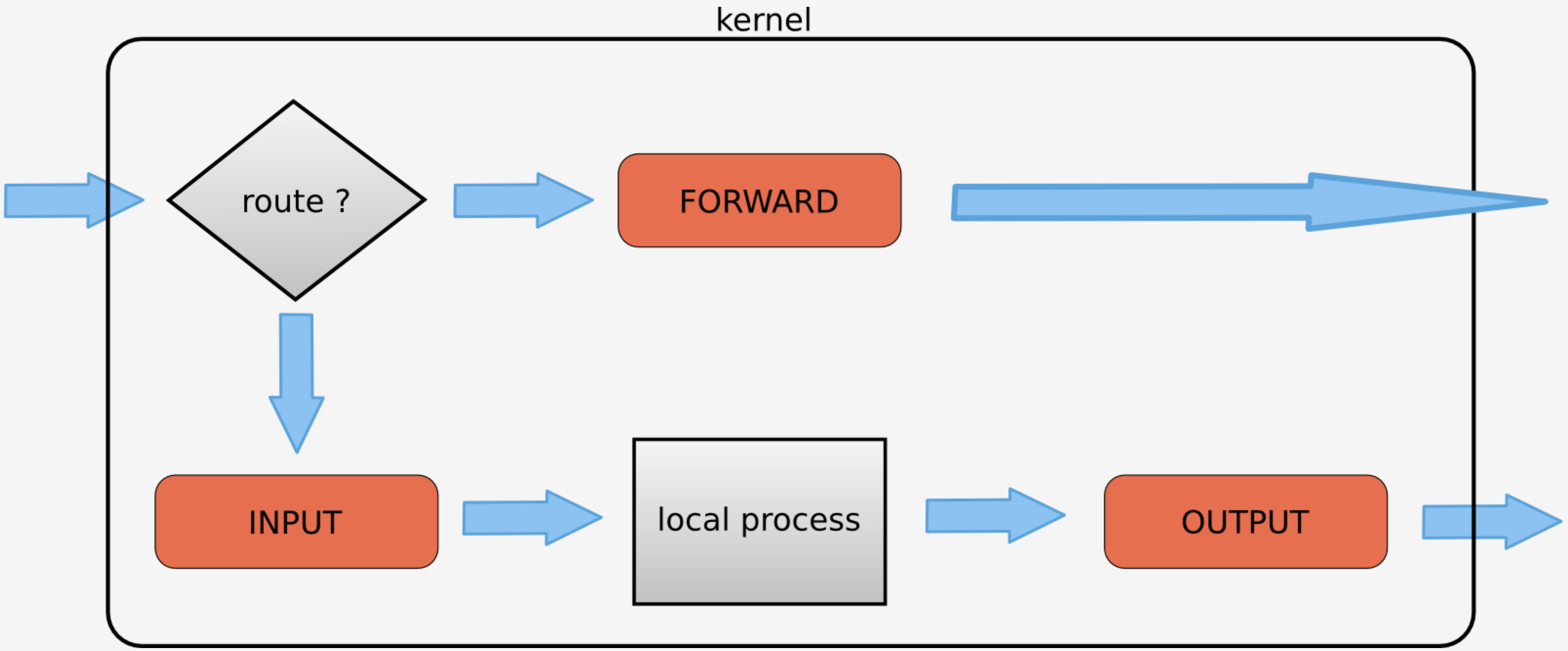
(b) Application-level gateway

Packet filtering in Linux using IPTables/NetFilter

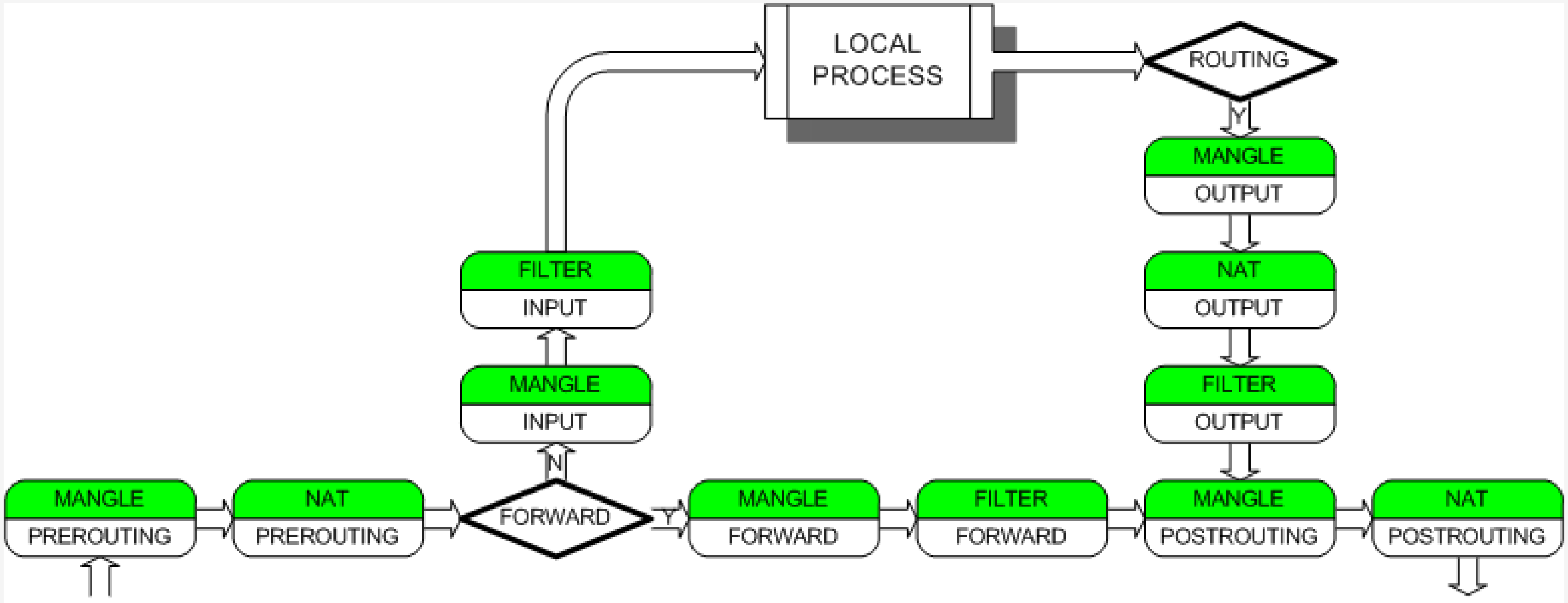
- Allows filtering of IP packets in well defined processing stages of the Linux Kernel
- Processing stages are defined as **chains,** available in **tables**

Table	Chain	Usage
filter	INPUT	IP packets entering the system
	OUTPUT	IP packets leaving the system
	FORWARD	IP packets forwarded by the system
nat	PREROUTING	Modify IP packets entering the system (before routing)
	OUTPUT	Modify IP packets created by local applications
	POSTROUTING	Modify IP packets before they leave the system
mangle	INPUT	Alter the IP header of the packet entering the system
	OUTPUT	Alter the IP header of the packet leaving the system
	FORWARD	Alter the IP header of the packet forwarded by the system
	PREROUTING	Alter the IP header of the packet entering the system (before routing)
	POSTROUITING	Alter the IP header of the packet leaving the system

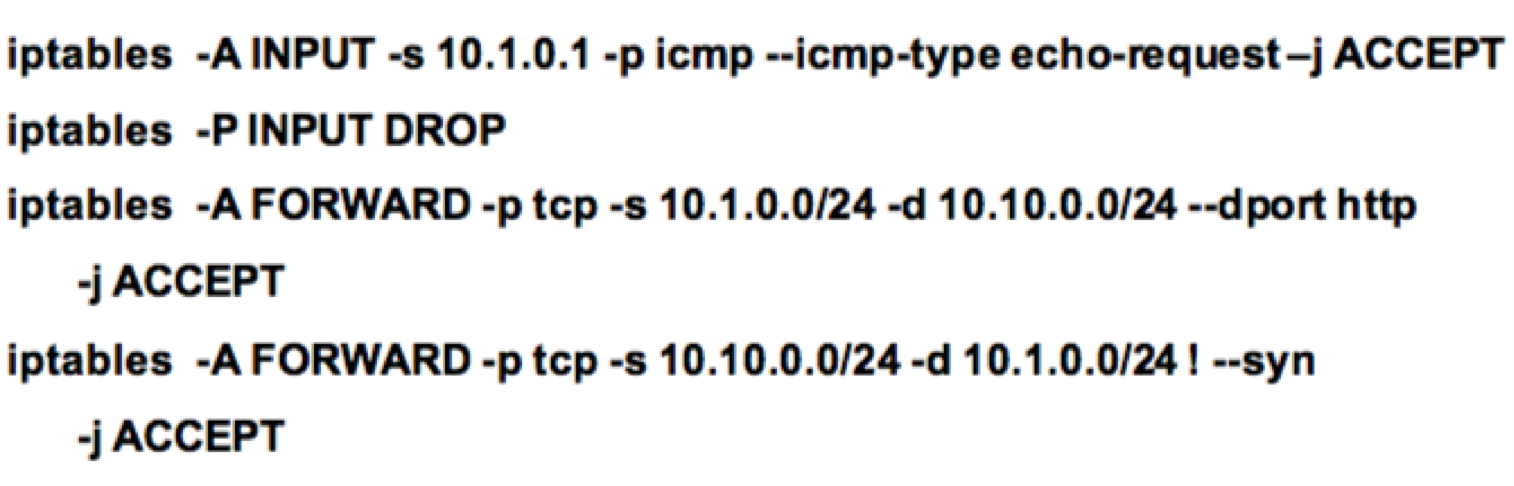
Using IPTables (with the “filter” table)



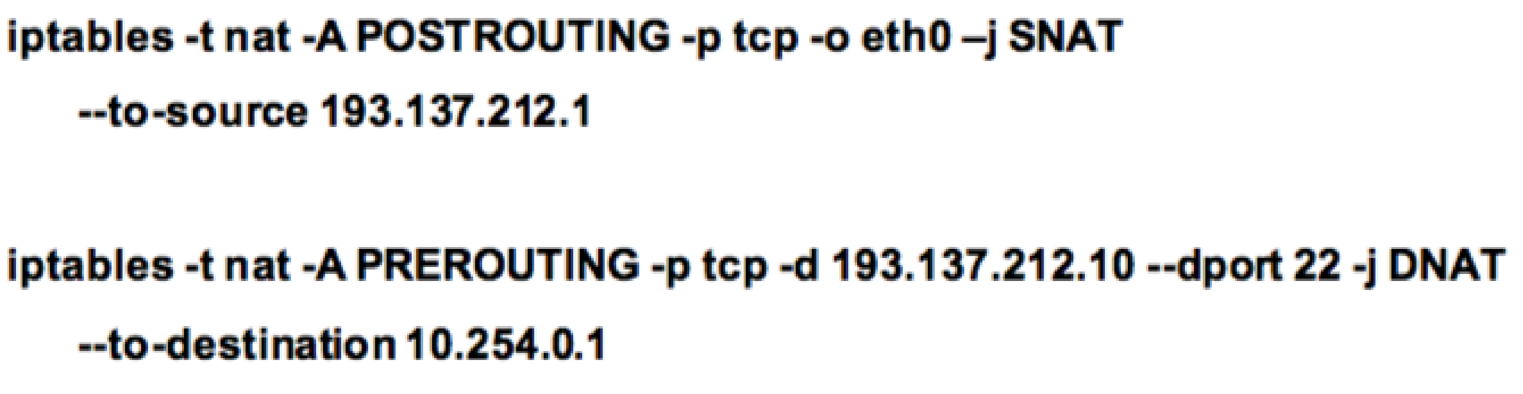
Using IPTables (“filter”, “nat” and “mangle” table)



Defining IPTables rules (examples)



```
iptables  -A INPUT -s 10.1.0.1 -p icmp --icmp-type echo-request –j ACCEPT
iptables  -P INPUT DROP
iptables  -A FORWARD -p tcp -s 10.1.0.0/24 -d 10.10.0.0/24 --dport http
    -j ACCEPT
iptables  -A FORWARD -p tcp -s 10.10.0.0/24 -d 10.1.0.0/24 ! --syn
    -j ACCEPT
```



```
iptables -t nat -A POSTROUTING -p tcp -o eth0 –j SNAT
    --to-source 193.137.212.1


iptables -t nat -A PREROUTING -p tcp -d 193.137.212.10 --dport 22 -j DNAT
    --to-destination 10.254.0.1
```

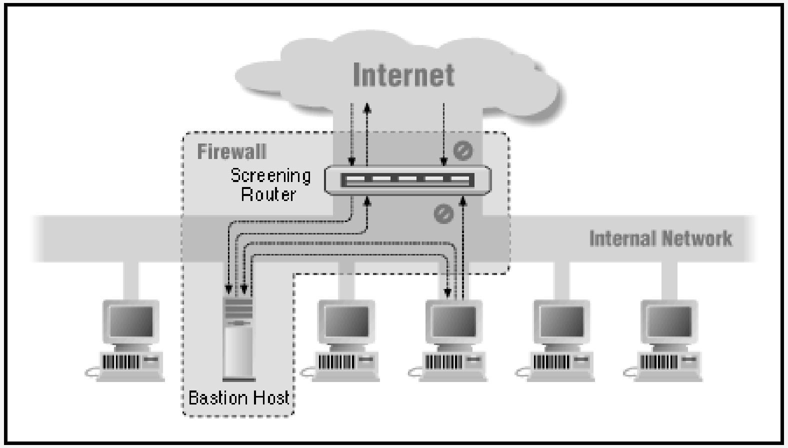
Firewall configurations

- Screened host firewall system (single-homed bastion host)
- Screened host firewall system (dual-homed bastion host)
- Screened-subnet firewall system

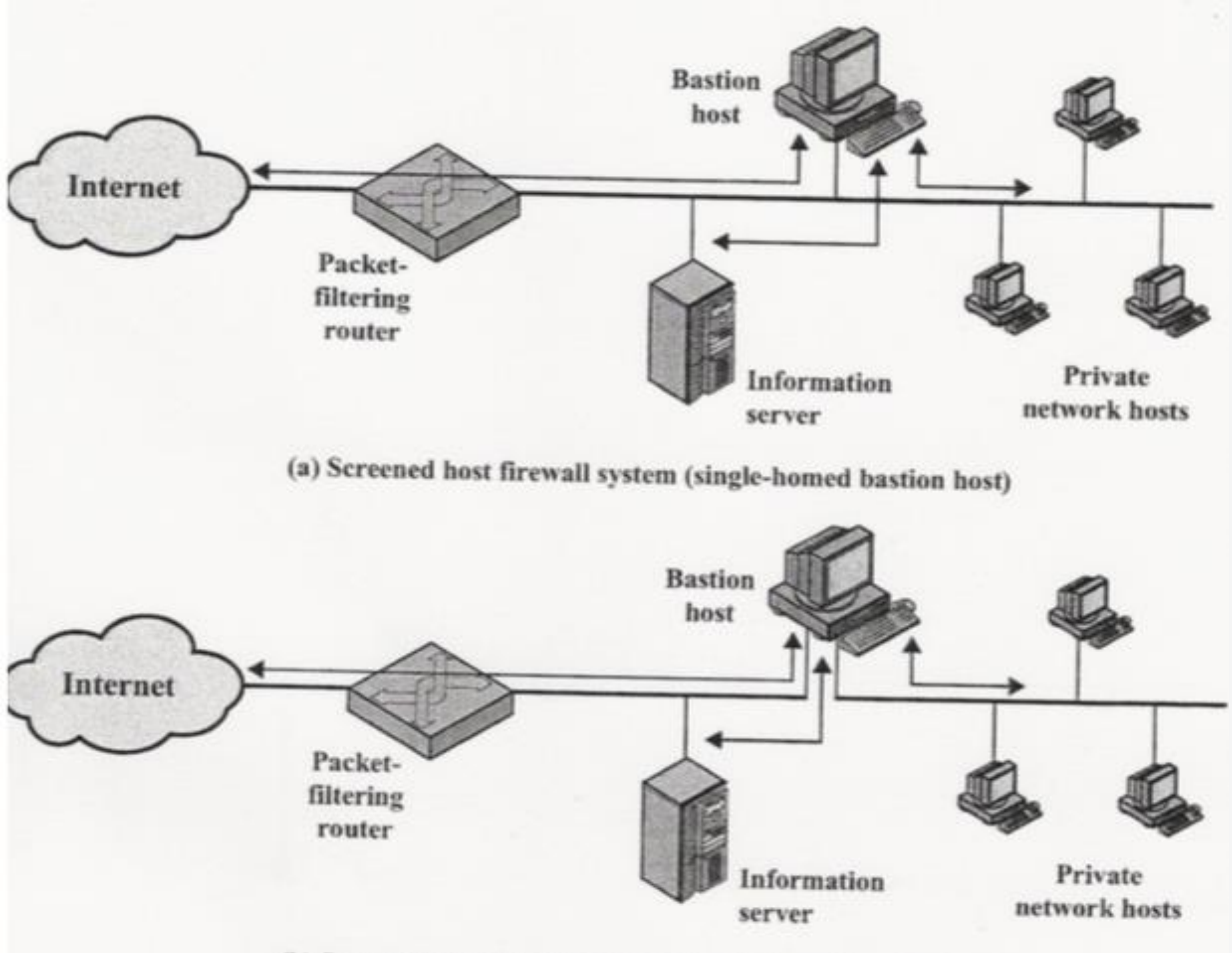
Firewall configurations (screened host)

- The usage of a “Bastion host”:
  - ✓ Controls communications with the security perimeter
  - ✓ Uses a secure version of the OS and supports only the required services
  - ✓ May support gateways (circuit and application-level)
  - ✓ Uses one or two network interfaces

- Topologies:
  - ✓ Screened host: protected host
  - ✓ Screened subnet: protected subnet



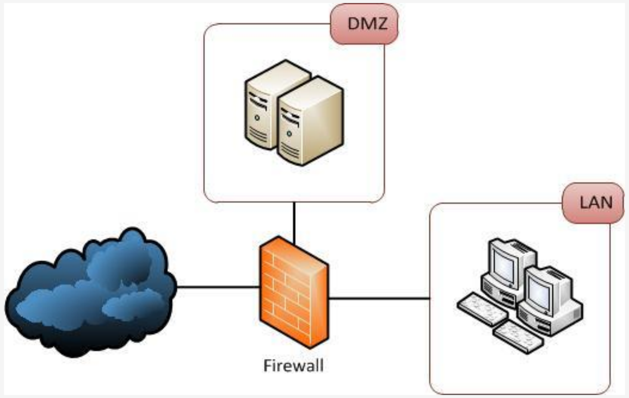
Firewall configurations (screened host)



(a) Screened host firewall system (single-homed bastion host)

(b) Screened host firewall system (dual=-homed bastion host)

Firewall configurations (screened subnet)

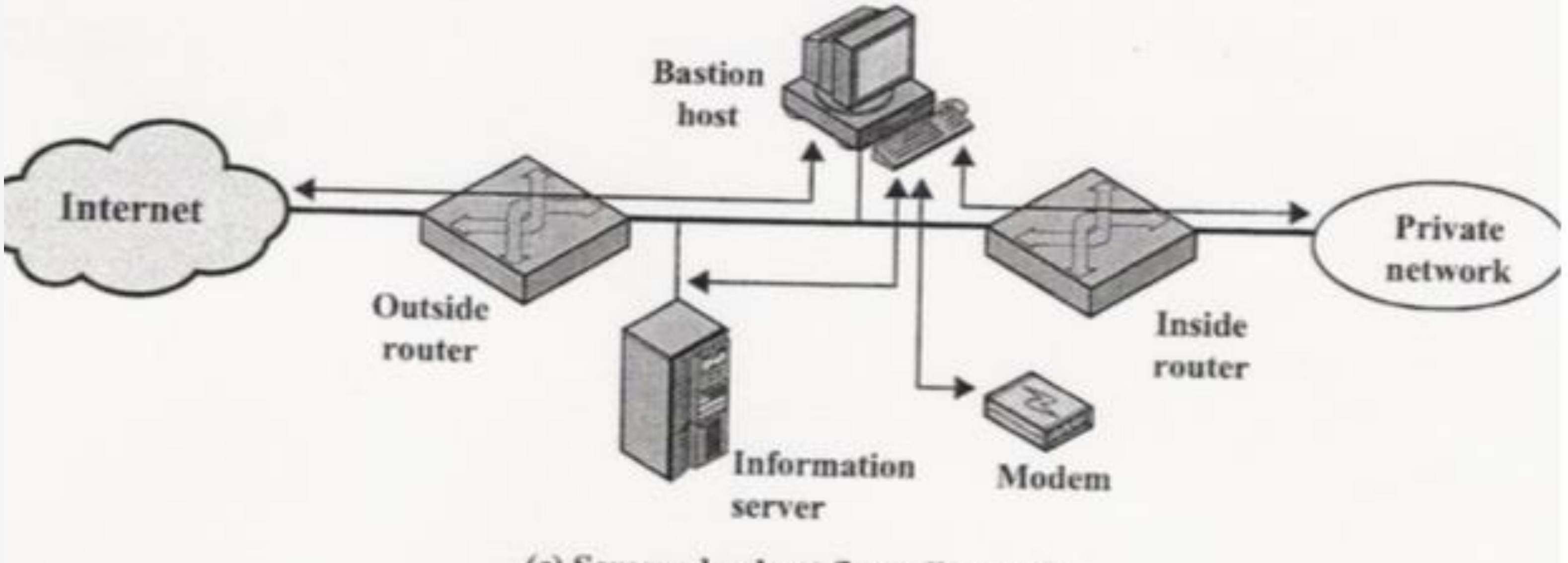


- Implements three defence levels:
  - ✓ Exterior
  - ✓ Demilitarized zones (DMZ)
  - ✓ Secure network (security perimeter)

- In the DMZ:
  - ✓ Bastion host controls accesses and authenticates users
  - ✓ One or more hosts supporting public services

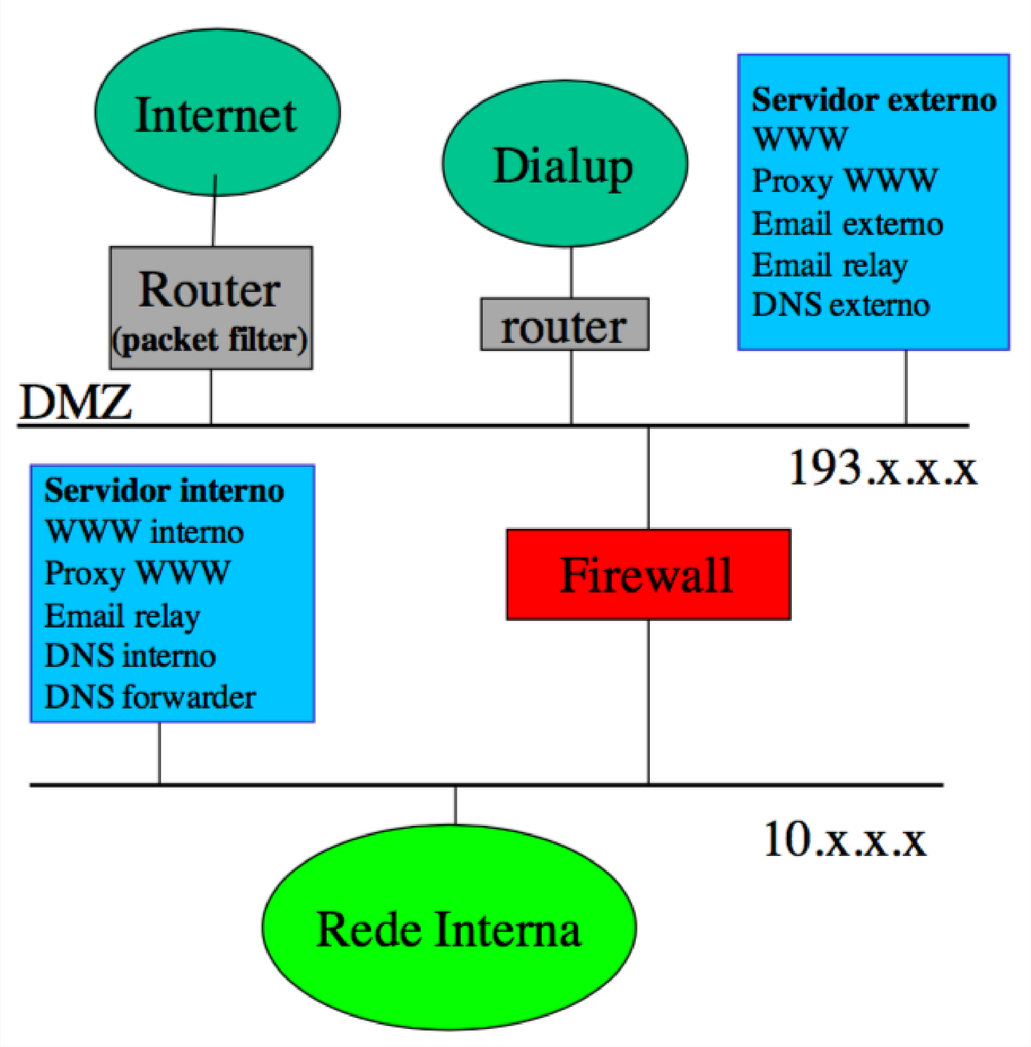
- Allowed communications:
  - ✓ From the outside (Internet) to the services available in the DMZ
  - ✓ From the internal network to the services available in the DMZ
  - ✓ Packet filtering control communications between the various networks
  - ✓ May also implement NAT (Network Address Translation)

Firewall configurations (screened subnet)



(c) Screened-subnet firewall system

Firewall example configuration



Intrusion Detection Systems

- Operation
  - ✓ Monitor IP communications for detecting attack patterns in real-time
  - ✓ Uses rules and heuristics
  - ✓ May support AI (Artificial Intelligence) techniques

- Goals
  - ✓ Complements the security provided by a Firewall
  - ✓ Detect new forms of attacks
  - ✓ Filtering contents
  - ✓ Detect virus, trojan horses, etc.

- Components of an IDS architecture
  - ✓ Detection engine (captures and analyses communications)
  - ✓ Console (generates alarms and reports)
  - ✓ The two components may be supported by separate or the same server

What is an Intrusion Detection System?

- Defined as the tools, methods, and resources to help identify, assess, and report unauthorized or unapproved network activity.

- An IDS detects activity in traffic that may or may not be an intrusion.

- IDSs can detect and deal with insider attacks, as well as, external attacks, and are often very useful in detecting violations of corporate security policy and other internal threats.

Host-based Intrusion Detection

- Are usually installed on servers and are more focused on analysing the specific operating systems and applications, resource utilization and other system activity residing on the Host-based IDS host

- It will log any activities it discovers to a secure database and check to see whether the events match any malicious event record listed in the knowledge base

- Host-based IDS are often critical in detecting internal attacks directed towards an organization’s servers such as DNS, Mail, and Web Servers

- Example: OSSEC

Network-based Intrusion Detection

- Are dedicated network devices distributed within networks that monitor and inspect network traffic flowing through the device

- Instead of analysing information that originates and resides on a host, Network-based IDS (NIDS) uses packet sniffing techniques to pull data from TCP/IP packets or other protocols that are traveling along the network

- Most Network-based IDS log their activities and report or alarm on questionable events.

- Network-based IDS work best when located on the DMZ, on any subnets containing mission critical servers and just inside the firewall

- Example: SNORT

Host or Network IDS (comparison)

Host Based

- Narrow in scope (watches only specific host activities)
- More complex setup
- Detection is based on what any single host can record
- Usually only responds after a suspicious log entry has been made
- OS-specific
- Detects local attacks before they hit the network
- Verifies success or failure of attacks

Network Based

- Broad in scope (watches all network activities)
- Easier setup
- Less expensive to implement
- Detection is based on what can be recorded on the entire network
- Near real-time response
- OS-independent
- Detects network attacks as payload is analysed
- Detects unsuccessful attack attempts

Hybrid Intrusion Detection

- Are systems that combine both Host-based IDS, which monitors events occurring on the host system and Network-based IDS, which monitors network traffic, functionality on the same security platform.

- A Hybrid IDS, can monitor system and application events and verify a file system’s integrity like a Host-based IDS, but only serves to analyse network traffic destined for the device itself.

- A Hybrid IDS is often deployed on an organization’s most critical servers.

- Example: Prelude SIEM

PRELUDE
A CS Product

Signature-based IDS

- Monitor network or server traffic and match bytes or packet sequences against a set of predetermined attack lists or signatures
- Should a particular intrusion or attack session match a signature configured on the IDS, the system alerts administrators or takes other pre-configured action
- Signatures are easy to develop and understand if you know what network behaviour you're trying to identify
- However, because they only detect known attacks, a signature must be created for every attack
- New vulnerabilities and exploits will not be detected until administrators develop new signatures
- Another drawback to signature-based IDS is that they are very large and it can be hard to keep up with the pace of fast moving network traffic

Anomaly-based IDS

- Use network traffic baselines to determine a “normal” state for the network and compare current traffic to that baseline.
- Use a type of statistical calculation (or machine learning algorithm) to determine whether current traffic deviates from “normal” traffic, which is either learned and/or specified by administrators.
- If network anomalies occur, the IDS alerts administrators.
- A new attack for which a signature doesn’t exist can be detected if it falls out of the “normal” traffic patterns.
- High false alarm rates created by inaccurate profiles of “normal” network operations.

Issues

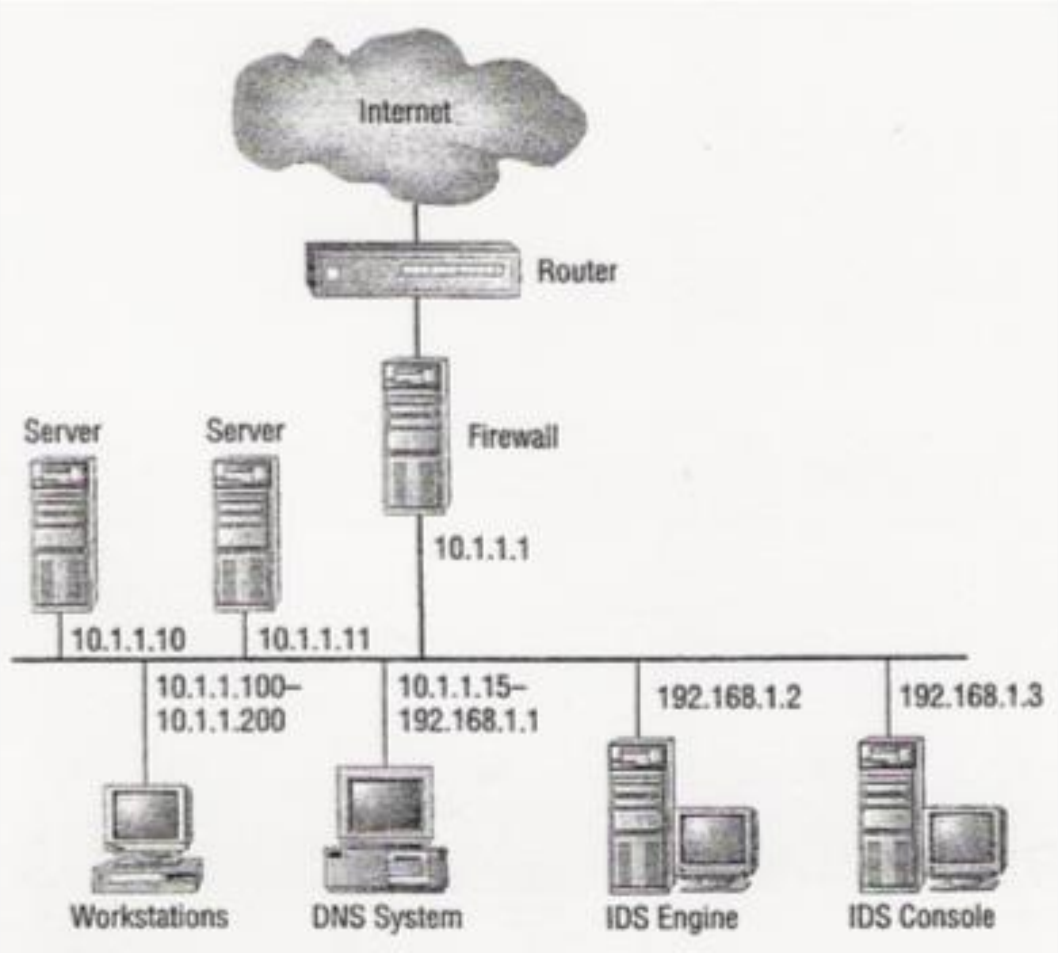
False Negatives

- When an IDS fails to detect an attack
- False negatives occur when the pattern of traffic is not identified in the signature database, such as new attack patterns.
- False negatives are deceptive because you usually have no way of knowing if and when they occurred.
- You are most likely to identify false negatives when an attack is successful and wasn’t detected by the IDS.

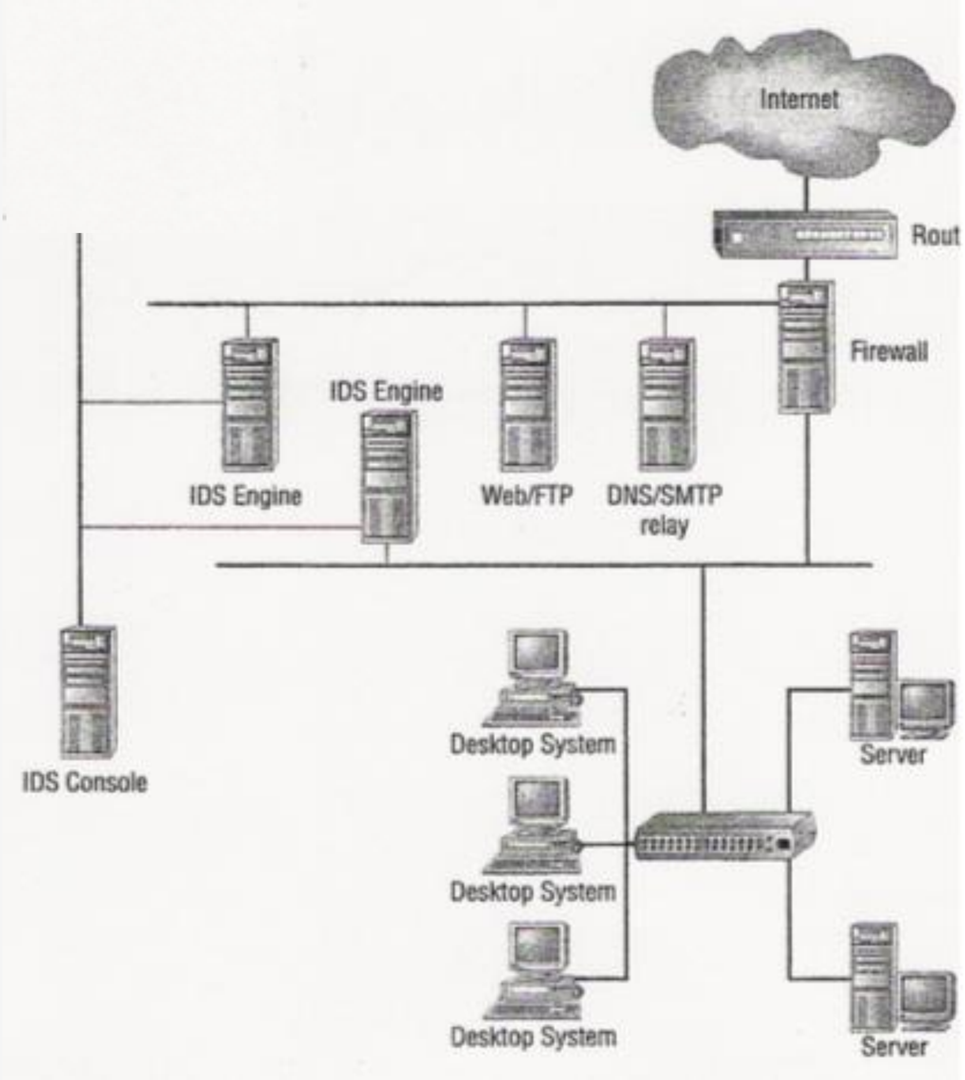
False Positives

- Described as a false alarm.
- When an IDS mistakenly reports certain “normal” network activity as malicious.
- Administrators have to fine tune the signatures or heuristics in order to prevent this type of problem.

Intrusion detection (deployment example)



Intrusion detection (deployment example)



Intrusion detection (Snort)

- SNORT is a NIDS (Network Intrusion Prevention and Detection), www.snort.org
- May operate as a:
  - ✓ Sniffer
  - ✓ Packet logger
  - ✓ NIDS

Usage examples (in Sniffer mode)

```
# prints TCP/IP (IP, UDP, TCP and ICMP) headers
snort -v
# prints also data payloads
snort -vd
```

Intrusion detection (Snort)

Usage examples (in Packet Logger mode)

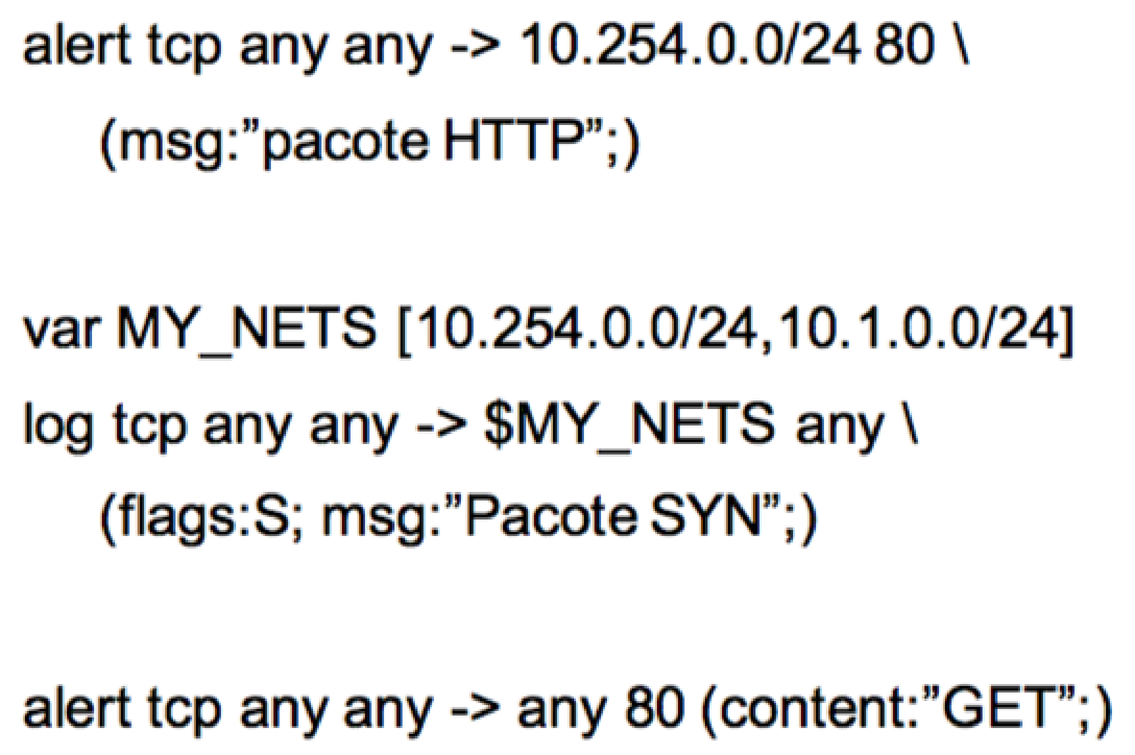
```
# Logs packets in the indicated directory
snort -vd -l /var/log/snort
```

```
# As the previous example but now using the indicated source IP range
snort -vde -l /var/log/snort -h 192.168.1.0/24
```

Usage examples (in NIDS mode)

```
# Use the detection rules defined in the configuration file
snort -d -l /var/log/snort -h 192.168.1.0/24 -c snort.conf
```

Intrusion detection (Snort detection rules)



```
alert tcp any any -> 10.254.0.0/24 80 \
    (msg:”pacote HTTP”;)

var MY_NETS [10.254.0.0/24,10.1.0.0/24]
log tcp any any -> $MY_NETS any \
    (flags:S; msg:”Pacote SYN”;)

alert tcp any any -> any 80 (content:”GET”;)
```

Accessing the network traffic

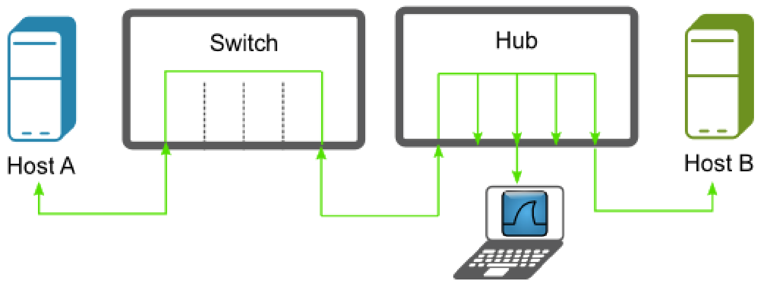
Mirroring ports

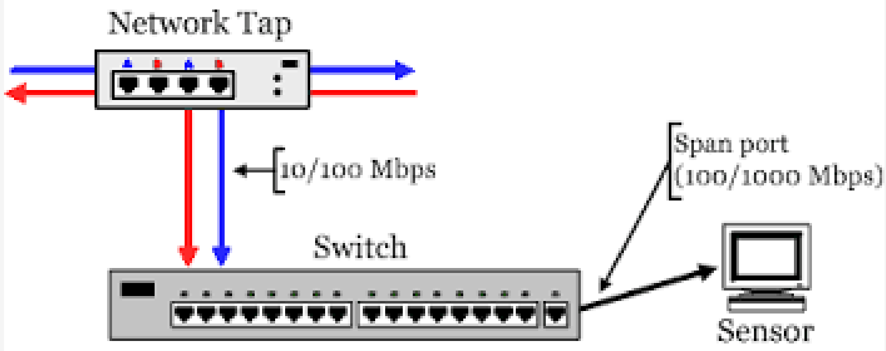
- Device (e.g. switch) sends a copy of network packets from one port (or an entire VLAN) to another (monitoring port).
- Example on Cisco: switched Port ANalyzer (SPAN) or Remote Switched Port ANalyzer (RSPAN) ports

Networking TAPS

- Inserted between network devices to copy data continuously without compromising network integrity
- Available with a variety of features for both copper and fiber networks

Forced packet repetition using a non-switched Hub



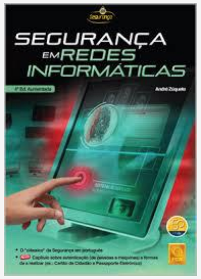


Summary

- Access control
  - ✓ Access control policies and mechanisms
  - ✓ Access control elements
- Firewalls
  - ✓ Types of firewalls
  - ✓ Packet filters
  - ✓ Circuit-level gateways
  - ✓ Application-level gateways
  - ✓ Packet filtering with IPTables
  - ✓ Firewall configurations
- Intrusion Detection Systems
  - ✓ Host-based Intrusion Detection
  - ✓ Network-based Intrusion Detection
  - ✓ Hybrid Intrusion Detection
  - ✓ Honeypots
  - ✓ Signature-based IDS
  - ✓ Anomaly-based IDS
  - ✓ Intrusion detection with Snort

Bibliography

Segurança em Redes Informáticas, André Zúquete, FCA, Capítulo 6: Firewalls, Capítulo 7: Sistemas de Deteção de Intrusão



Segurança Prática em Sistemas e Redes com Linux, Capítulo 5: Servidores WWW seguros, Capítulo 7: Proteção de Servidores, Capítulo 10: Deteção e Prevenção de Intrusões