

# **Information System Security**

## **Network and application filtering**

# Summary

---

- ▶ Network concepts
- ▶ Definitions
- ▶ Firewall
- ▶ Strengths/weaknesses of packet filtering
- ▶ Rules for interconnection gateways
- ▶ HTTP proxy
- ▶ SSL VPN
- ▶ HTTP reverse proxy

# Network concepts

---

- ▶ A digital network is built with a collection of computers interconnected by physical links

- ▶ Purpose of networks

- Allow sharing resources
- Access to remote services
- Communicate (email, teleconferencing)
- Increasing the resilience



- ▶ Internet is a generic name meaning Interconnection of Networks

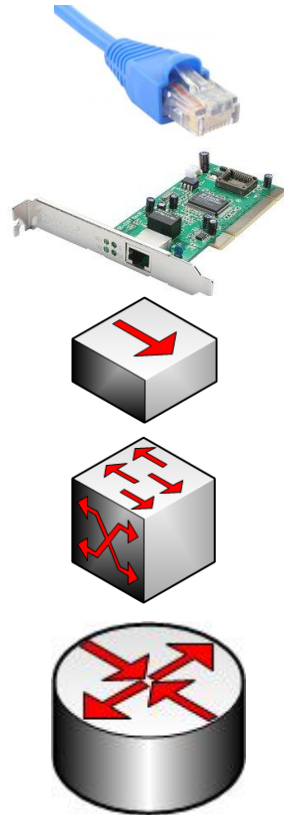
- To achieve networks interconnection, it was necessary to establish **protocols**

# Network concepts

---

## ► Computer networks are made up of hardware:

- **Cable:** Ethernet cable is the cable used to connect computers together
- **Network Interface Controller (NIC):** the NIC is the interface through which passes all information to send and receive network
- **Hub :** it sends all that it receives on one port to all other ports (it does not read the information)
- **Switch :** it sends that it receives only to the recipient (based on MAC address)
- **Router:** it works as a switch but it allows the connection between different networks (eg Internet box). It is based on the MAC address and IP address.



# Network concepts

---

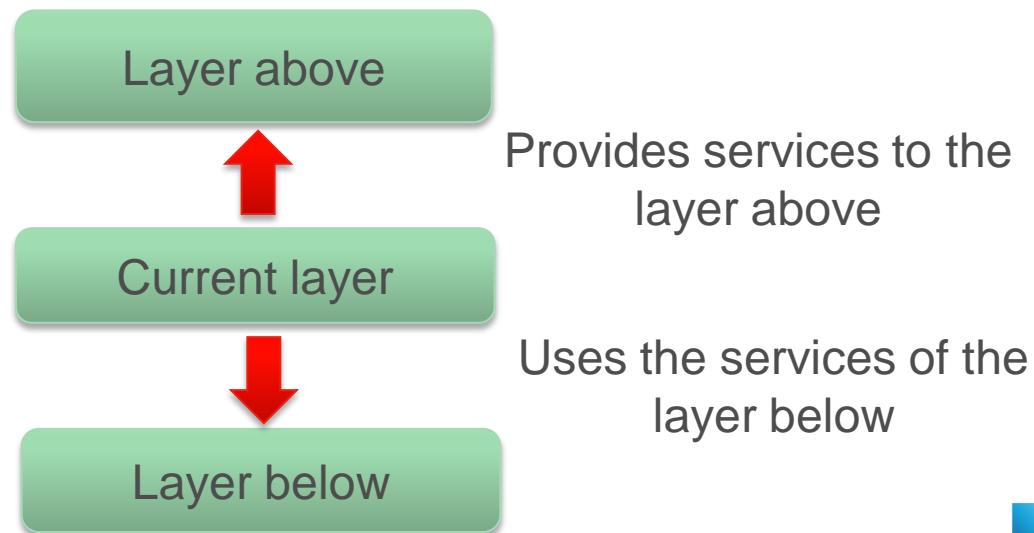
- ▶ A protocol is a set of steps to allow communication between multiple computers or devices connected in a network
- ▶ Before everything is standardized, each manufacturer had its architecture and it was not easy to communicate between different devices
- ▶ To avoid that each manufacturer has its own protocol and connector, ISO has developed a reference model called OSI (Open Systems Interconnection)
  - This model describes the concepts used to standardize systems interconnection



# OSI model

---

- ▀ **Protocol:** set of rules that define how communication occurs in a network
- ▀ The OSI (Open Systems Interconnection) is a standard that segments the communications process into 7 layers
- ▀ Each OSI layer communicates with the layer above and below it



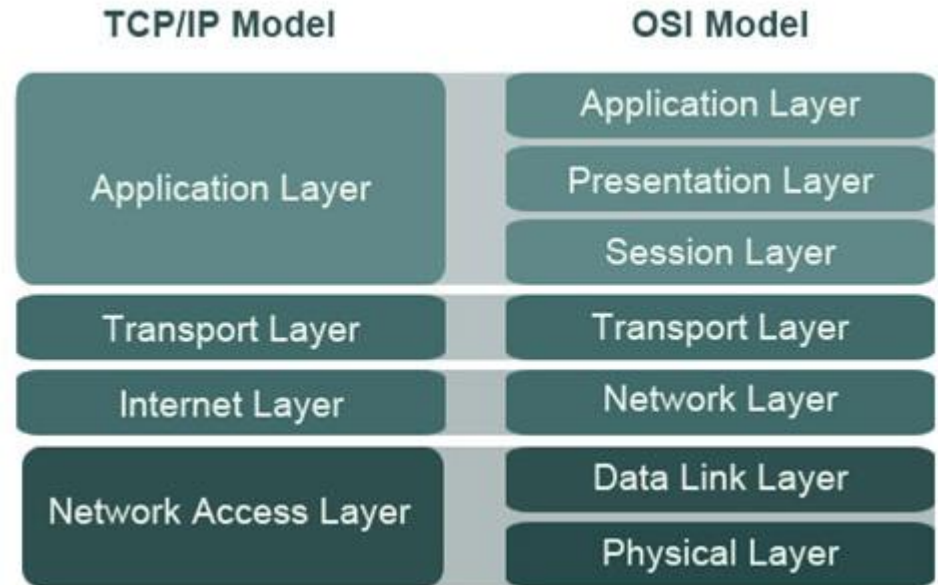
# OSI model

---

Position in OSI model	Layer name	Layer role
7	Application	Contact point with network services.
6	Presentation	It takes care of anything related to the presentation of data: format, encoding, etc.
5	Session	Responsible for initializing the session, its management and its closure.
4	Transport	Choice of transmission protocol and preparation for sending data. It specifies the port number used by the sending application and port number of the receiving application. It splits data into multiple sequences (or segments).
3	Network	Logical connection between hosts. It deals with everything related to the identification and routing in the network.
2	Data link	Establishing a physical connection between hosts. Splits data into multiple frames.
1	Physical	Frames conversion in bits and physical transmission of data on the media.

# Suite of TCP/IP protocols

- ▶ The TCP/IP suite is the set of protocols used for data transfer over the internet
- ▶ The OSI model is the most theoretical and the easiest to understand, but the TCP/IP model is the most used in practice
- ▶ Examples of TCP/IP protocols:

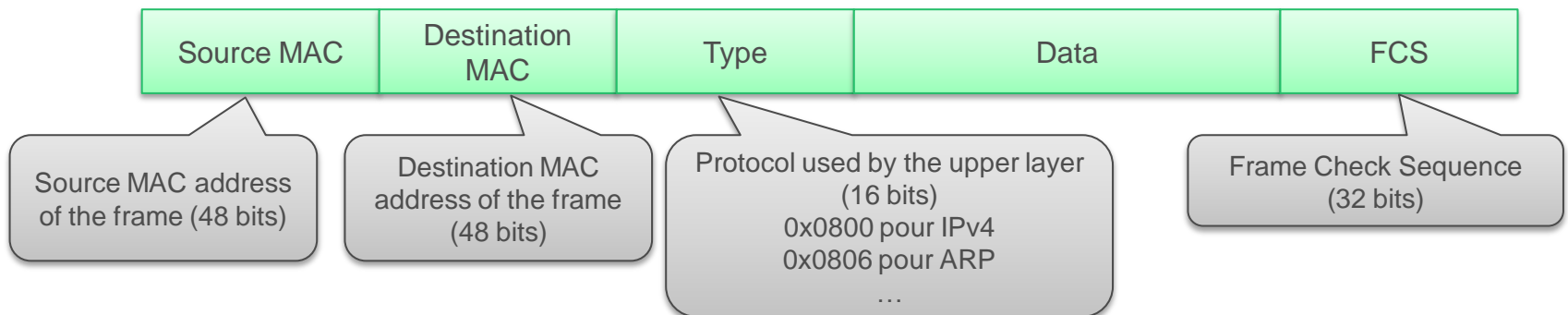


Layer	Protocols
Application	HTTP, FTP, DNS
Transport	TCP, UDP
Internet	IP
Link	Ethernet



# Layer 2 : Data link layer

- ▶ **Role: transmit data between directly connected equipment**
- ▶ **On a network, there are often several machines connected, we have to be able to differentiate them one from the others**
  - We use the MAC addresses that are encoded on the network card
- ▶ **The Ethernet protocol defines the rules allowing the machines to discuss**
- ▶ **Ethernet Frame :**



# Layer 3 : Network layer

---

- ▶ **Role: routing information from one network to another**

- ▶ **The networks are interconnected by routers**



- Routers have a connection on each network
- Since all networks are not interconnected, it is often necessary to use intermediate networks

- ▶ **To identify the machines we use the IP addresses**

- Layer 2 **MAC addressing** identifies machines **ON THE SAME NETWORK**
- Layer 3 **IP addressing** allows the machines to be addressed **ON SEPARATE NETWORKS**

- ▶ **The IP address contains a network address and a machine address**

- The subnet mask is a separator between the network portion and the machine part of an IP address

# Reserved range

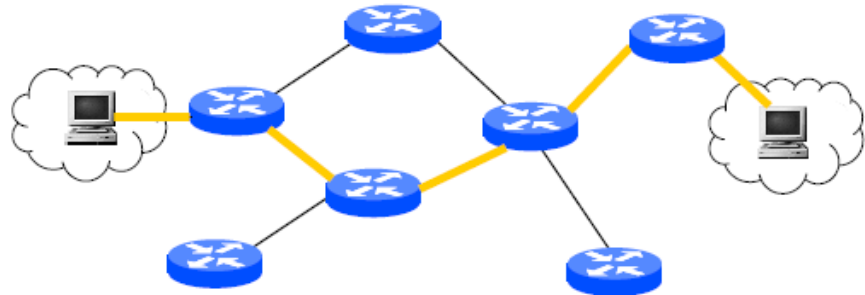
---

- ▶ **Some address ranges have been reserved for local use**
- ▶ **To configure a LAN when there is no public address range available, you must use these private address ranges**
  - 10.0.0.0/255.0.0.0 (more than 16 million addresses available)
  - 192.168.0.0/255.255.0.0 (close to 65,000 addresses)
  - 172.16.0.0/255.240.0.0 (more than one million addresses)
- ▶ **Loopback addresses (localhost) : 127.0.0.0/255.0.0.0**
- ▶ **Private address ranges are not routed over the Internet**
- ▶ **The ranges can be divided into several subnets thanks to the mask (part of address after the /)**
  - The ranges are generally cut according to the number of machines which need to communicate directly

# Internet Protocol

---

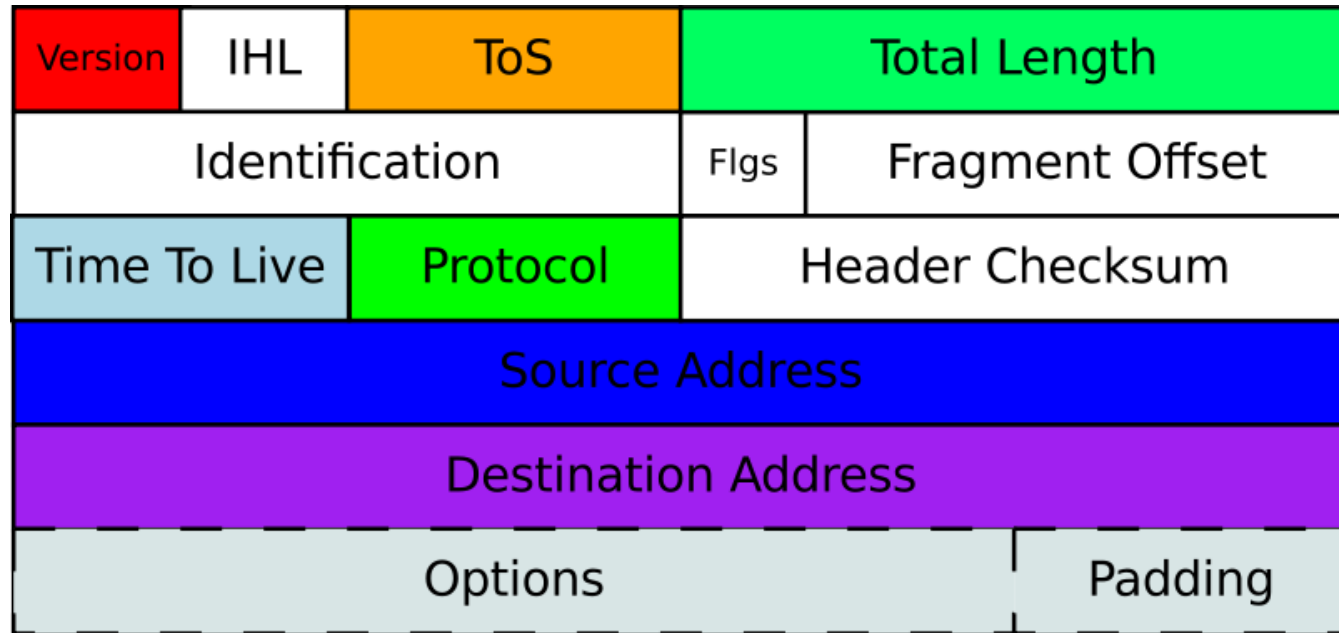
- ▶ IP protocols are part of the network layer of the OSI model
- ▶ IP routing protocols provide the best-effort delivery of packets
- ▶ IP protocols are considered "unreliable":
  - data corruption
  - arrival order of the packets
  - packet loss or destruction
  - duplication of packets
- ▶ IPv4 is the most used protocol



# IPv4

---

- ▶ One or more IP addresses encoded in 32 bits is allocated to each interface of a machine that wants to communicate
- ▶ In theory there are  $2^{32}$  addresses available (4 billion)
- ▶ The IPv4 header specifically adds the source and destination addresses



# Layer 4 : Transport layer

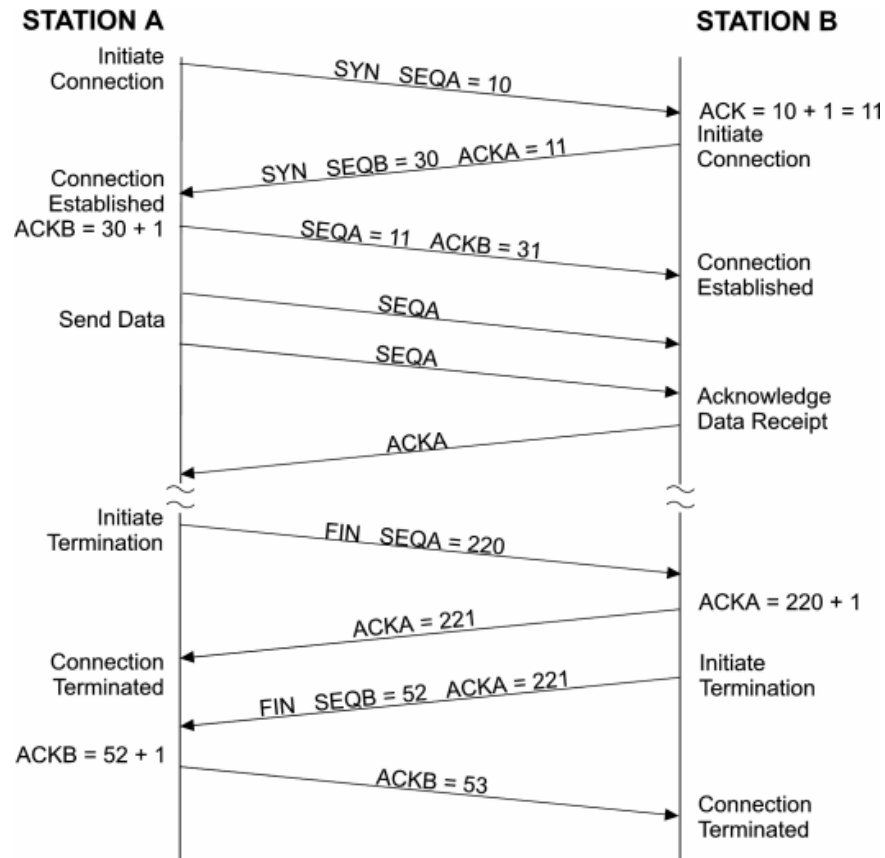
---

- ▶ The TCP segment specifically adds source port, destination port and sequence and acknowledgment numbers of segment
- ▶ TCP as UDP, use port numbers to identify applications
- ▶ Well known applications running as a server and listening for connections typically use the same ports:
  - HTTP: port 80
  - HTTPS: port 443
  - FTP: port 21

# Layer 4 : Transport layer

## Communication modes:

- TCP (Transmission Control Protocol) = connected mode (phonecall)
- UDP (User Datagram Protocol) = not connected mode (sending mail)



# Layer 4 : Transport layer

---

## ► TCP advantage

- Integrity (acknowledgment and manages the retransmission of lost segments)
- Flow control (changing the window size to avoid overloading the destination)

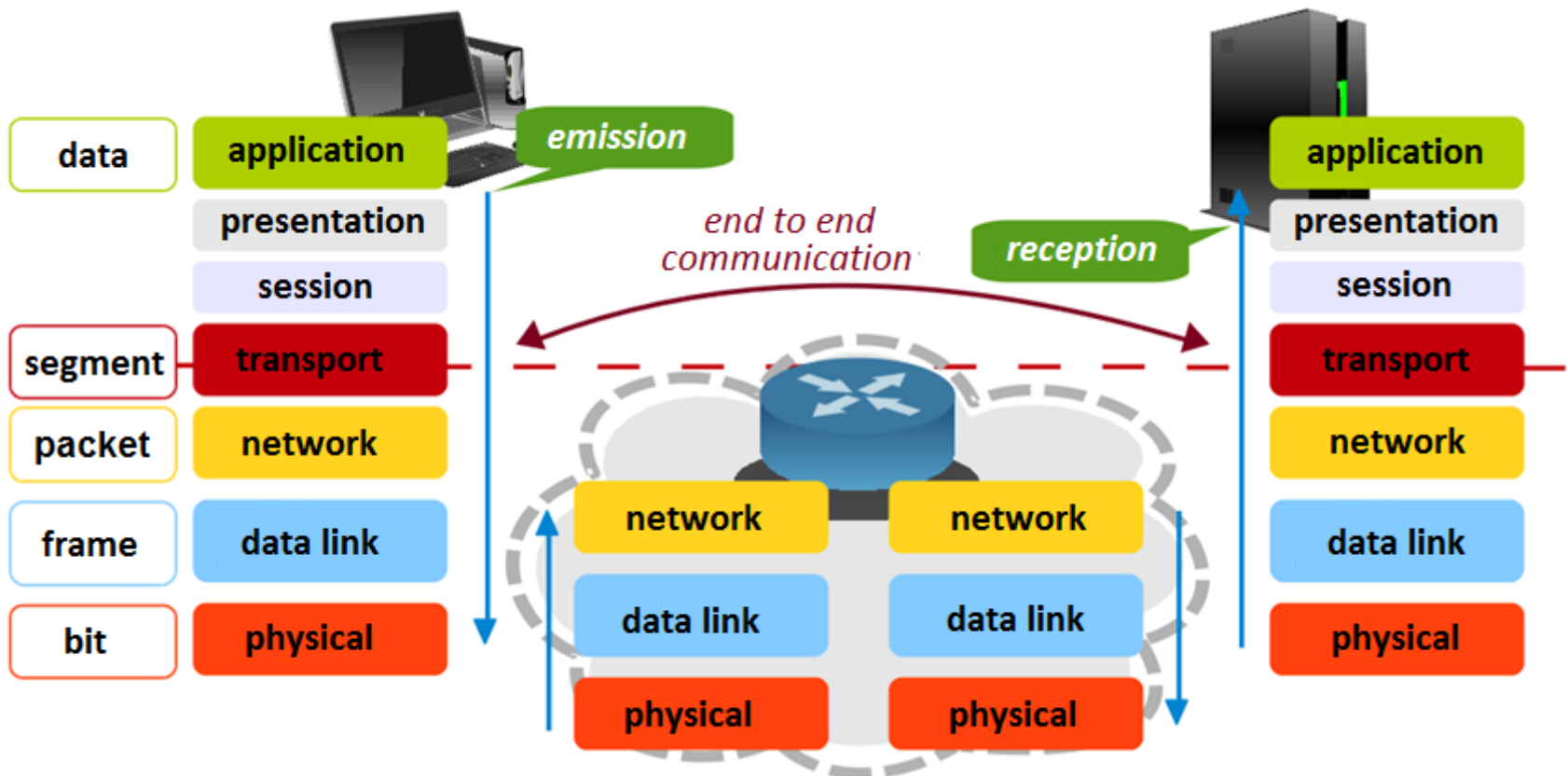
## ► UDP advantage

- Quick (no acknowledgment or connection establishment)
- Simple (one message)
- Inexpensive in resources



# Example of data transmission

- During transmission of data from one machine to another, each layer of the OSI model adds its complement and sends to the adjacent layer



# Definitions

---

## ■ SSH

- SSH or Secure Shell, is a secure communication protocol
- The connection protocol requires an encryption key exchange at the beginning of connection
- It allows to remotely connect to a computer to get a shell or command line
- It uses TCP port 22 (IANA)
- Tunnels can be made from any ports but SSH is often used to create tunnels

# Definitions

---

## VPN

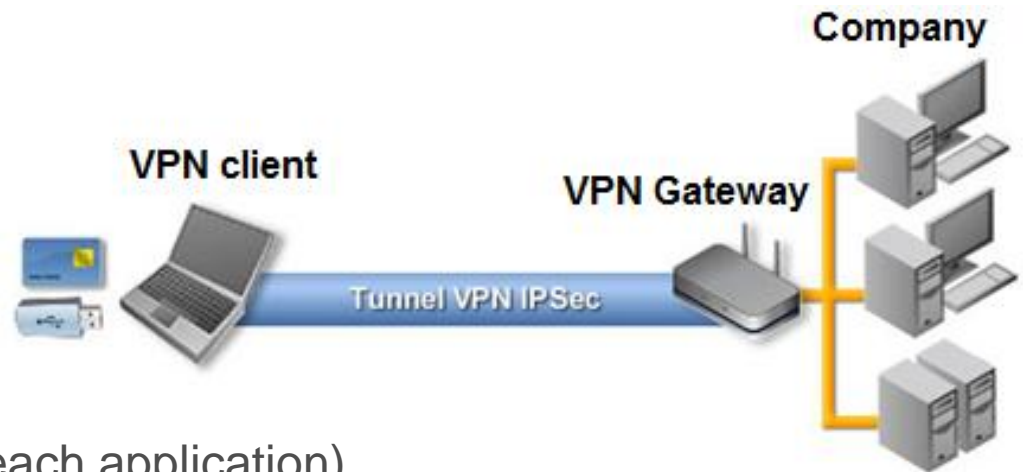
- Virtual Private Network: system for creating a direct link between remote computers
- Computers connected to a VPN are on the same local network (virtual)
- A VPN enables access to remote computers as if they were physically in the local network
  - ✓ Including access to the corporate network
- VPN connections are not necessarily encrypted
- Example: GRE protocol (Generic Routing Encapsulation) used to avoid connectivity problems



# Definitions

## VPN IPSec

- Internet Protocol Security: A set of protocols using algorithms for a secure transport of data over an IP network
- Independent of the applications (requires no configuration by the user for each application)
- Objective: Authenticate and encrypt data
  - ✓ The stream can only be understood by the final recipient (confidentiality)
  - ✓ Modification of data by intermediaries will be impossible (integrity)



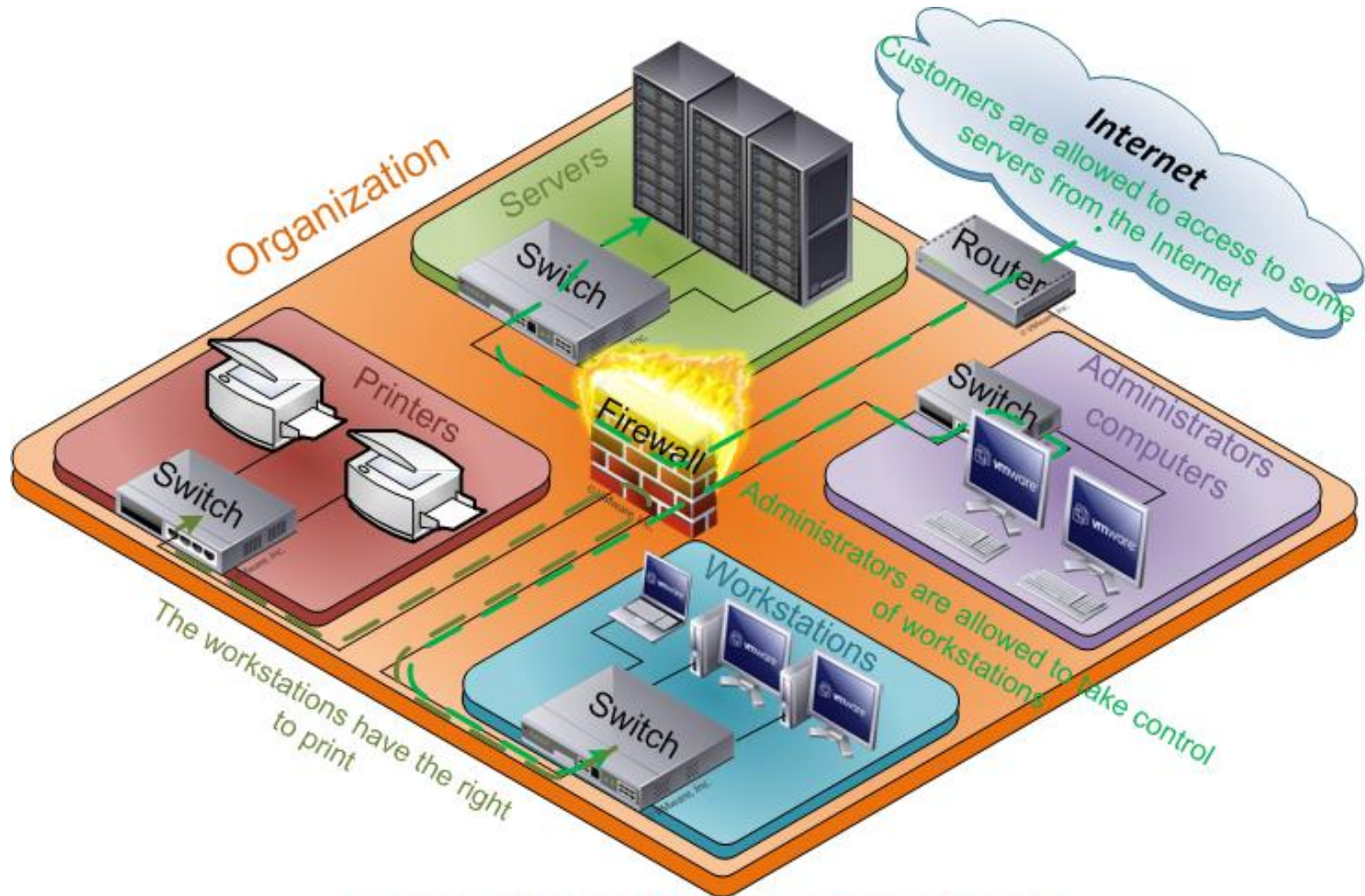
# Control the network

---

## ► Secure the internal network:

- **Network partitioning and filtering** between subnets (function, sensitivity and homogeneous level of security): user workstations, administrators desktops, servers, printers ...
  - ✓ This function is provided by the firewall
- **Strict control of entry / exit points** between networks and outside : application relay with authentication and logging
  - ✓ This function is performed by proxy or SSL VPN.
- **Traffic control and logging** of packets rejected by filters

# Firewall within a network example



Everything which is not explicetely allowed is forbidden









# Firewall

---

- ▶ **The firewall uses IP packet information (source and destination addresses) and those of the segment (source and destination ports) to ensure compliance with a security policy**
- ▶ **To allow visit of web servers from the internal, we "open" TCP port 80 (which corresponds to HTTP)**
  - On a static firewall, we configure two rules:
    - ✓ allow <any internal source> to <any external source on port 80>
    - ✓ allow <any external source on port 80> to <any internal source> (response)
  - When we request a connection, the system use a free port generally between 1024 and 65535 (the choice is random)
  - The problem of static firewall is that the second rule therefore opens all ports between 1024 and 65535:
    - ✓ allow <any external source:80> to <all internal sources:1024-65535>

# Stateful firewall

- ▶ To avoid the above problem, we use a stateful firewall which keeps record of current connections
- ▶ In this type of firewall, we only configure one rule by setting into the source the machine (or network) that establishes the connection and in destination the other machine (or network) with the desired service
- ▶ To allow the visit of a web server from the internal :

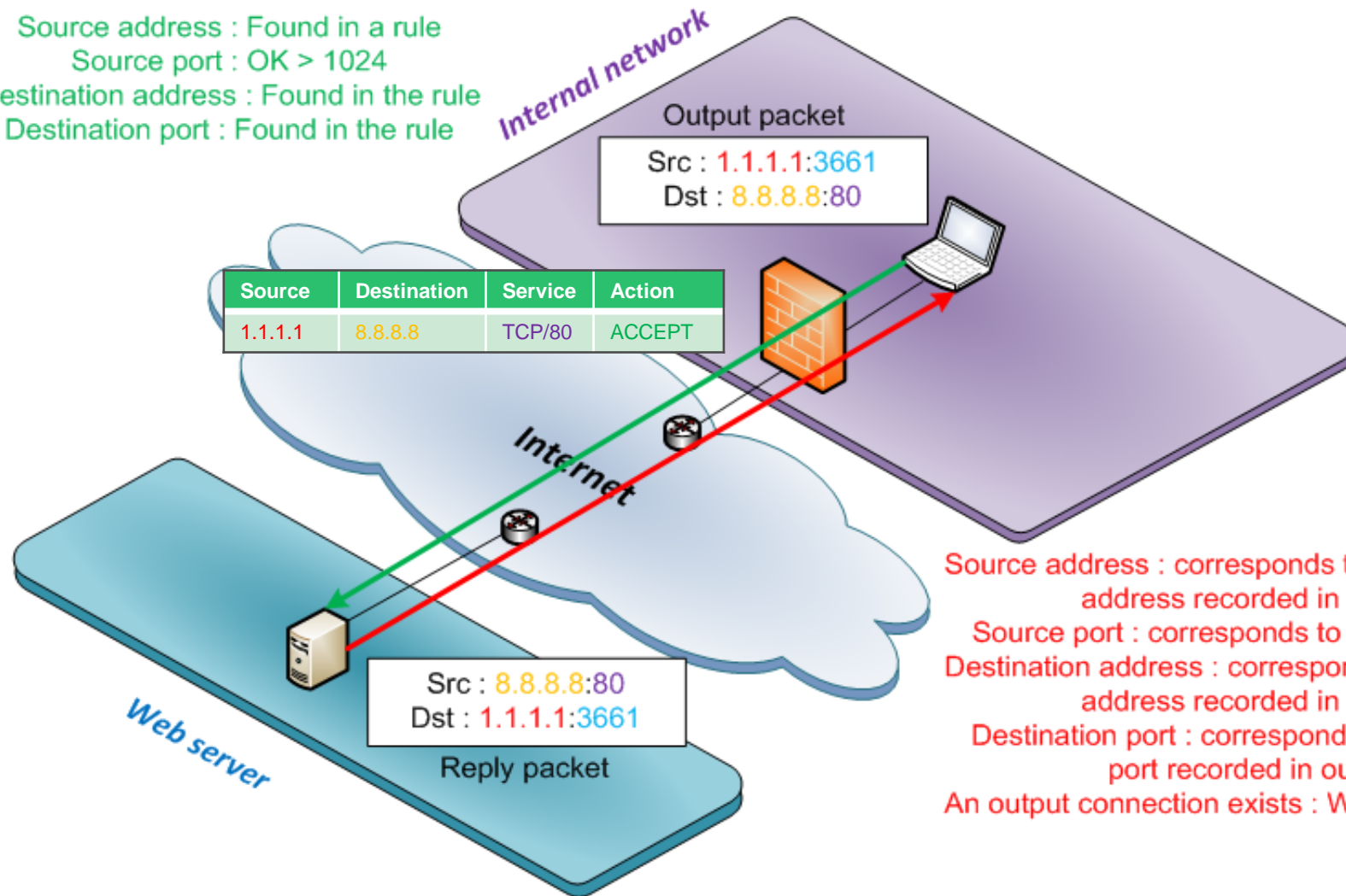
No.	Hits	Name	Source	Destination	Service	Action	Track	Time
1	 0	Consultation Internet	 InternalNet	 All_Internet	 https  http	 accept	 Log	 Office_hour

- ▶ A stateful firewall keeps track of current connections to allow only compatible packets of existing connections or packets in rules



# Firewall

Source address : Found in a rule  
Source port : OK > 1024  
Destination address : Found in the rule  
Destination port : Found in the rule



Source address : corresponds to the destination address recorded in output  
Source port : corresponds to the output port  
Destination address : corresponds to the source address recorded in output  
Destination port : corresponds to the source port recorded in output  
An output connection exists : We allow the reply

# Firewall operating

- ▶ Firewall must cut the network (to prevent a flow does not pass through the firewall)
- ▶ A firewall contains a set of rules allowing or prohibiting communications between machines
  - The rules are read by the firewall from top to bottom
  - For each rule, the firewall checks whether the packet matches the rule. If this is not the case, it goes to the next rule







Example for a packet whose source IP 192.168.10.1 and for destination the public IP address 10.10.10.10 on port TCP/22 (ssh) :

No.	Hits	Name	Source	Destination	VPN	Service	Action
1	0		IP_192.168.10.1	IP_172.16.10.15	Any Traffic	<u>TCP</u> ssh	accept
2	0		IP_192.168.10.1	IP_10.10.10.10	Any Traffic	<u>TCP</u> http	accept
3	0		IP_192.168.10.1	IP_10.10.10.10	Any Traffic	<u>TCP</u> ssh	accept
4	0		Any	Any	Any Traffic	Any	drop

# Decision of the filter system

---

- ▶ The firewall must be configured to reject what is not explicitly allowed (clean-up rule)

No.	Hits	Name	Source	Destination	VPN	Service	Action
1	 0		 Any	 Any	 Any Traffi	 Any	 drop

- ▶ Every need for communication between two machines must be studied and then added to the firewall
- ▶ Prohibited communications may be rejected in two ways:
  - Explicitly with an error message returned to sender
  - Silently slowing ports scans
- ▶ In all cases, the actions are registered (logging)

# Strengths of packet filtering

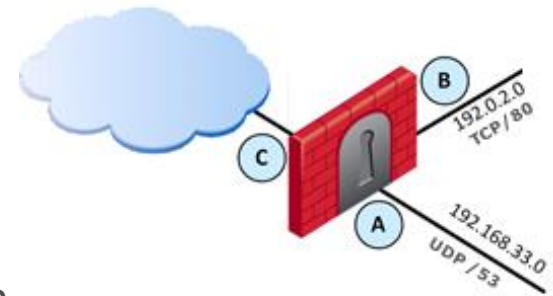
---

- ▶ Reduction of servers exposure in one place (the firewall)
- ▶ Transparency: do not ask the user collaboration
- ▶ Available on many devices
- ▶ Generally fast flow processing
- ▶ First part of an intrusion detection architecture

# Firewall (summary)

## ► Firewall: control traffic between different areas of trust

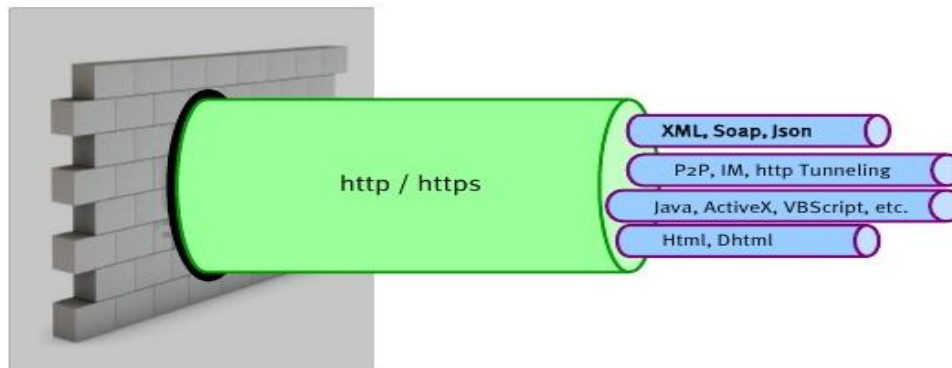
- Filters the data flow passing through it
- The main criteria: Source and destination of the packet (IP address, TCP or UDP ports)
- Corporate firewalls are "stateful": If a rule allows a packet to pass, it will automatically allow the answer to pass without writing the rule
  - ✓ A rule allows a computer to join a server on TCP port 80 (HTTP)
  - ✓ The response from server to client requires no rule → Firewall has memorized a request was sent and passes the answer



# Network filtering issue

---

- ▶ Firewalls filter necessary traffic based on IP addresses and ports TCP or UDP
- ▶ Problem: any service can listen on any port (SSH can listen on port 80, etc.)
- ▶ It is necessary to validate the application protocol (HTTP on port 80, SSH on port 22, etc.)
- ▶ This validation requires application filters

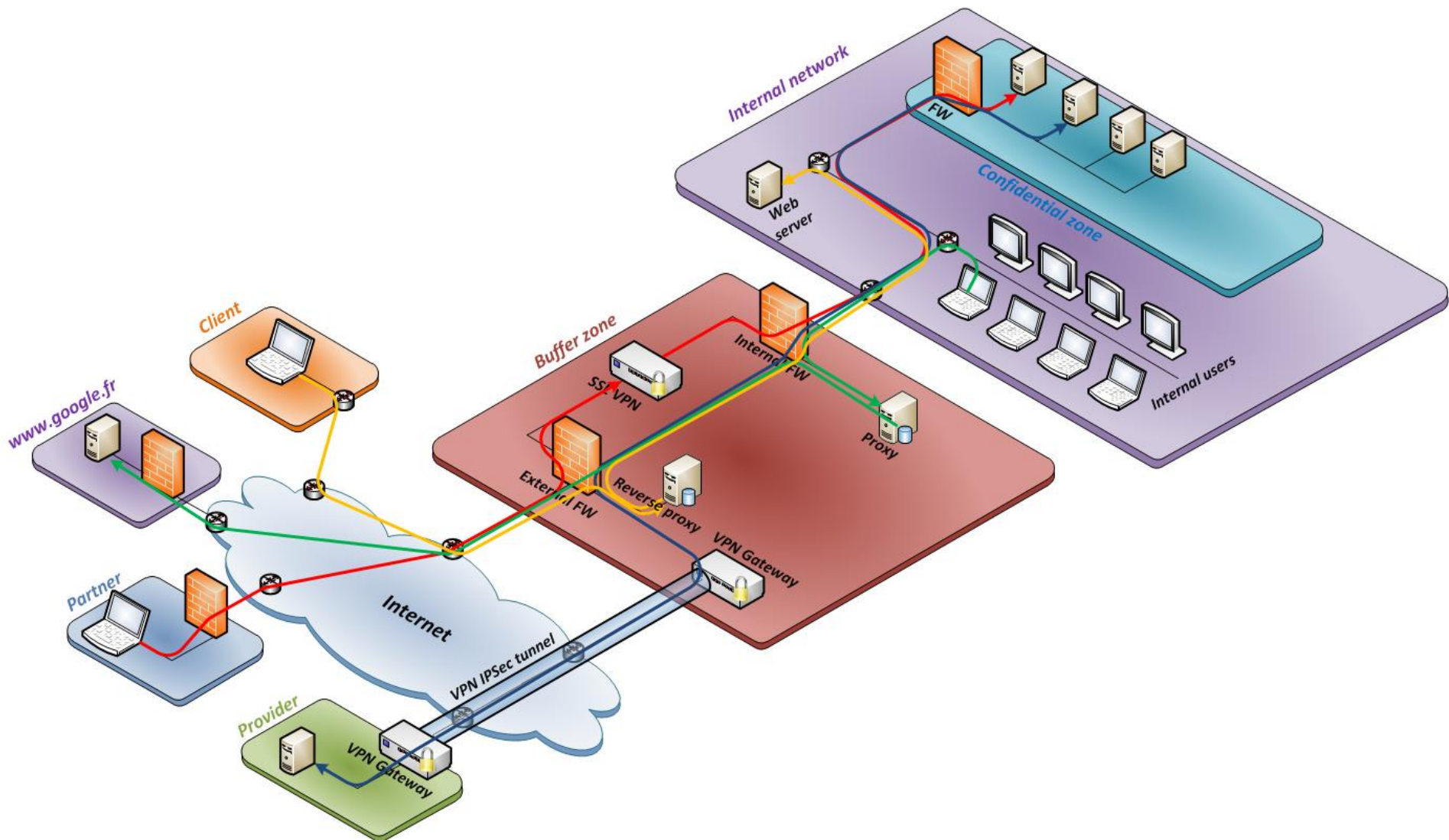


# Rules for interconnection gateways

---

- ▶ **Break flow between LAN and WAN**
- ▶ **Reverse the direction of flow and /or application layer analysis**
- ▶ **Partition functions**
  - ✓ To limit the risks and consequences of an attack
- ▶ **Diversify the technologies used**
  - ✓ To the extent permitted by the maintainability
- ▶ **Make the appropriate security updates**
- ▶ **Monitor system logs**

# Example of secure architecture



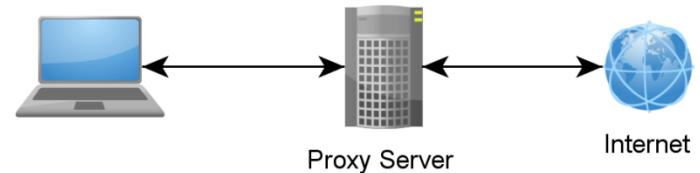


# Definitions

---

## Proxy

- A proxy server is originally a machine acting as an intermediary between the computers of a local network and internet.
- The proxy is involved in network security
- Mainly used for the Web (HTTP proxy) and emails
- There are proxy servers for each application protocol (HTTP, SMTP...)



## Reverse Proxy

- Proxy server which relay requests coming from the Internet to the internal network
- It's used to protect the internal web server

# Proxy operation

1. Client browser connects to proxy (port 3128, 8080, etc.)

2. Sending of HTTP request :

GET / HTTP/1.1

Host: www.google.fr

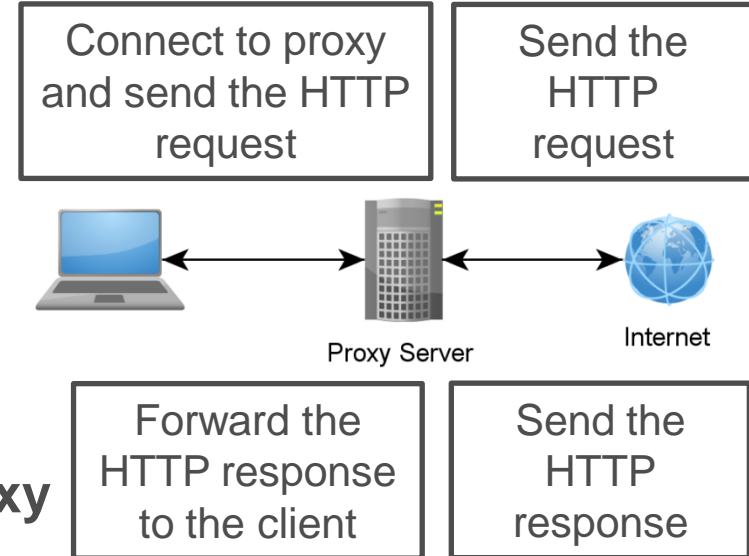
3. Proxy connection to the specified server

4. Sending the HTTP request by the proxy

5. HTTP response received by the proxy

6. Forwarding the response from the proxy to client

➤ DNS request made by the proxy (prevents disclosure of internal IPs)



# Functions of HTTP proxy

---

## ► Access logging

- Detection of abnormal behavior and traceability in case of anomalies
- Compliance with legislation

## ► User authentication and filtering profiles

- Transparent authentication using Active Directory
- Example: download of executable files only for administrators

## ► Validation of compliance to standard (RFC, etc.)

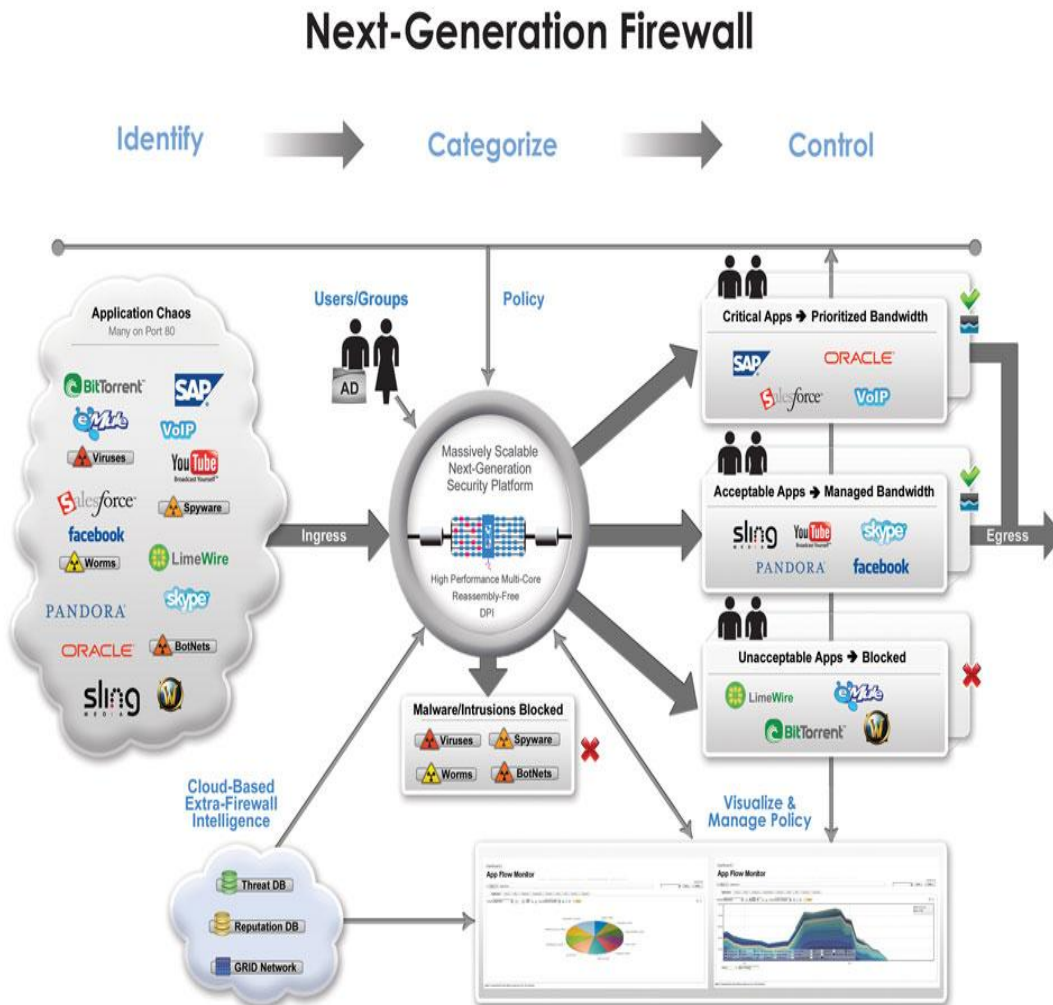
- It can block some legitimate connection which not corresponds to the RFC

## ► Filtering

- URL: Using black or white lists
- Content: keyword lists with weighting, anti-virus filtering and various controls (specific extensions, javascript)

## ► Cache (faster browsing)

# Next-Generation Firewall



- **NextGen firewall (NGFW)** is able to filter traffic on application layer level (layer 5 to 7)
- It integrates functionality of :
  - ✓ **IPS** (Intrusion Prevention System)
  - ✓ **Proxy** in order to allow or forbid some domains or applications
  - ✓ **Signature system** to detect malwares (antivirus function)
- But, all the market solutions can be bypassed by attacks ([NSS Labs](#) test)
- This device becomes a point of failure in the information system

# Intrusion Detection System (IDS)

---

- ▶ **An Intrusion Detection System is a system capable of detecting malicious activities or policy violations on a network**
  - It helps administrators and management to make decisions
- ▶ **Some systems may attempt to stop an intrusion : they are called Intrusion Prevention System (IPS)**
- ▶ **IDS focused on identifying possible incidents, logging information about them, and reporting attempts**
  - IDS is like an antivirus on the network and recognize the following signals:
    - ✓ Denial-of-Service
    - ✓ Backdoor
    - ✓ Trojans
    - ✓ Buffer overflows

# Definitions

---

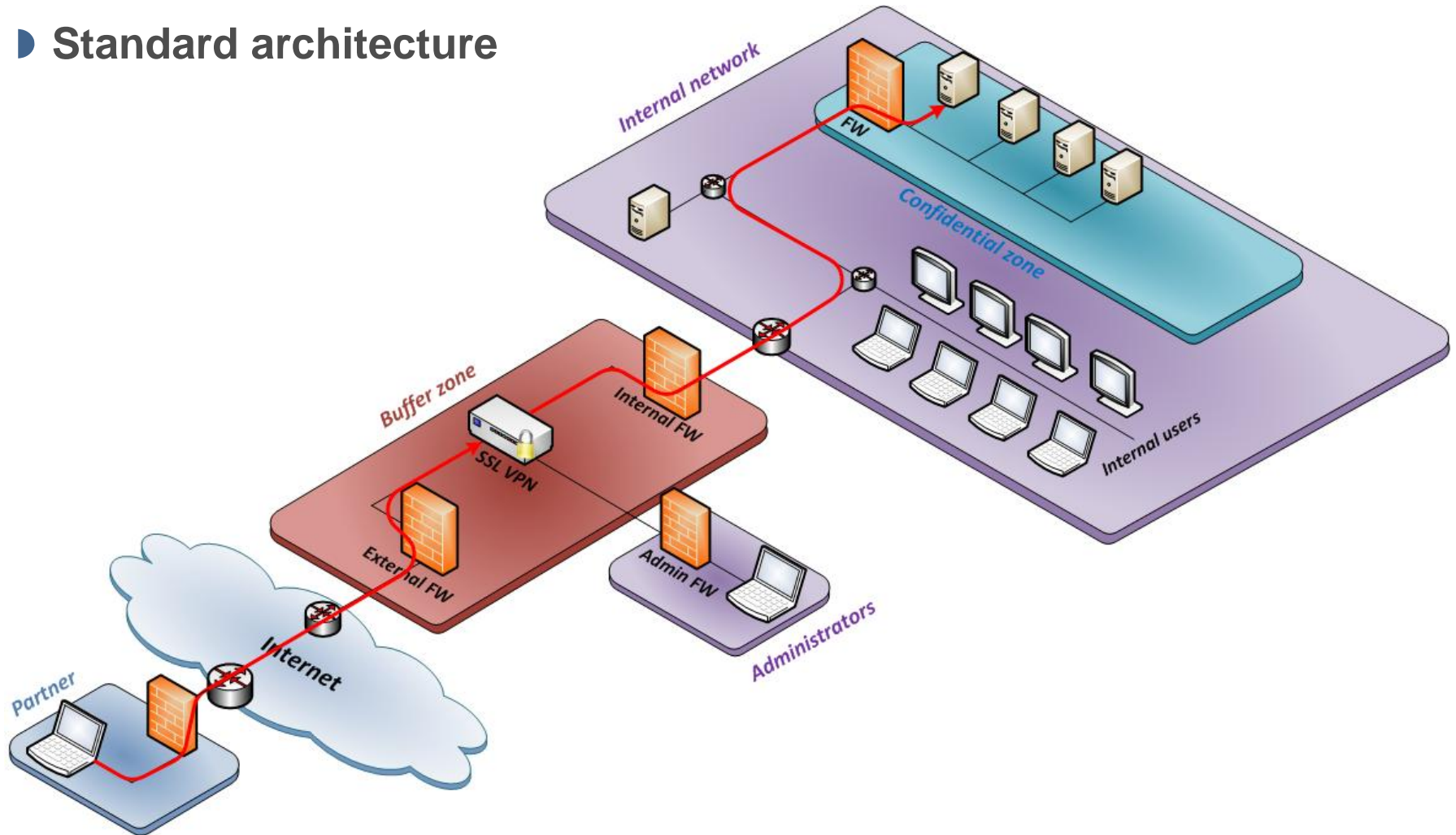
## ■ SSL VPN



- Secure Sockets Layer Virtual Private Network
- Is a very particular type of virtual private network (VPN), it uses a protocol designed to transport application data (SSL) to build a VPN
- Accessible from a web browser via HTTPS (using TLS)
- It allows users to access to corporate network from an Internet connection in the same conditions as if they were in the corporate network
- The main advantage of this protocol is that it uses HTTPS port 443 which is generally open in every networks
- It allows access logging

# SSL VPN

## Standard architecture



# Reverse proxy HTTP

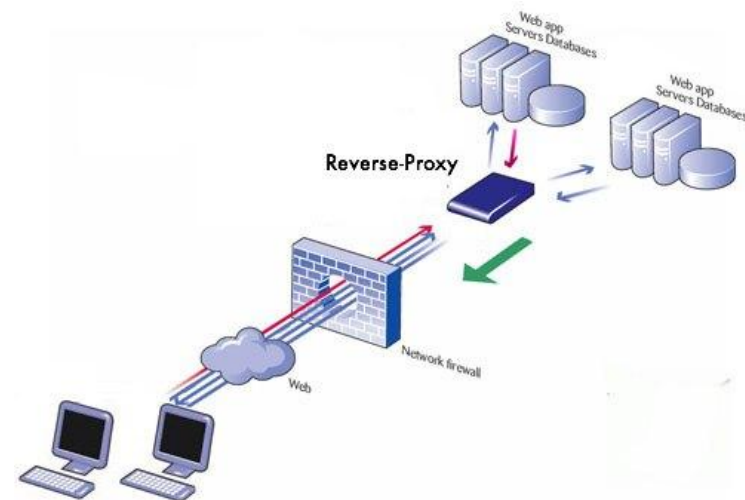
## ► Functions of filtering and URLs standardization

- Compliance of application flows to the HTTP standard
- Compliance of application flows to the security policy
  - ✓ Filtering of the full HTTP request (headers and body) based on patterns (regular expressions)
  - ✓ Filtering the HTTP response (black list of keywords, removal of error which gives server information, etc.)

## ► Function of authentication (verification of strong authentication before reaching the server)

## ► Function of compression and load balancer

## ► Function of logging (GET, POST)





# Web Application Firewall (WAF)

- ▶ WAF is a reverse-proxy applying rules allowing to protect an application or a service
- ▶ WAF works on application layer (layer 5 to 7 in OSI model)
  - It inspects the traffic content and can block some specific content
  - Rules implemented in WAF protect from application attacks such as Cross-Site Scripting (XSS) and SQL injection
- ▶ WAF can intercept SSL/TLS and handle authentication for the web server
- ▶ To be efficient, WAF should be personalized indicating pages and fields existing in the application in order to create a white list

