Network Security - Firewalls
Proxy Server, IDS/IPS
Web Content Filters
UTMs

Network Security

- Network security is any activity designed to protect the usability and integrity of your network and data.
- It includes both hardware and software technologies
- It targets a variety of threats
- It stops them from entering or spreading on your network
- Effective network security manages access to the network

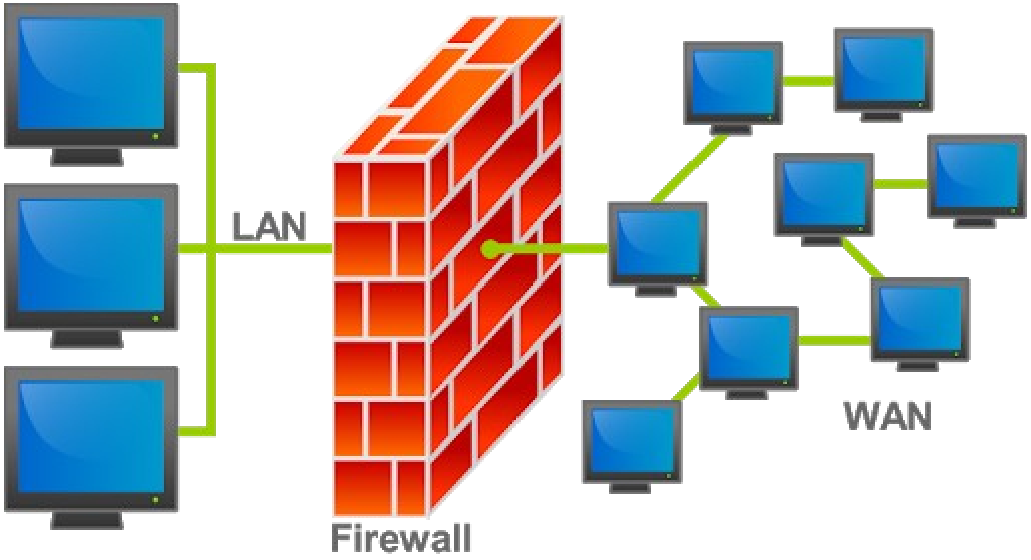
Types of network security

- Firewalls
- Email security
- Anti-virus and anti-malware software
- Network segmentation
- Access control
- Application security
- Behavioral analytics
- Data loss prevention
- Intrusion prevention systems
- Mobile device security
- Security information and event management
- VPN
- Web security
- Wireless security

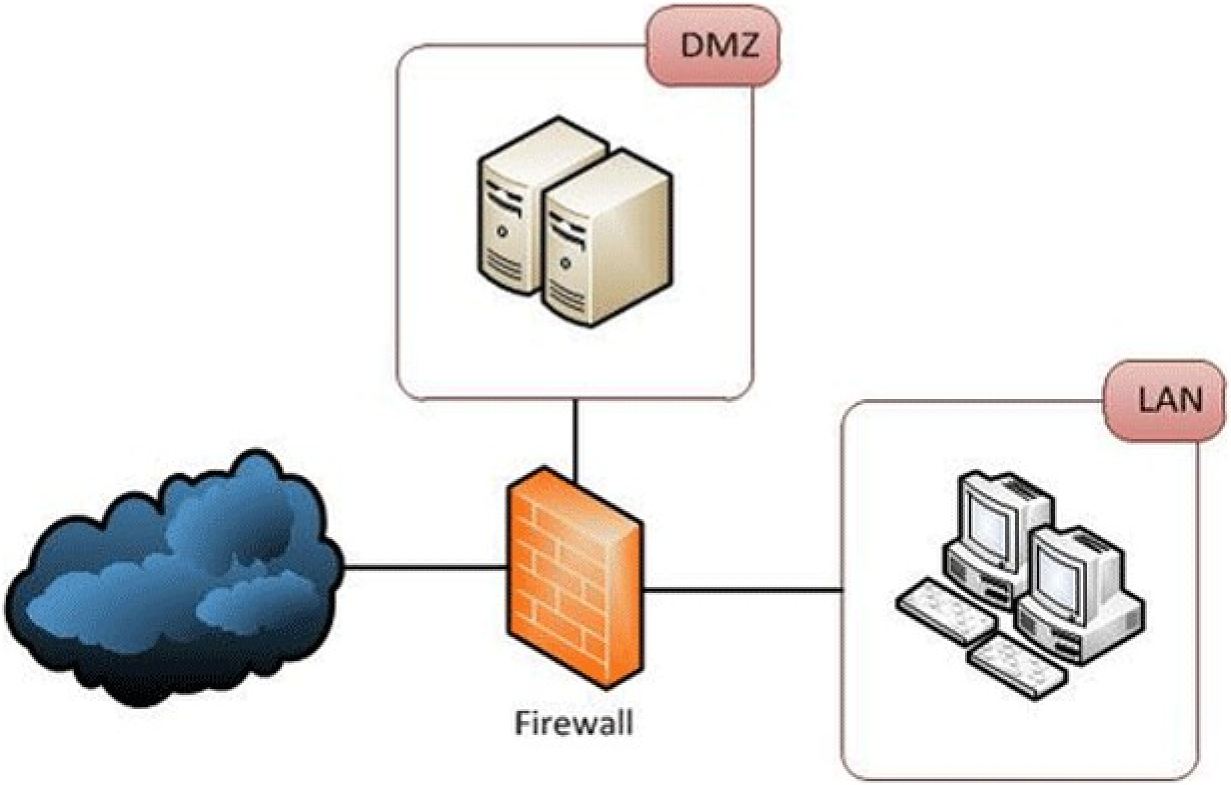
Firewalls

- A firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- Firewalls have been a first line of defense in network security for over 25 years.
- They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.
- A firewall can be hardware, software, or both.

Basic Network Firewall



Firewall with DMZ



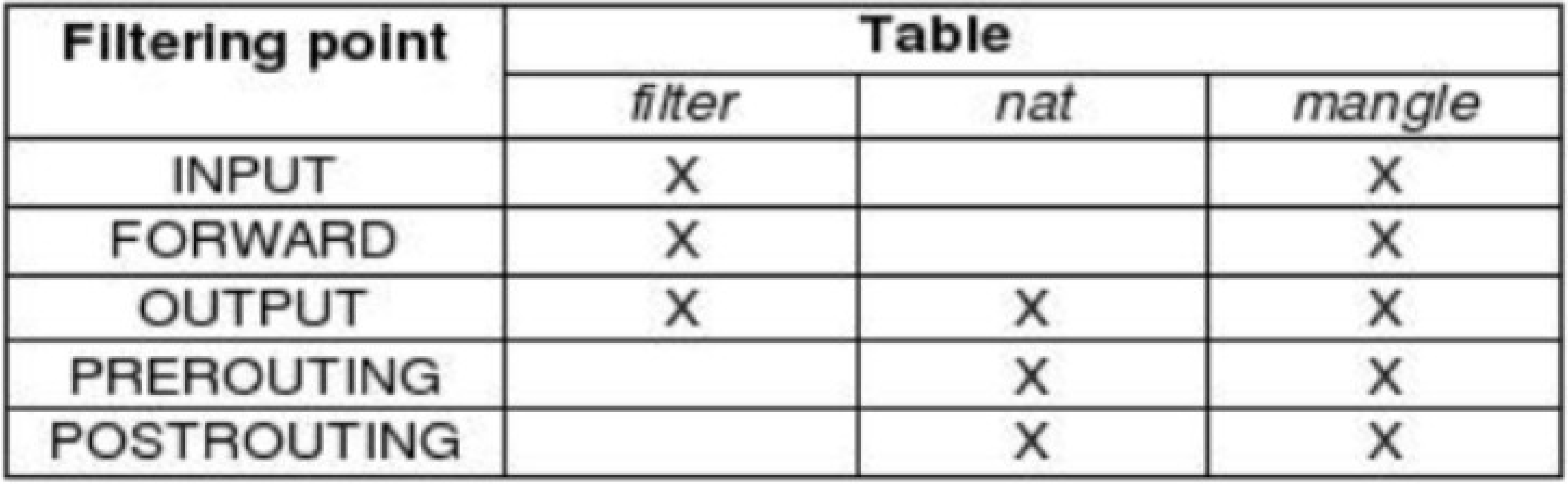
Linux firewalls

- netfilter/iptables
- Firewalld
- Nftables
- ufw

Netfilter Overview

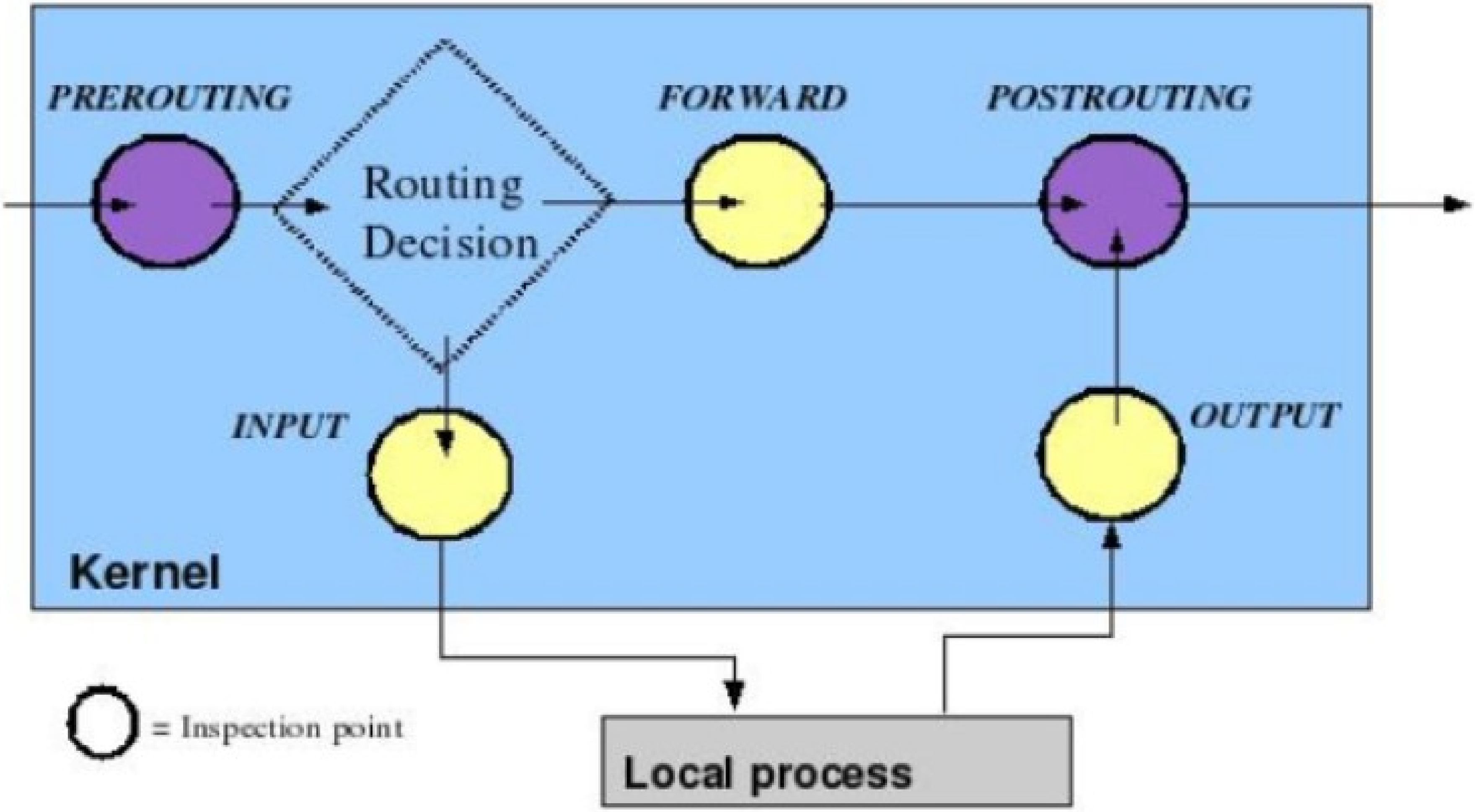
- Filtering in the kernel: no daemon
- Asserts policies at layers 2, 3 & 4 of the OSI Reference Model
- Only inspects packet headers
- Consists of `netfilter` modules in kernel, and the **iptables** user-space software

Netfilter Tables and Chains



Filtering point	**Table**		
	filter	*nat*	*mangle*
INPUT	X		X
FORWARD	X		X
OUTPUT	X	X	X
PREROUTING		X	X
POSTROUTING		X	X

Netfilter Packet Flow



Netfilter – Rule Matching

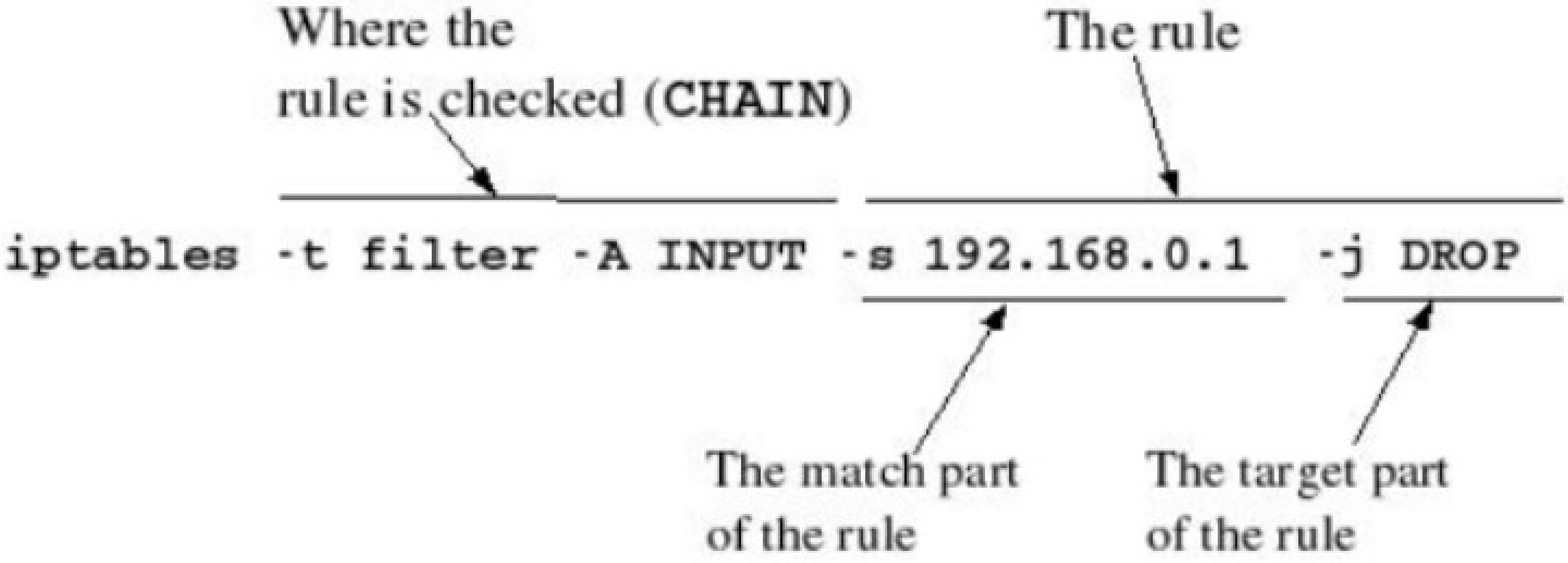
- Rules in ordered list
- Packets tested against each rule in turn
- On first match, the target is evaluated: usually exits the chain
- Rule may specify multiple criteria for match
- Every criterion in a specification must be met for the rule to match (logical AND)
- Chain policy applies if no match

Rule Targets

- Built-in targets: `DROP`, `ACCEPT`
- Extension targets: `LOG`, `REJECT`, custom chain
  - `REJECT` sends a notice returned to sender
  - `LOG` connects to system log kernel facility
  - `LOG` match does not exit the chain
- Target is optional, but no more than one per rule and defaults to the chain policy if absent

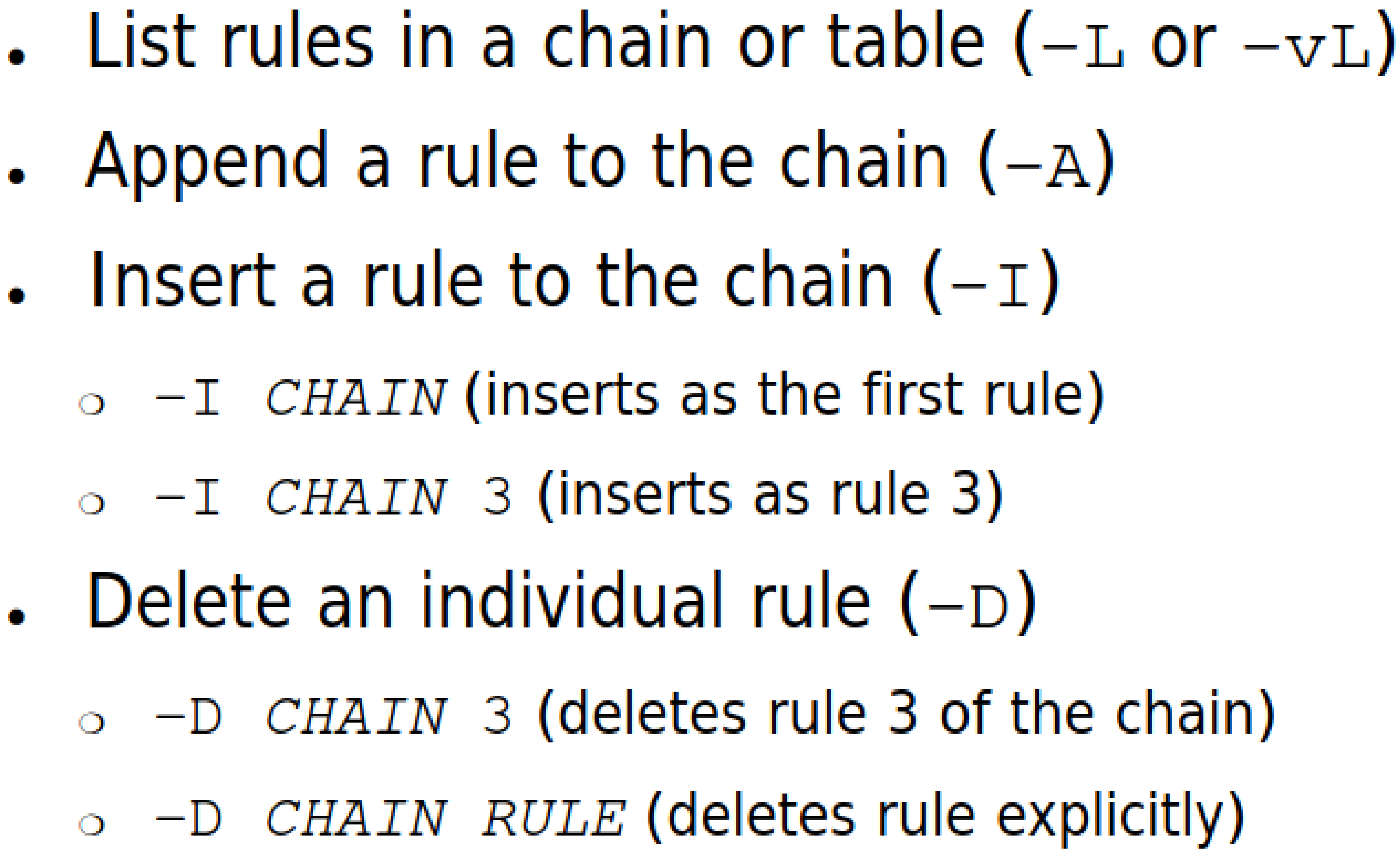
A simple example

- An `INPUT` rule for the filter table:



```
iptables -t filter -A INPUT -s 192.168.0.1 -j DROP
```

Basic Chain Operations



- List rules in a chain or table (`-L` or `-vL`)
- Append a rule to the chain (`-A`)
- Insert a rule to the chain (`-I`)
  - `-I` *`CHAIN`* (inserts as the first rule)
  - `-I` *`CHAIN`* `3` (inserts as rule 3)
- Delete an individual rule (`-D`)
  - `-D` *`CHAIN`* `3` (deletes rule 3 of the chain)
  - `-D` *`CHAIN`* *`RULE`* (deletes rule explicitly)

Additional Chain Operations

- Assign chain policy (-P *CHAIN* *TARGET*)
  - ACCEPT (default, a built-in target)
  - DROP (a built-in target)
  - REJECT (not permitted, an extension target)
- Flush all rules of a chain (-F)
  - Does not flush the policy
- Zero byte and packet counters (-Z [*CHAIN*])
  - Useful for monitoring chain statistics

General Considerations

- Mostly closed is appropriate
  - **iptables -P INPUT DROP** or
  - **iptables -A INPUT -j DROP**
  - **iptables -A INPUT -j REJECT**
- Criteria also apply to loopback interface
  - The example rules above will have the side effect of blocking localhost!
- Rules, like routes, are loaded in memory and must be saved to a file for persistence across reboots

Match Arguments

- Mostly closed is appropriate
  - **iptables -P INPUT DROP** or
  - **iptables -A INPUT -j DROP**
  - **iptables -A INPUT -j REJECT**
- Criteria also apply to loopback interface
  - The example rules above will have the side effect of blocking localhost!
- Rules, like routes, are loaded in memory and must be saved to a file for persistence across reboots

Connection tracking

- Provides inspection of packet's "state"
  - a packet can be tested in a specific context
- Simplifies rule design
  - without connection tracking, rules are usually in pairs (inbound & outbound)
- Implemented in "state" match extension
- Recognized states: **NEW**, **ESTABLISHED**, **RELATED**, **INVALID**
- Requires more memory

- One rule to permit established connections:

```
iptables -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

- Many rules; one for each permitted service:

```
iptables -A INPUT -m state --state NEW -p tcp --dport 25 \
      -j ACCEPT
```

- Lastly, one rule to block all others inbound:

```
iptables -A INPUT -m state --state NEW -j DROP
```

Network Address Translation

- Translates one IP address into another (inbound and/or outbound)
- Allows "hiding" internal IP addresses behind a single public IP
- Rules set within the `nat` table
- Network Address Translation types:
  - Destination NAT (DNAT) - Set in the PREROUTING chain where filtering uses translated address
  - Source NAT (SNAT, MASQUERADE) - Set in the POSTROUTING chain where filtering *never* uses translated address

DNAT Example

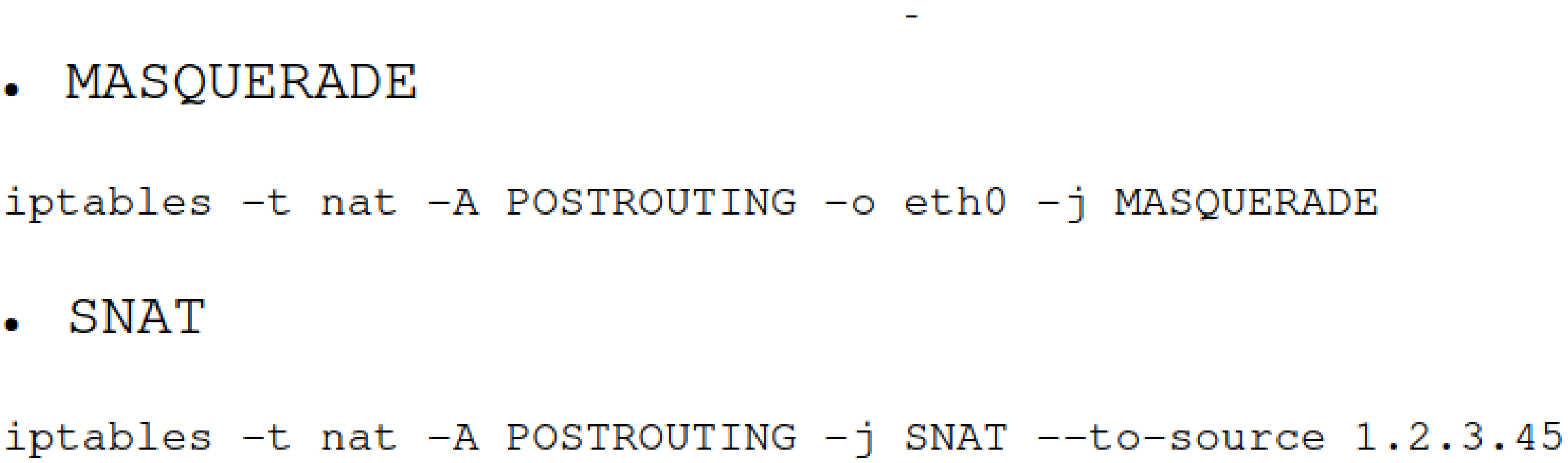
- INBOUND

```
iptables -t nat -A PREROUTING -p tcp --dport 80 -j DNAT \
     --to-dest 192.168.0.20
```

- OUTBOUND (with port redirection)

```
iptables -t nat -A OUTPUT -p tcp --dport 80 -j DNAT \
     --to-dest 192.168.0.200:3128
```

SNAT Example



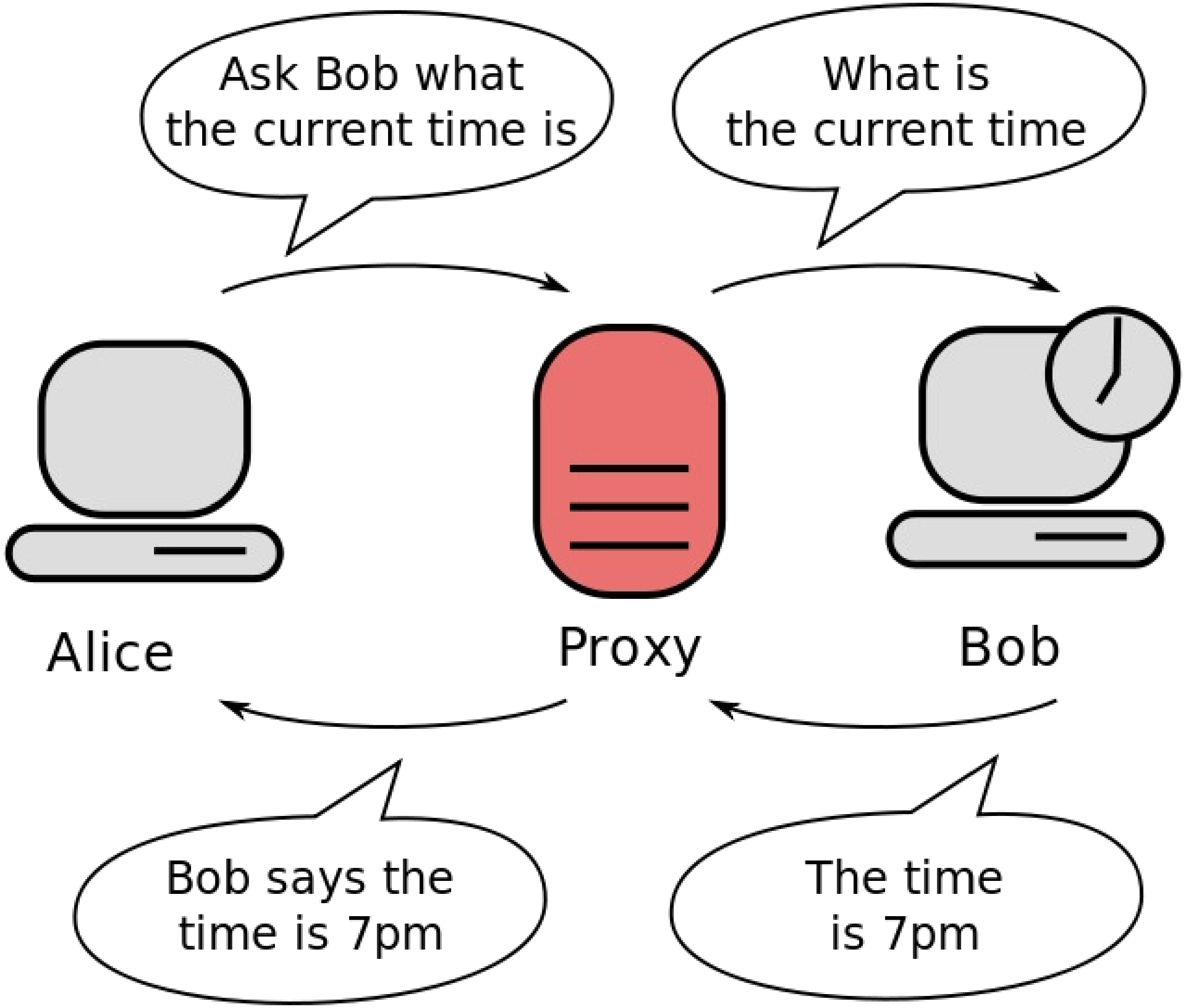
- MASQUERADE

```
iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

- SNAT

```
iptables -t nat -A POSTROUTING -j SNAT --to-source 1.2.3.45
```

Proxy Server



Proxy Server..

- In computer networking, a proxy server is a server application or appliance that acts as an intermediary for requests from clients seeking resources from servers that provide those resources.
- A proxy server thus functions on behalf of the client when requesting service, potentially masking the true origin of the request to the resource server.

Example – Squid Proxy

- Squid is a caching proxy for the Web supporting HTTP, HTTPS, FTP, and more.
- It reduces bandwidth and improves response times by caching and reusing frequently-requested web pages.
- Squid has extensive access controls and makes a great server accelerator.
- It runs on most available operating systems, including Windows and is licensed under the GNU GPL.
- http://www.squid-cache.org/

Intrusion Detection/Prevention

Security Scenario

- Physical Security
  - Locks
  - Walls
  - Gates
  - Guards
  - Motion sensors
  - Pressure plates

- Network and Data
  - Passwords
  - Firewalls
  - Access control lists
  - File permissions
  - Intrusion detection/prevention systems

What is Intrusion Detection

- Intrusion detection is a set of techniques and methods that are used to detect suspicious activity both at the network and host level.
- Two types (mode of operation):
  - Signature based
  - Anomaly based
- Based on the placement, again two types:
  - Host based
  - Network based

What is an Intrusion Detection System

- *Intrusion Detection System* or IDS is software, hardware or combination of both used to detect intruder activity.

IDS mapping

- Physical security
  - Burglar alarms

- Network/Data Security
  - Intrusion Detection systems

Purpose of IDS

- Identify suspicious or malicious activity
- Note activity that deviates from normal behavior
- Catalog and classify the activity
- If possible, respond to the activity

IDS Components

- Traffic Collector
- Analysis Engine
- Signature database
- User interface and reporting

Host Based IDS

- Installed as agents on a host
- Is a system that examines:
  - Log files
  - Audit trails
  - Network traffic coming into or leaving the host

Detection of Hostile actions or misuse, from log files

- Logins at odd hours
- Login authentication failures
- Adding new user accounts
- Modification or access of critical system files
- Modification or removal of executables
- Starting and stopping processes
- Privilege escalation
- Use of certain programs

Advantages of Host based IDS

- They can be very operating system-specific and have more detailed signatures.
- They can reduce false positive rates
- They can examine data after it has been decrypted.
- They can be very application specific.
- They can determine whether or not an alarm may impact that specific system.

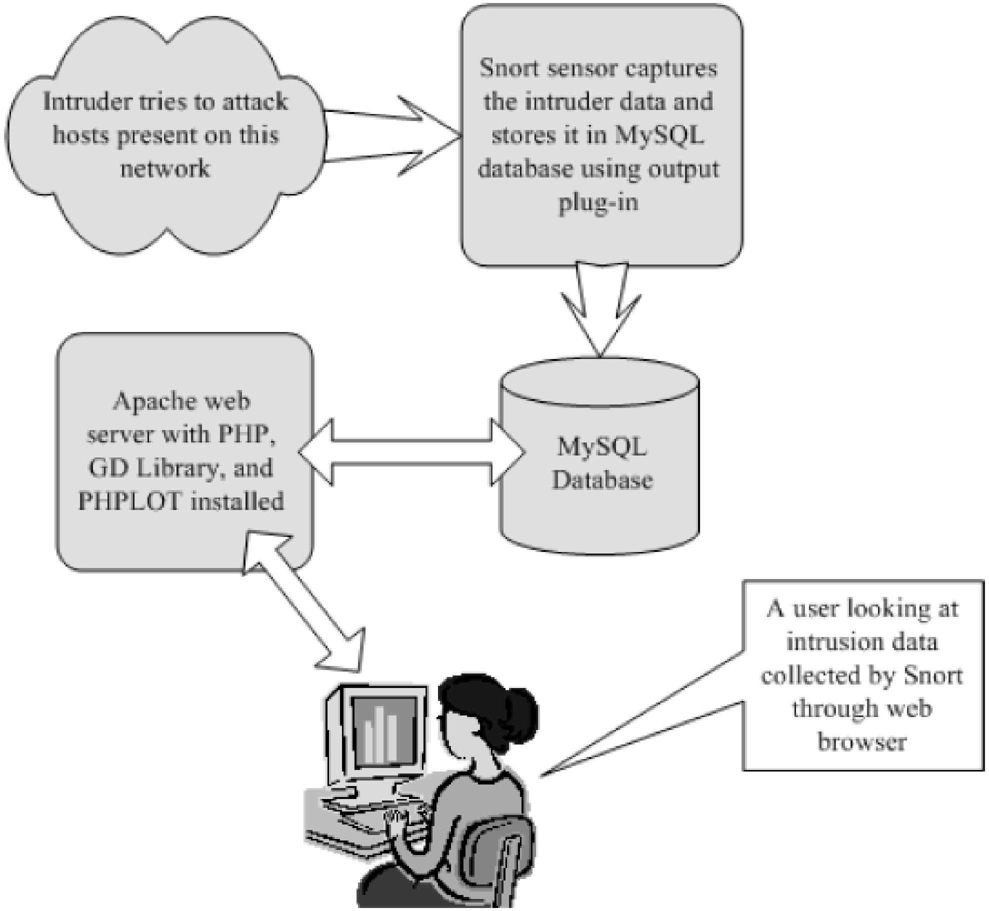
Disadvantages of Host based IDS

- The IDS must have a process on every system you want to watch
- The IDS can have a high cost of ownership and maintenance
- The IDS uses local system resources
- The IDS has a very focused view and cannot relate to activity around it.
- The IDS, if logged locally, could be compromised or disabled.

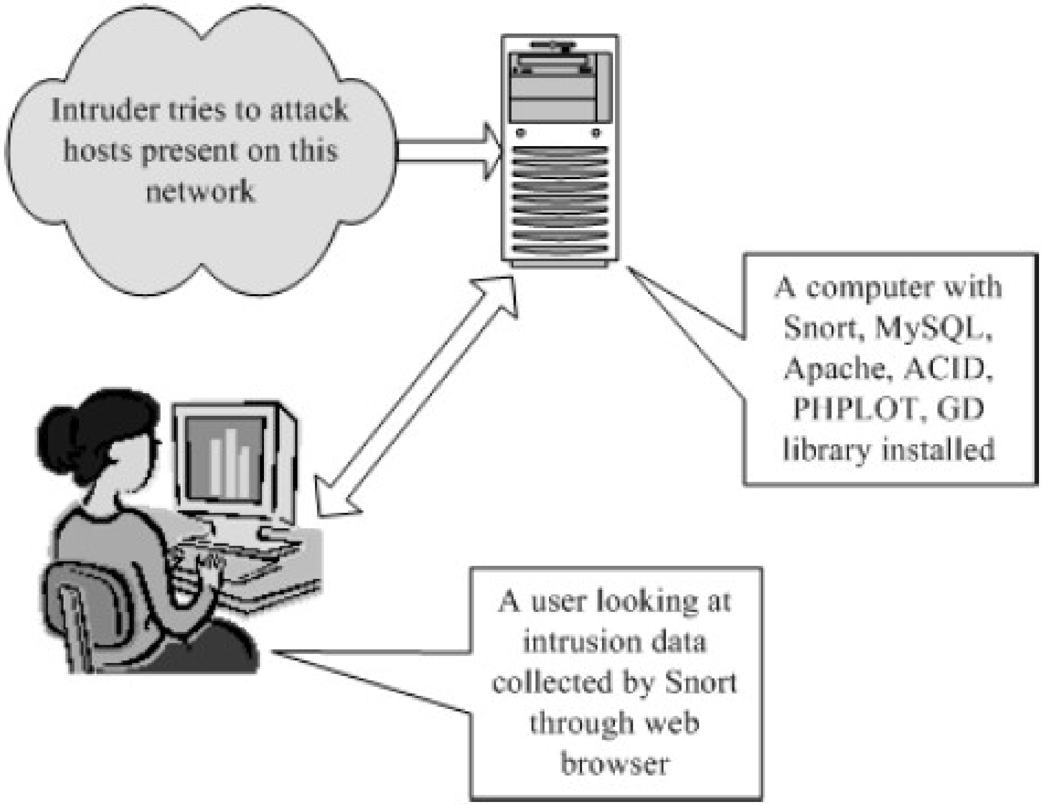
Network based IDS

- NIDS are intrusion detection systems that capture data packets traveling on the network media (cables, wireless) and match them to a database of signatures.
- Depending upon whether a packet is matched with an intruder signature, an alert is generated or the packet is logged to a file or database.

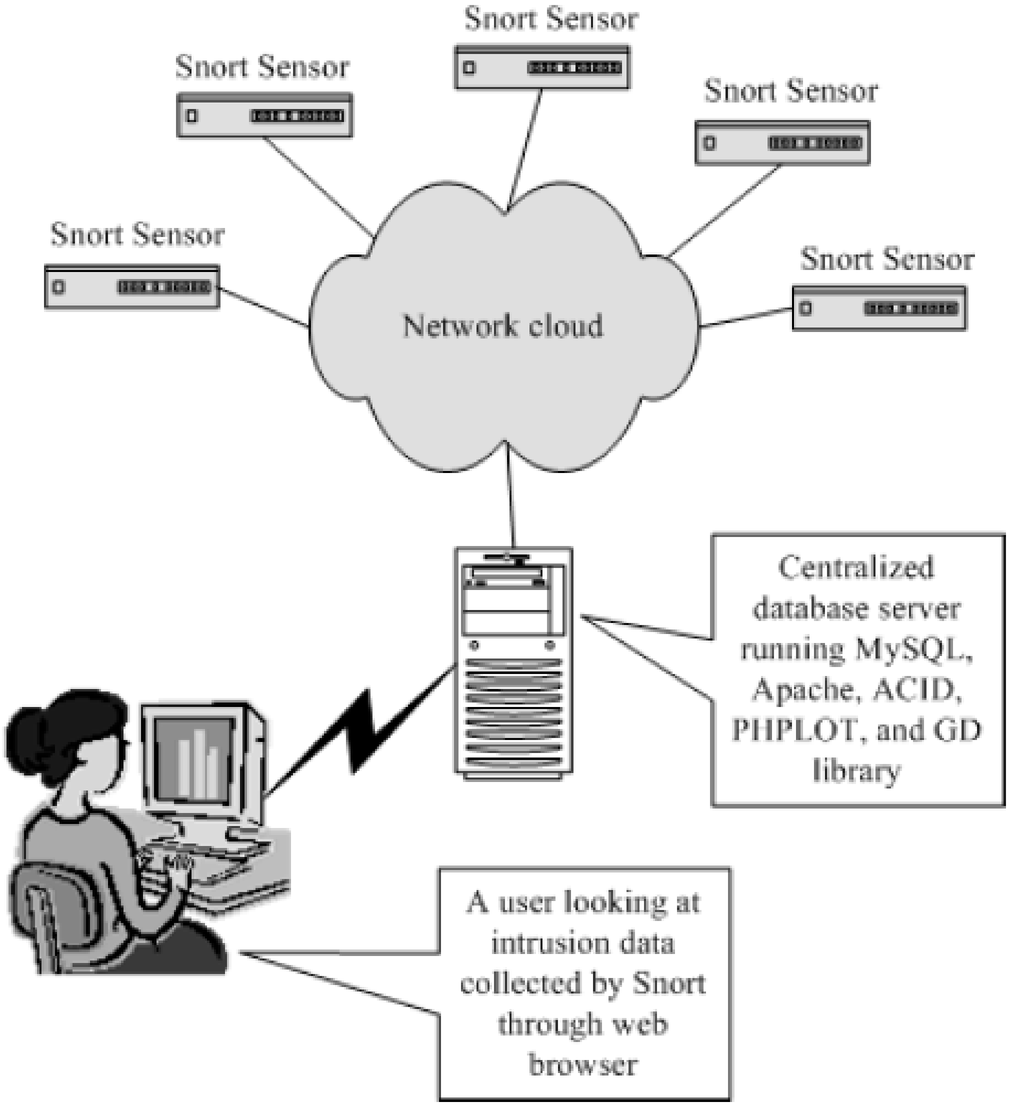
Case Study - Snort


Intruder tries to attack hosts present on this network
Snort sensor captures the intruder data and stores it in MySQL database using output plug-in
MySQL Database
Apache web server with PHP, GD Library, and PHPLOT installed
A user looking at intrusion data collected by Snort through web browser

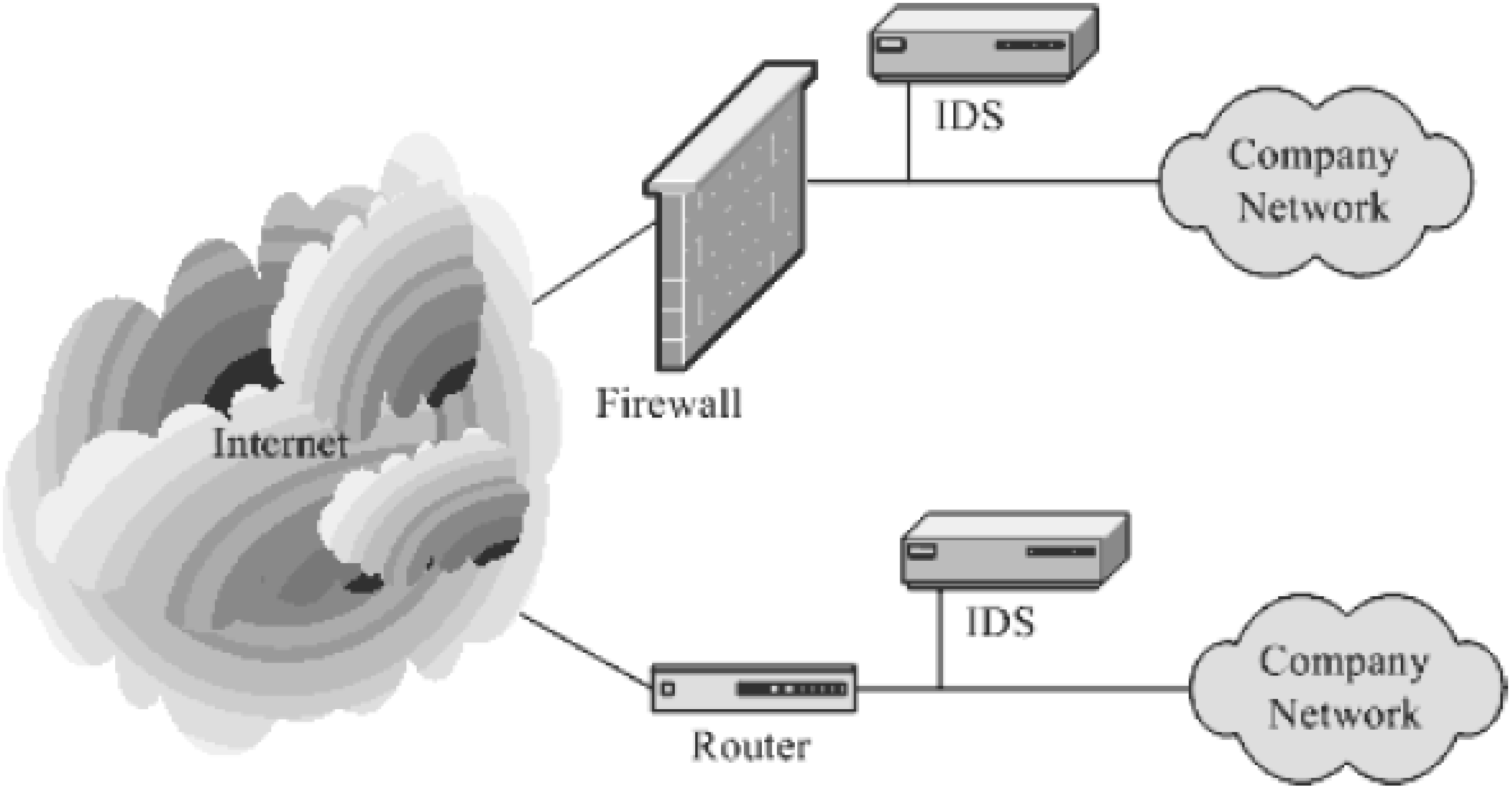
Block diagram of a complete network intrusion detection system consisting of Snort, MySQL, Apache, ACID, PHP, GD Library and PHPLOT.


Intruder tries to attack hosts present on this network
A computer with Snort, MySQL, Apache, ACID, PHPLOT, GD library installed
A user looking at intrusion data collected by Snort through web browser

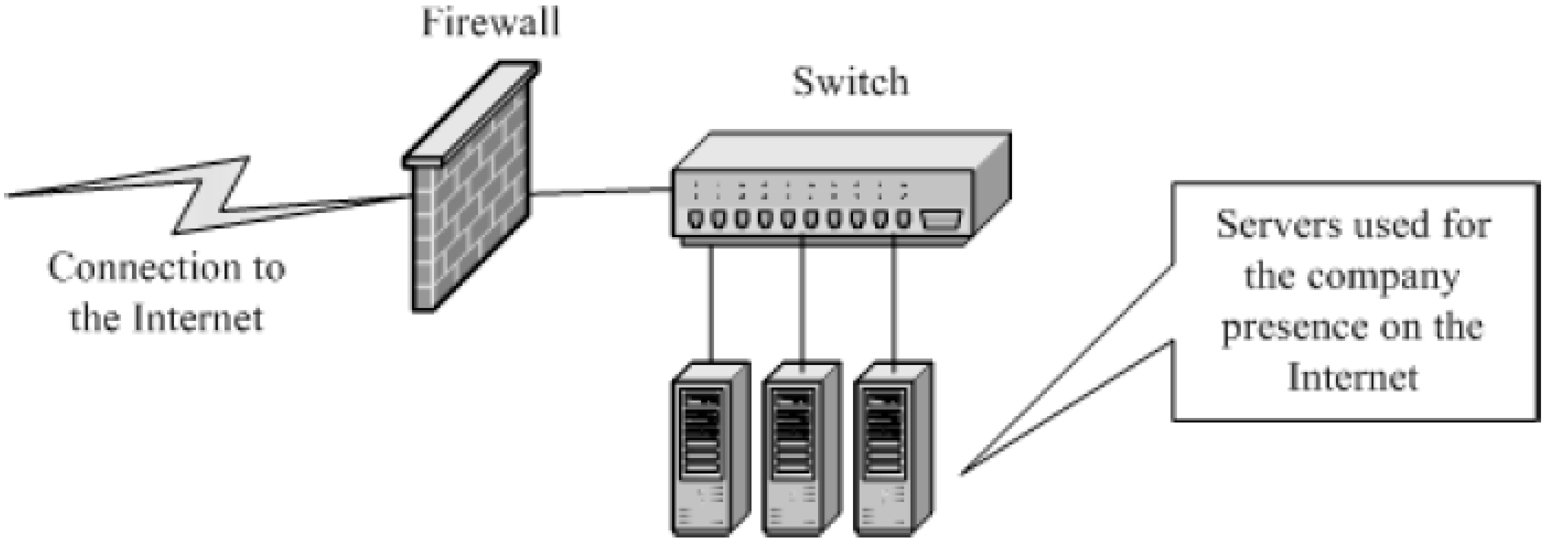
A network intrusion detection system with web interface.


Snort Sensor
Snort Sensor
Snort Sensor
Snort Sensor
Snort Sensor
Network cloud
Centralized database server running MySQL, Apache, ACID, PHPLOT, and GD library
A user looking at intrusion data collected by Snort through web browser

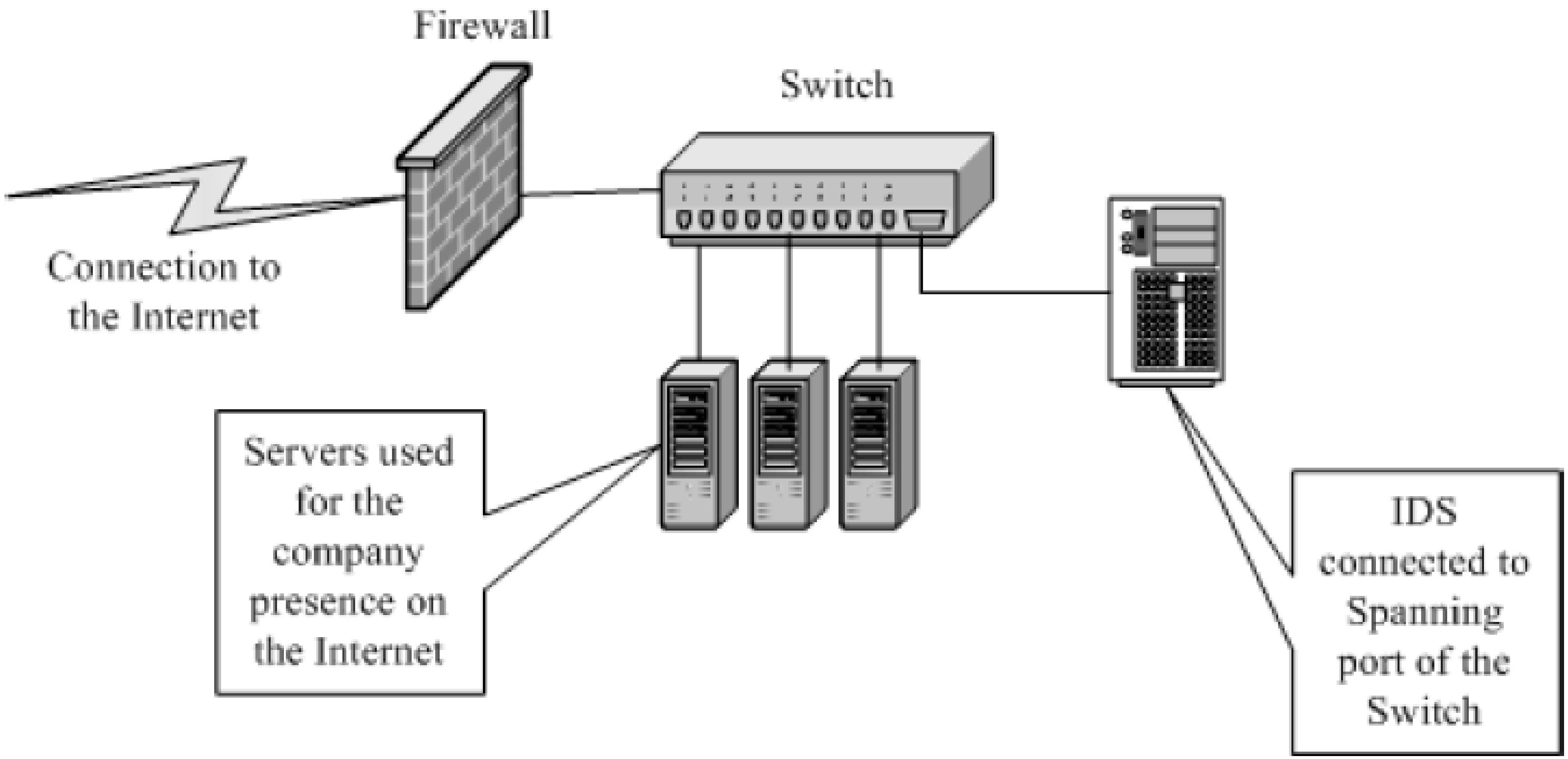
Multiple Snort sensors in the enterprise logging to a centralized database server.



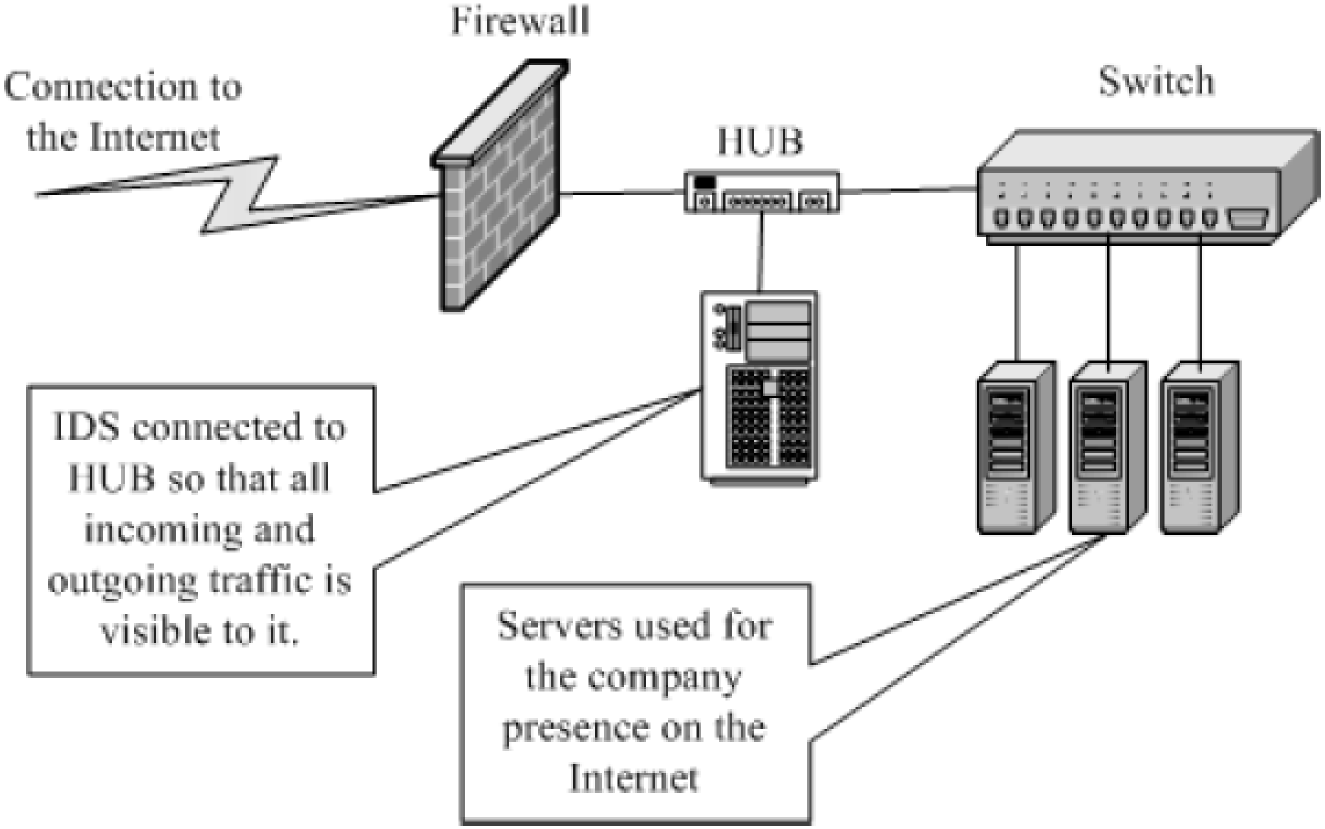
Typical locations for an intrusion detection system.


Firewall
Switch
Connection to the Internet
Servers used for the company presence on the Internet

A typical connection scheme with one firewall and switched network.

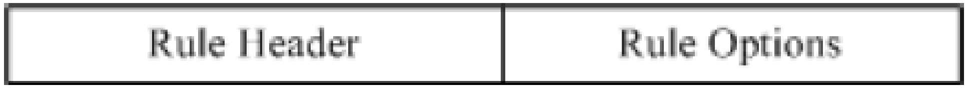

Firewall
Switch
Connection to the Internet
Servers used for the company presence on the Internet
IDS connected to Spanning port of the Switch

IDS connected a spanning port.


Firewall
Connection to the Internet
HUB
Switch
IDS connected to HUB so that all incoming and outgoing traffic is visible to it.
Servers used for the company presence on the Internet

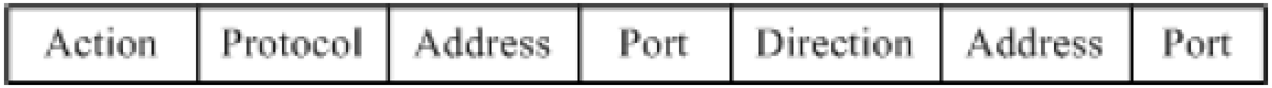
Connecting an IDS in a switched environment.

Snort Rules



Rule Header	Rule Options

Basic structure of Snort rules.



Action	Protocol	Address	Port	Direction	Address	Port

Structure of Snort rule header.

alert icmp any any -> any any (msg: "Ping with TTL=100“; ttl:100;)

alert tcp any any -> 192.168.1.10/32 80 (msg: "TTL=100"; ttl: 100;)

alert tcp any any -> 192.168.1.0/24 any (flags: A; ack: 0; msg: "TCP ping detected";)

Intrusion Prevention

- Prevent intrusions
- NIDS works with Firewall
- The previous NIDS Rule would become:

```
drop tcp any any -> 192.168.1.0/24 any (flags: A; ack: 0; msg: "TCP ping detected";)
```

- Care should be taken to avoid false positives.

Website

- Www.snort.org

Web Intrusion Detection and Prevention

- mod_security
  - An application layer firewall

Web Content filter

- Web content filtering is the practice of blocking access to web content that may be deemed offensive, inappropriate, or even dangerous.
- Families will be well aware of the need to apply internet content filters to material not suitable for young children, but content filtering has its place in the business world, too.

http://e2guardian.org/cms/

- e2guardian is an Open Source web content filter, It filters the actual content of pages based on many methods including phrase matching, request header and URL filtering, etc. It does not purely filter based on a banned list of sites

UTM Firewall

- In the early days of network security, a firewall merely filtered traffic based on ports & IP addresses.
- Unfortunately, cyber threats also evolved & diversified to meet these new challenges, organizations deployed multiple appliances, each with differing roles to defend against different classes of attacks:....

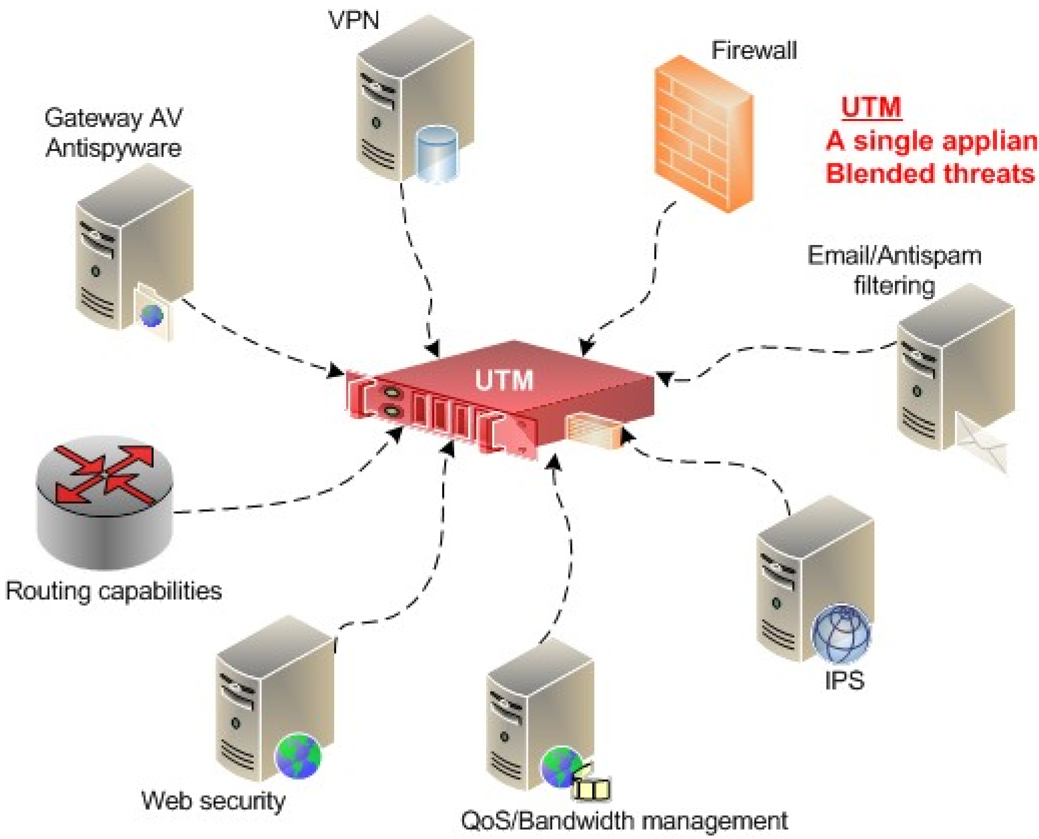
UTM .... why

- A stateful packet inspection firewall allowed inbound & outbound traffic on the network
- An additional web proxy filtered content & URLs while scanning with antivirus services
- A separate Intrusion Prevention System (IPS) was often deployed to detect & block malicious traffic
- An appliance was needed for spam filtering to filter junk emails & phishing attempts
- VPN servers connected remote offices or allowed remote users to access company resources

UTM .... why

- As more & more threats evolved, the industry required new types of appliances & services to meet the challenge

UTM Firewall



UTM

A single appliance

Blended threats protection

Benefits of UTM

- UTM firewalls protect inbound & outbound traffic from a multitude of threats & attack types
- Antivirus, anti-malware, & anti-spyware services could run concurrently to prevent attacks at the gateway
- Integrated Intrusion Prevention blocked the exploit of vulnerabilities
- Email filtering blocked unwanted emails like spam & email-borne threats
- Web sites & web content could be filtered & monitored from the same central command dashboard
- Control & visibility over traffic flows improved with Quality of Service enhancements & bandwidth management
- Working remotely became more convenient with the ability to connect easily to remote locations with a site-to-site VPN
- Simplification of complex networks allowed for dynamic routing, policy-based routing, & multiple Internet connections on a single secure network

Some (Popular) UTMs

Fortinet.

Check Point Next Generation Firewalls (NGFWs)

Cisco Meraki.

SonicWall.

Sophos.

WatchGuard Network Security.

Juniper.

Cisco ASA 5500-X Series.

Useful (review) sites

- https://www.itcentralstation.com/categories/firewalls
- https://www.esecurityplanet.com/products/top-utm-unified-threat-management-vendors.html
- https://www.trustradius.com/firewalls

....

Questions?