Université Grenoble Alpes

Course on “security of information systems”

4. Security technologies (security of the infrastructures)

4.1 Simple components: switches, bridges and gateways
4.2 Routers: Filtering of packets (ACL)
4.3 Firewalls
4.2.1 Inspection of packets (SPI) (firewalls)
4.2.2 NAT function (network address translation)
4.4 Proxy firewalls
4.5 DMZ (demilitarized zone, perimetric security)

Introduction

Lorsqu'ils ont été conçus, le protocole IP et les protocoles associés (TCP, UDP, ICMP, routage…) n'ont pas pris en compte la sécurité

•« Concept sécurité » inconnu à l'époque, personne n'imaginait que ces protocoles pourraient être détournés à des fins malveillantes ;

•**Aucun mécanisme de sécurité n'est donc implémenté au sein de ces protocoles.**

Quelques exemples de faiblesses de ces protocoles

•**Absence d'authentification des émetteurs et récepteurs** d'un datagramme : usurpation d'adresse IP possible ;

•**Absence de chiffrement des données**, celles-ci sont donc transmises en clair. Un hacker positionné sur un réseau peut donc écouter les connexions et accéder aux données ;

•**Le routage des datagrammes peut être modifié** de façon à rediriger les datagrammes vers un autre destinataire ;

•Note : l'exploitation de ces faiblesses nécessite des prérequis techniques, i.e. elles ne sont pas systématiquement applicables à tous les réseaux.

Les diapositives suivantes illustrent ces faiblesses.

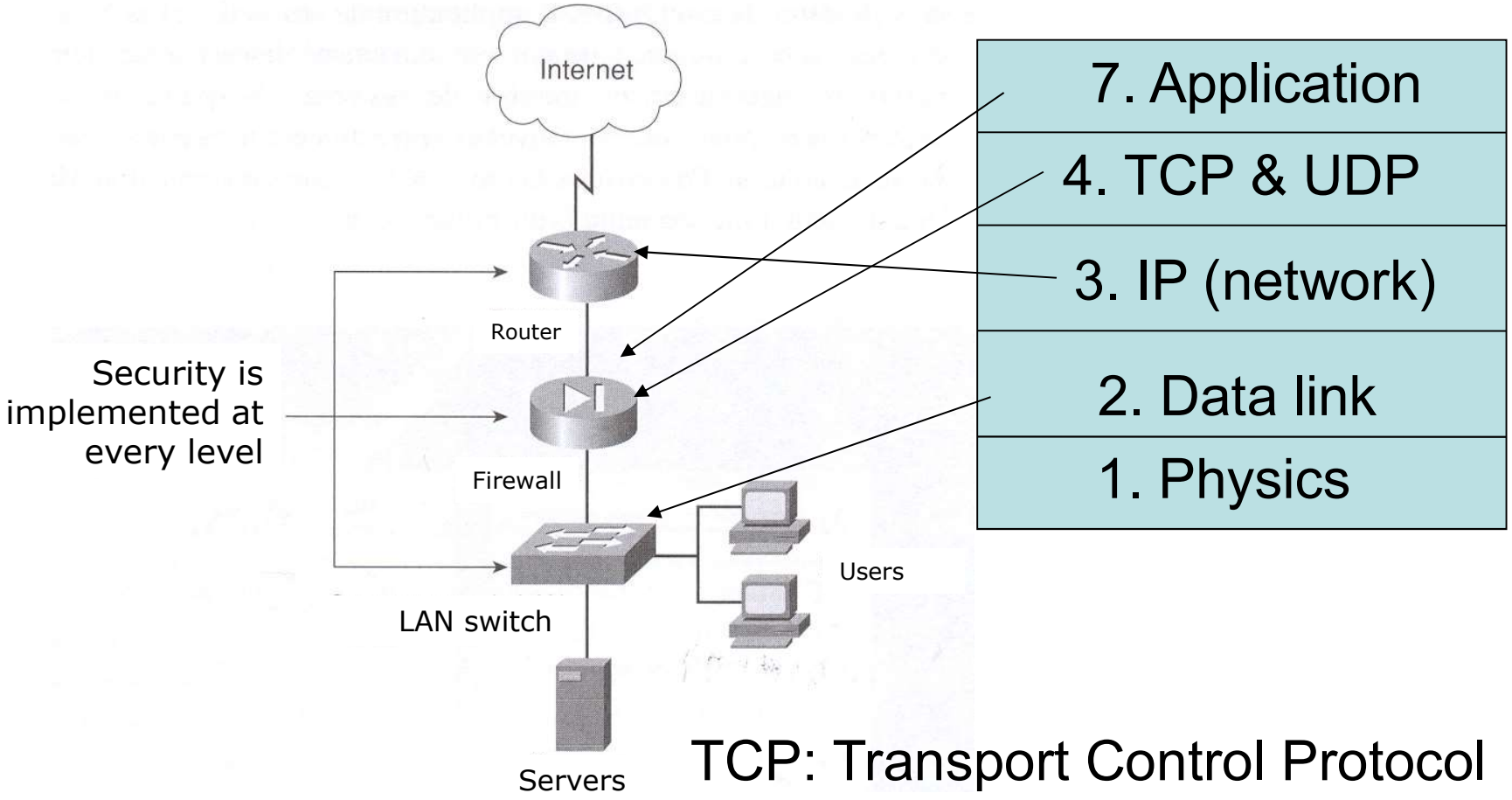
Introduction

Ainsi, il est nécessaire de **mettre en œuvre des mécanismes de sécurité complémentaires** afin de réduire et maitriser les risques émanant des protocoles historiques régissant les réseaux.

Exemple de mécanismes :

- Chiffrement des communications ;
- Authentification des entités ;
- Cloisonnement réseau ;
- Filtrage ;
- Dimensionnement adapté des infrastructures ;
- Règles de renforcement des configurations des équipements ;
- Supervision des équipements ;
- etc.

security in layers (TCP/IP layers) implemented in several points of the network



TCP: Transport Control Protocol
UDP: User Datagram Protocol

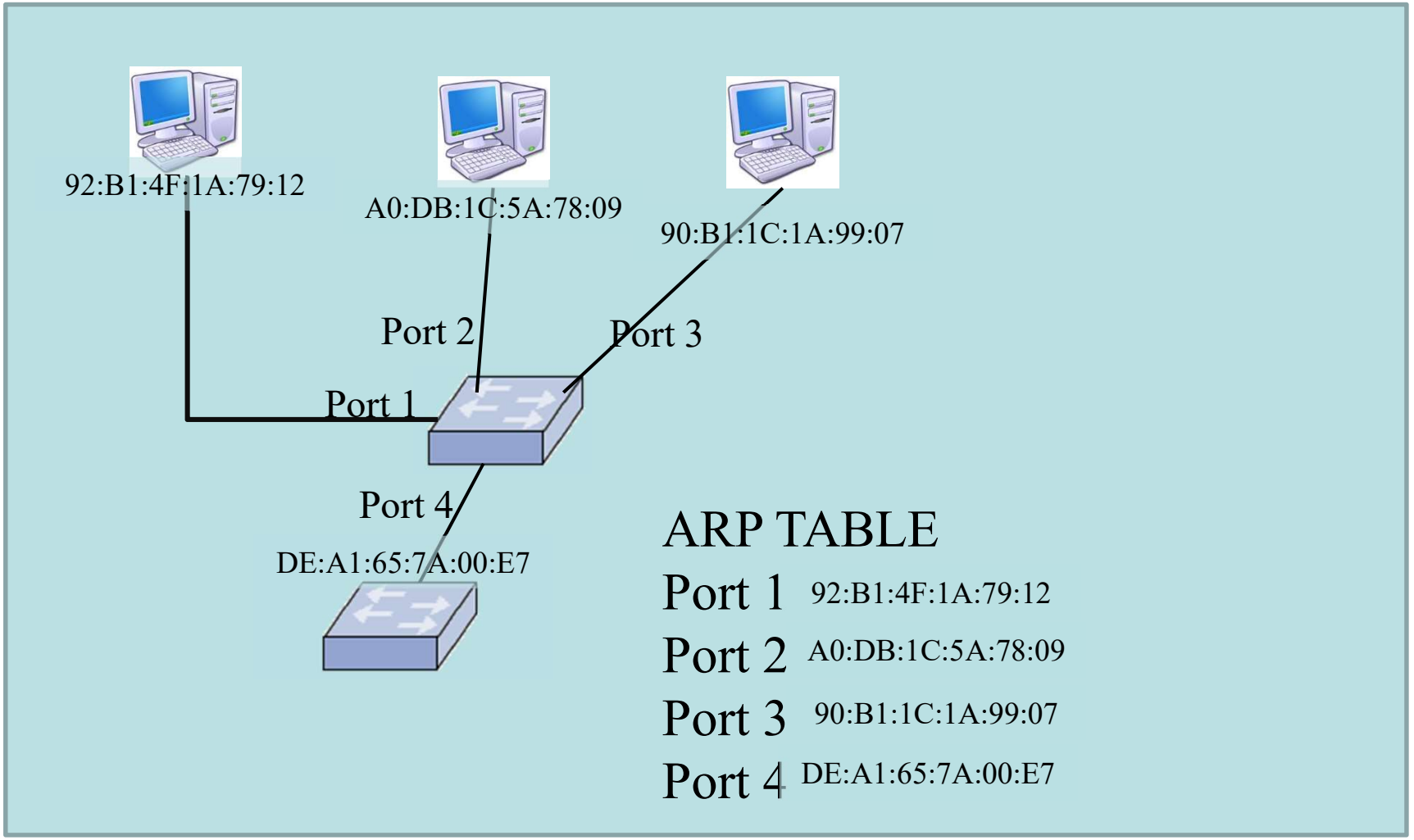
Université Grenoble Alpes

4.1 Simple components: switches, bridges and gateways

4.1.1 Switch

4.1.3 Gateway

4.1.1 Switch


92:B1:4F:1A:79:12
A0:DB:1C:5A:78:09
90:B1:1C:1A:99:07
Port 2
Port 3
Port 1
Port 4
DE:A1:65:7A:00:E7
ARP TABLE
Port 1 92:B1:4F:1A:79:12
Port 2 A0:DB:1C:5A:78:09
Port 3 90:B1:1C:1A:99:07
Port 4 DE:A1:65:7A:00:E7

4.1.1 Switch

- Use
  - 2nd layer of the OSI model
  - Link the stations together
  - Allow to increase the flow
    - Collision detection (avoidance)
    - Allow to use a full-duplex mode
- Functioning
  - The switch learns the MAC addresses (protocol ARP: Address Resolution Protocol)
    - Record the source addresses of the packets
    - Send the packet directly to the destination port (if the destination address is known)
    - If not => send to all the other ports

4.1.1 Switch: by-pass

- False ARP announcements
- Modification of the MAC address
  - Linux: ifconfig
  - Windows: ipconfig (« *Propriétés de la carte réseau* » / properties of the network card)
  - Consequences
    - All the packets are entering on the network
- Convert the switch as a hub
  - Huge sending of ARP announcements
  - Saturation of the table, learning begins
  - Consequences
    - Denial of service
- Possibility to control the complete network
  - Access to all the MAC addresses

4.1.1 Commutateur (switch) : Countermeasures

Segmenting the physical network

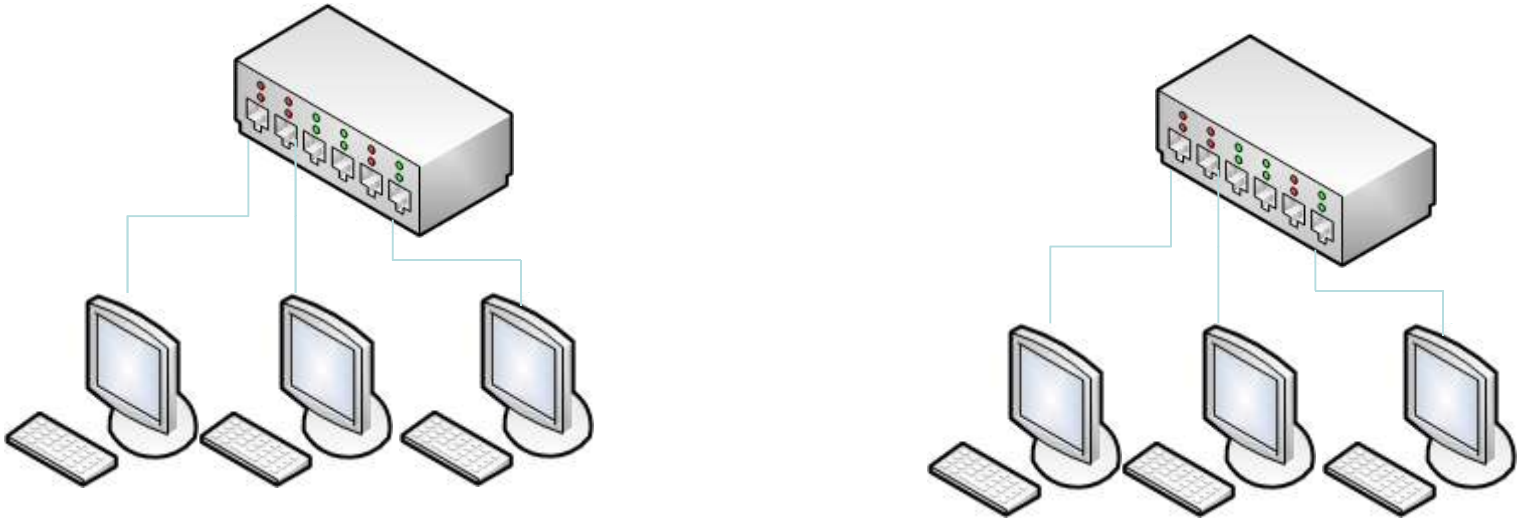
A major principle of security is that of the **least privilege**: Access rights to a resource should be given only to those persons / entities with a legitimate need to access it.

Applied to the network domain, **segmentation is used to separate** the network into different zones.

The access rights to these zones must then be **filtered** in order to allow only the necessary flows between each zone.

4.1.1 Commutateur (switch) : Contre-mesures

There are several techniques for segmentation. The most obvious technique: Implement two separate unconnected networks.



Implementation of two different physical networks, not connected.

Advantage: **perfect network sealing** (no communication possible between these two zones).

Disadvantage: suitable for some very sensitive networks only, **not suited to corporate networks** that need to communicate.

4.1.1 Commutateur (switch) : Contre-mesures

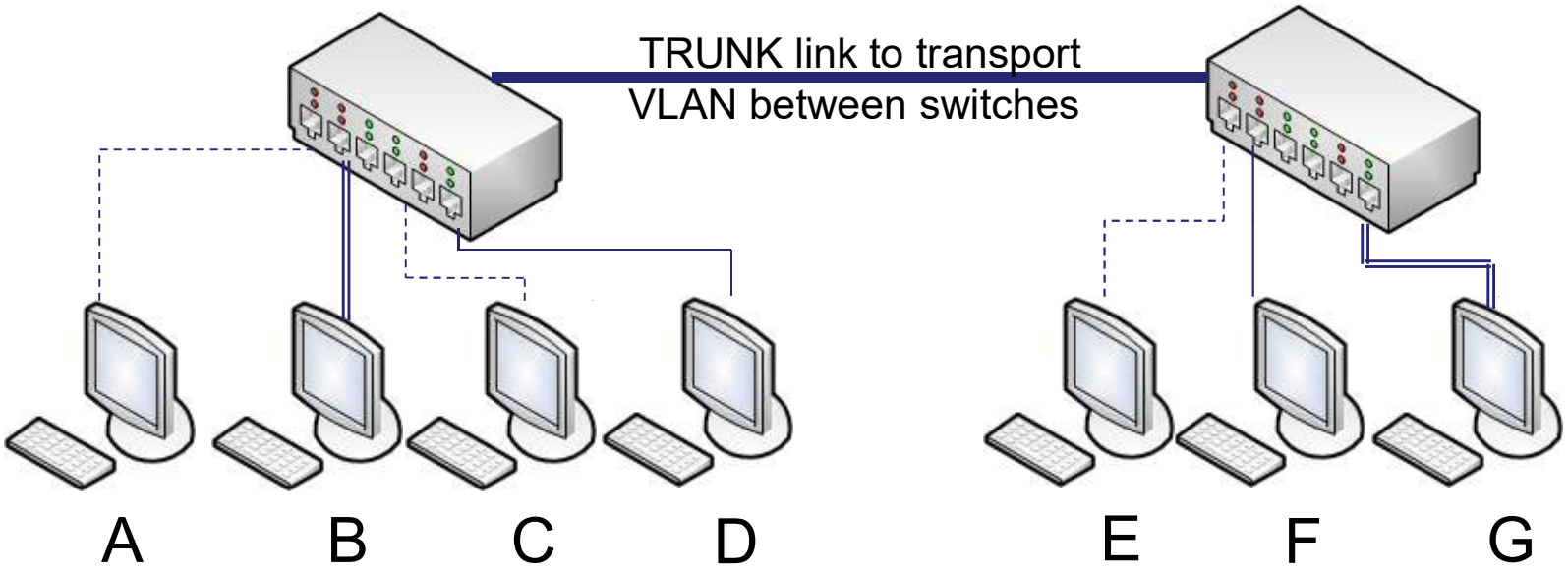
Other segmentation technique : **VLAN** (Virtual LAN).

VLANs are virtual **networks implemented by the switches**. These **restrict communication between systems according to rules** configured on the network equipment :

- The segmentation can be done by the Ethernet ports of each switch (a particular VLAN is assigned to each port of the switches, the two switches being linked together by a TRUNK link in order to carry the VLAN tags) ;
- The segmentation can also be done using the MAC addresses of the systems.
  - Warning: Since the MAC addresses of the network cards can be easily modified by the users, the filtering on the MAC addresses must be considered - logically - with caution because the effective level of security is limited.

See example on next slide.

4.1.1 Commutateur (switch) : Contre-mesures



Implementation of 3 VLAN on distant networks.

VLAN 1. Computers B and G are segmented from other systems and can communicate with each other only.

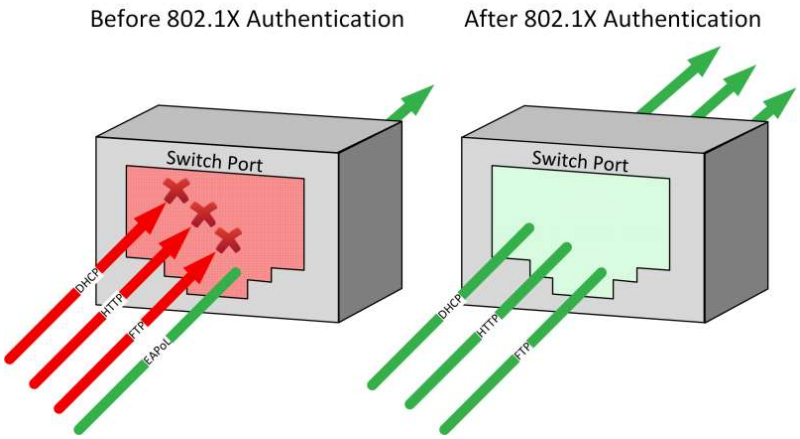
VLAN 2. Computers A, C and E Are segmented from other systems and can communicate with each other only.

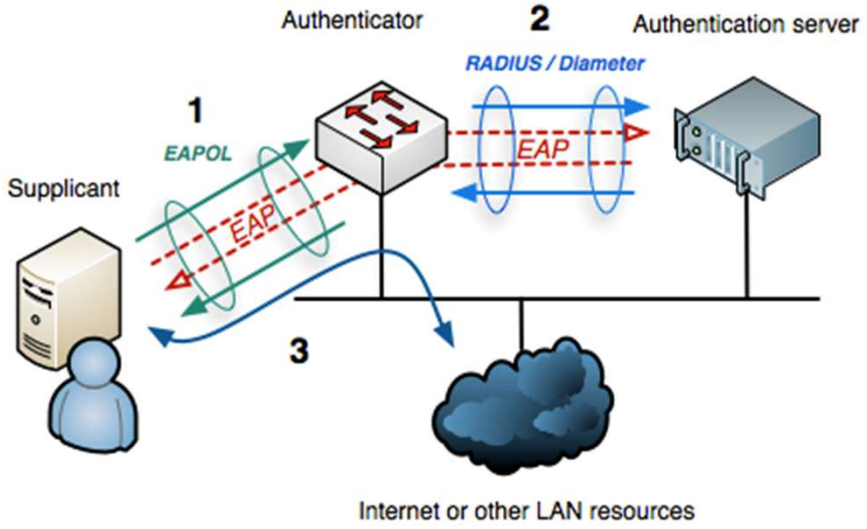
VLAN 3. Computers D and F Are segmented from other systems and can communicate with each other only.

4.1.1 Commutateur (switch) : Contre-mesures

- Use security on the switches
  - Use only manageable switches
  - Use Authentication (802.1X) on ports
    - Allows authentication of connected hardware
    - Allows authentication of user
    - Allows dynamic VLAN assignement
    - Allows to block access to the network
- Real-time monitoring of the blocked ports

4.1.1 Commutateur (switch) : Contre-mesures





4.1.3 Gateway: its role

- Allow to go from a network to another one
  - From private to private
  - From private to public
- Use of address translation
  - PAT: Port Address **Translation**
  - NAT: Network Address **Translation**
- Filtering between two networks (use restriction)
  - MAC level
  - IP level
  - On the higher layers (contents, applications)

4.1.3 Gateway: by-pass

- If there are restrictions for the users
  - IP spoofing
  - MAC spoofing
- Crossing of the gateway
  - Sending of packets by using the other network
    - (if problem with the config, the gateway will transmit the packet)
- Denial of service through the massive sending of reset packets (IP spoofing)

4.1.3 Gateway: counter-measures

- Configure correctly
  - Avoid the sending of simple packets
  - Configure the rules
    - For each ***computer***
    - For each ***service***
- Use jointly with an IDS
  - Avoid the massive sending of packets
  - Be careful
    - Do not forbid the connection coming from the pirate
    - If the IP address is usurped, the real server will be “forbidden”
- The gateway can be used as a probe (*fr. sonde*)
  - Information about the network state (worms, virus)

Université Grenoble Alpes

4.2 Routers

4.2.1 Routers

- System of interconnection of different networks
  - Are used in general as links between the internal (private) and external (public) networks
- Allows the connection to Internet
- Compulsorily named and (IP) addressed
- Ensure the functions:
  - Of security by
    - address filtering
    - protocol filtering
  - Of interconnection of the LAN, WAN and MAN
  - Of routing at the network level: it is so compulsory to know the topology at the Internet level (OSI 3 level)
  - Of improvement and management of the traffic
- Allow Remote Administration

4.2.1 Router: by-pass

- Same problems as for the gateway
  - MAC spoofing
  - IP spoofing
  - Denial of service
- Bad construction of packets
  - Bufferised in the router
  - Until saturation of the buffer
- Router management
  - Telnet and WEB
  - SNMP

4.2.1 Routers: counter-measures

- Use access-lists
  - But sensitive to the MAC, IP spoofings
- Desactivate remote management
  - Web, telnet
  - SNMP
  - Use preferably ciphered accesses (HTTPS, SSH)
- Imperative update of the IOS and logs
- Use logs (Take care of the size of logs)

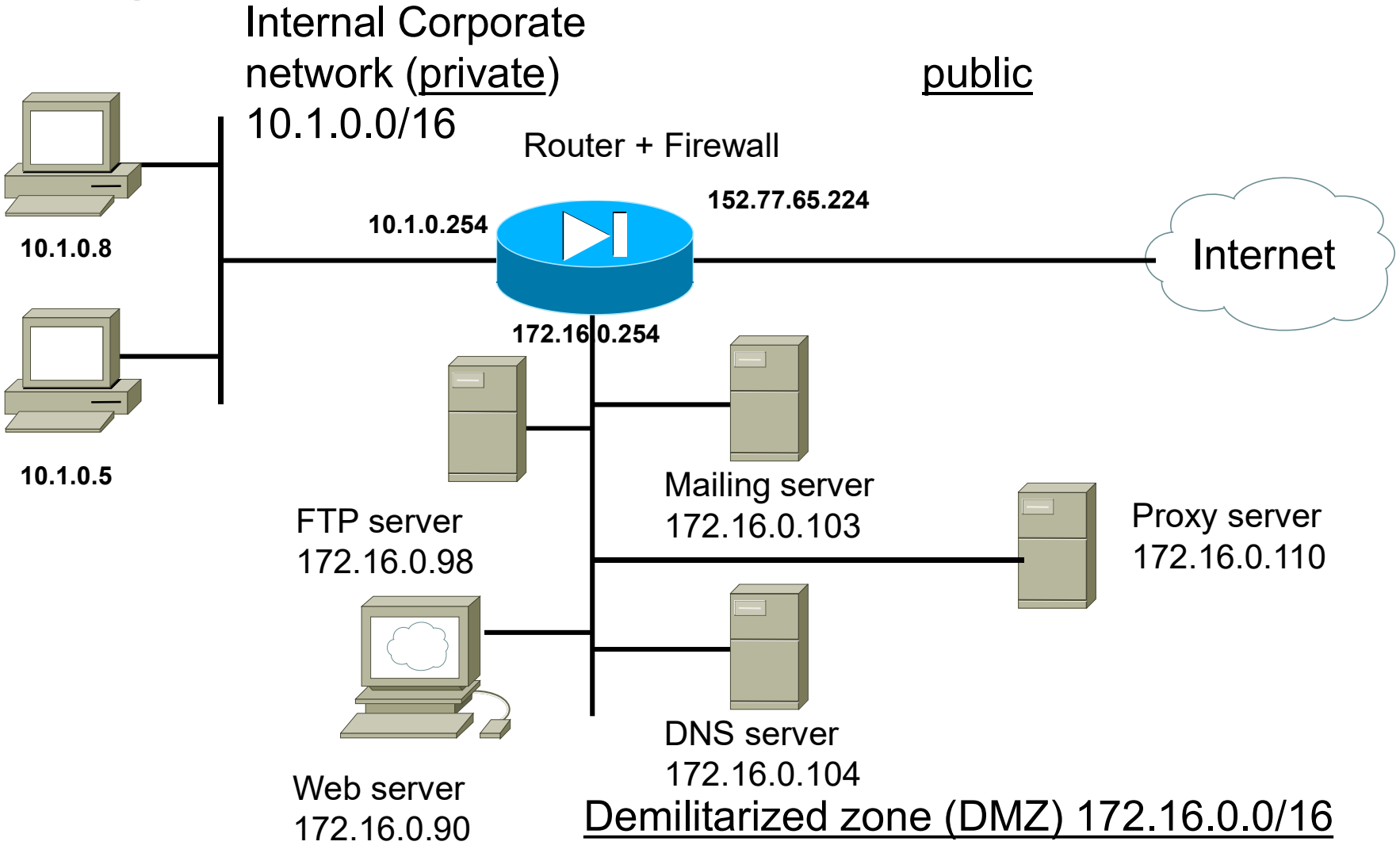
4.2.1 “Secure” configuration of the router

- To prevent the router to provide information on the network (usable by attackers)
- To prevent the immobilization of the router (and the network) by pirates or by configuration errors
- To prevent that the router serves as a springboard (*fr. tremplin*) to tackle the internal network or other networks

Université Grenoble Alpes

Firewalls

A network…


Internal Corporate
network (private)
10.1.0.0/16
public
Router + Firewall
10.1.0.254
152.77.65.224
Internet
10.1.0.8
10.1.0.5
172.16.0.254
FTP server
172.16.0.98
Mailing server
172.16.0.103
Proxy server
172.16.0.110
Web server
172.16.0.90
DNS server
172.16.0.104
Demilitarized zone (DMZ) 172.16.0.0/16

4.2.2 Filtering of packets by means of ACL (Access Control Lists)

- TCP/IP Data segmented in packets
  - Layer 3 of the TCP/IP model
- Examination of the contents of the packets and application of certain rules
  - Transmission of the packet
  - Removal of the packet
- Very widespread technology at the beginning of Internet
  - First line of defense
- Very much still used in the routers
- First line of defense, combined with other firewalls technologies

4.2.2 Types of ACLs

- Standard ACL
  - Takes into account the source address
- Extended ACL
  - Source and destination addresses
  - Possibly type of protocol and port number => for a wider research

4.2.3 Dynamic ACL (1/4)

- Dynamic filtering
  - Dynamic entries for responses to the TCP, UDP, ICMP requests
  - Does not require to keep open the static ports (the ports remain open only during the time of the session)
- Follow-up/monitoring of the TCP sequence numbers
  - Monitoring of the sequence numbers of the input and output packets to follow-up communication flows
  - Protection against “man in the middle” attacks and session hackings

4.2.2 Operation: inspection of each packet

- Source Address
- Destination Address
- Ports

- The decision to authorize or not depends on each inspected point
- Note: fast data processing
- Example of standard ACL on a Cisco router
  - To authorize the packets (permit)
  - To prohibit the packets (deny)

```
access-list 10 permit any 192.168.10.0
access-list 10 permit any 192.168.20.0
access-list 10 deny any 192.168.30.0
```

4.2.2 Types of traffic to be filtered

- Only the traffics of the authorized services must be allowed (explicitly)
- EXAMPLE:

E-mail delivery	SMTP mailing server	64.24.14.61
File transfers	FTP server	64.24.14.60
DNS Traffic (transfers of zones via UDP and requests of name via TCP)	DNS server	64.24.14.61
TCP and UDP Traffics beyond the “port 1023” to authorize output connections		

Only authorized outgoing connections:
-SSH (port 22)
-DNS (port 53)
-FTP (ports 20 and 21)
-HTTP (port 80)

Some kinds of ICMP messages

4.2.2 Ex: 121 ACL applied to router input, from Internet to LAN

```
ip address 192.168.254.1/30
ip address group 121 in
access-list 121 permit tcp any any eq 22
access-list 121 permit udp any any gt 1023
access-list 121 permit icmp any any gt 1023
access-list 121 permit icmp any any echo-reply
access-list 121 permit icmp any any unreachable
access-list 121 permit icmp any any administratively-
   prohibited
access-list 121 permit icmp any any time-exceeded
access-list 121 permit icmp any any packet-too-big
access-list 121 permit tcp any 64.24.14.60 eq ftp
access-list 121 permit tcp any 64.24.14.61 eq smtp
access-list 121 permit tcp any 64.24.14.61 eq domain
access-list 121 permit udp 64.24.14.61 eq domain
```

4.2.2 Ex: 122 ACL applied to router input, from LAN to Internet

```
ip address 64.24.14.1/24
ip address group 122 in
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any eq 22
access-list 122 permit udp 64.24.14.1 0.0.0.255 any eq domain
access-list 122 permit icmp 64.24.14.1 0.0.0.255 any echo
access-list 122 permit icmp 64.24.14.1 0.0.0.255 any echo-reply
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any eq ftp
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any eq http
access-list 122 permit tcp 64.24.14.1 0.0.0.255 any gt 1023 established
access-list 122 permit udp 64.24.14.1 0.0.0.255 any gt 1023
```

4.2.3 Dynamic ACL (2/4)

- Follow-up of the state of the sessions
  - Follow-up of half-opened, opened and closed TCP sessions, to avoid SYN Flood attacks
  - Session Numbers and transmission rates must be included between thresholds defined by the administrator
- Follow-up of UDP and ICMP connections
  - Protocols difficult to supervise (open-loop connection)
  - Follow-up by approximation (dynamic filtering, timers)
- Journalizing of the sessions
  - Dates and hours
  - Source and destination hosts
  - Ports
  - Total numbers of transmitted bytes

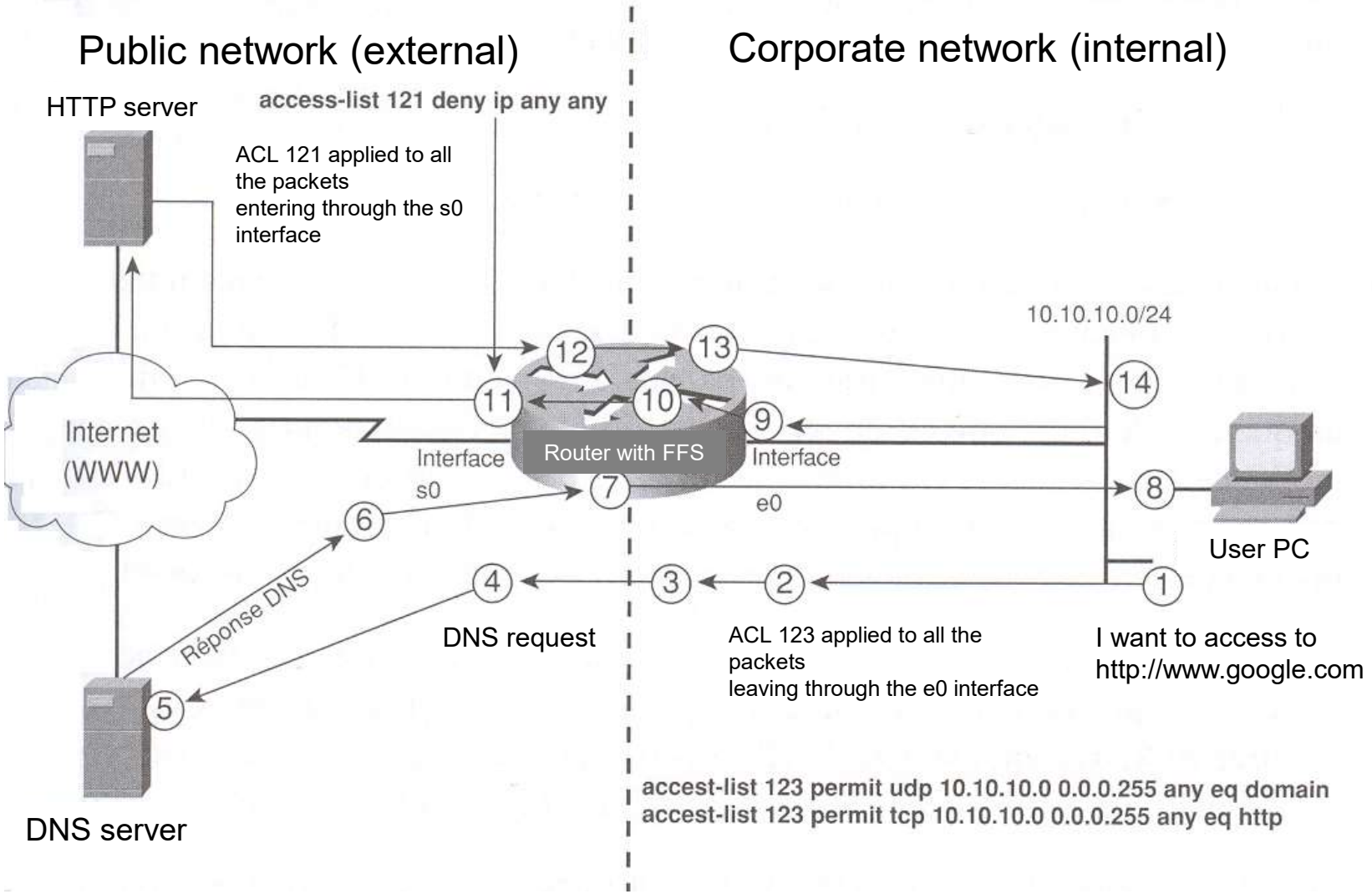
4.2.3 Dynamic ACL (3/4)

- Follow-up of specific applications (example of protocols)
  - Cu-SeeMe (port 7648): PTP videoconference
  - FTP (port 21)
  - H.323 (port 1720): multi-media communication (VoIP, video, audio)
  - ICMP: repairing of problems (administrator) + used by the pirates => to let pass only ICMP messages generated inside the network
  - MCGP (Media Control Gateway Protocol, port 2427): VoIP
  - MSRPC (Microsoft Remote Procedure Call Protocol, port 135): communication of inter-systems process

4.2.3 Dynamic ACL (4/4)

- NetShow (port 1755): Microsoft streaming
- R-EXEC (port 512): distant controls (Unix)
- R-SHELL (port 514): distant Shell (Unix)
- RTSP (Real-Time Streaming Protocol, port 544): streaming and VoIP
- SMTP (Simple Mail Transfer Protocol, port 25): mail
- SQLNet (port 1521): Communications clients-database
- Stream Works (port 1558): Real Networks Streaming
- Audio Real (port 7070): Real Networks Streaming
- TFTP (Trivial File Transfer Protocol, port 69): client-server file transfer
- VDOlive (port 7000): streaming

4.2.4 Example (1/5)



4.2.4 Example (2/5)

- 1. The user types www.google.fr
  - The station emits a request for DNS name resolution to obtain the URL IP address
- 2. The DNS request packet (a UDP datagram) arrives on the router Ethernet internal interface
  - It is compared with the list “123” (filtering)
  - It is transmitted if authorized or removed
- 3. The authorized packet is controlled by the CBAC (Context-Based Access Control => contextual access control)
  - Inspection
  - Consignment of information in the table of states
    - source IP Address and port number
    - destination IP Address, port number and protocol
- 4. Creation of a temporary instruction `permit` on list 121
  - Authorization of the responding traffic by the destination host (DNS server)
  - Temporary instruction placed in front of the static instructions in the ACL

4.2.4 Example (3/5)

- 5. The DNS request packet (UDP 53 port) is transmitted to the DNS server
  - Response of the DNS server
  - ACL dynamic input kept during 5 seconds
- 6. Arrival of the DNS response packet
  - Comparison with the ACL n. 121
  - Authorized since it belongs to an established session
- 7. Inspection of the DNS response packet
  - Conservation of information until expiration of the timer (timer for the keeping of UDP sessions)
- 8. Arrival of the DNS response to the user PC and initiation by the PC of an HTTP session with google
  - HTTP is based on TCP, therefore the first packet comprises the SYN (synchronization) bit; this bit is activated to start the three-times negotiation process of TCP

4.2.4 Example (4/5)

- 9. HTTP packet is authorized
  - list 123 is authorizing HTTP port n. 80
- 10. Inspection of the output packet and consignment of information in the table of states
  - Source IP address and port
  - Destination IP address, port and protocol
- 11. Creation of a temporary instruction `permit` on list 121
  - Authorization of the traffic in response by the destination host (HTTP server)
  - Temporary instruction placed in front of the static instructions of the ACL
  - Maintenance of the entry during 30 seconds (time to receive a SYN-ACK packet, synchronization-acknowledgement from the Web server)
- 12. Reception of the packet coming from the Web server
  - Authorized by list 121 (because it belongs to an established session)

4.2.4 Example (5/5)

- 13. Inspection of the packet coming from the Web server
  - Elimination of the packet if there are specific violations of protocols
- In the case of HTTP and other protocols requiring several sessions
  - Continual update of the table of states
  - Continual update of the ACL
- Times of removal of temporary entries in the ACL
  - ICMP and UDP, with expiration of a timer (configurable duration)
  - TCP, five seconds after the exchange of FIN packets

Université Grenoble Alpes

4.3 Firewalls

4.3.1 Firewall: its role

- Filtering accesses
  - Inputs and outputs
- Personal firewall
  - On personal computers (software)
  - Layers 1 to 7
- Professional firewall
  - Hardware component
  - Layers 1 to 7

4.3.1 Inspections of packets with follow-up of the state of connection (SPI: Stateful Packet Inspection)

- 4th-layer (transport layer) TCP/IP model
- Implemented on a firewall behind the router
- Second line of defense
- Supervise the “connection” between two computers

4.3.1 Firewall: by-pass

- Personal firewall
  - Download a pgm, the pirate can take control, if this program looks like a well-known pgm (iexplorer.exe)
  - No reaction from the firewall : known pgm and authorised port
- Professional firewall
  - MAC, IP spoofing
  - Some firewalls don’t process packets content
  - Firewall auto-blocking (massive sending of a flow with IP spoofing)
- logs saturation

4.3.1 Firewall: counter-measures

- To be updated
- Coupled to an IDS
  - To know what is going on
- Coupled to an IPS
  - To react automaticly in case of an attack
- Consultation of the logs
  - And clean the logs

4.3.2 Operation of the inspection of packets with follow-up of the state of connection (SPI) (1/2)

- Inspection of a first “authorized” packet (by the router)
- An entry is created in a table of the firewall (*new connection* state)
- Received packets => checking if they belongs to an existing connection (*related connection*)

4.3.2 Operation of the inspection of packets with follow-up of the state of connection (SPI) (2/2)

- Examination of packet header
  - Source and destination addresses
  - Protocol type(TCP, UDP, ICMP…)
  - Source and destination ports
  - Indicating bits (SYN, ACK, FIN, RST…)
  - …
- Comparison with the traffic control rules
  - Ex (classical): To let pass only HTTP traffic (TCP/80 and TCP/443)
- Generally, the firewall authorizes connections towards outside

  => inputs in the table of state

  => input packets (responses/feedbacks to requests) belonging to these connections are not filtered
- The rules can be complex (they are used only once per connection => thus complexity is not too synonymous with degradation of the performances)

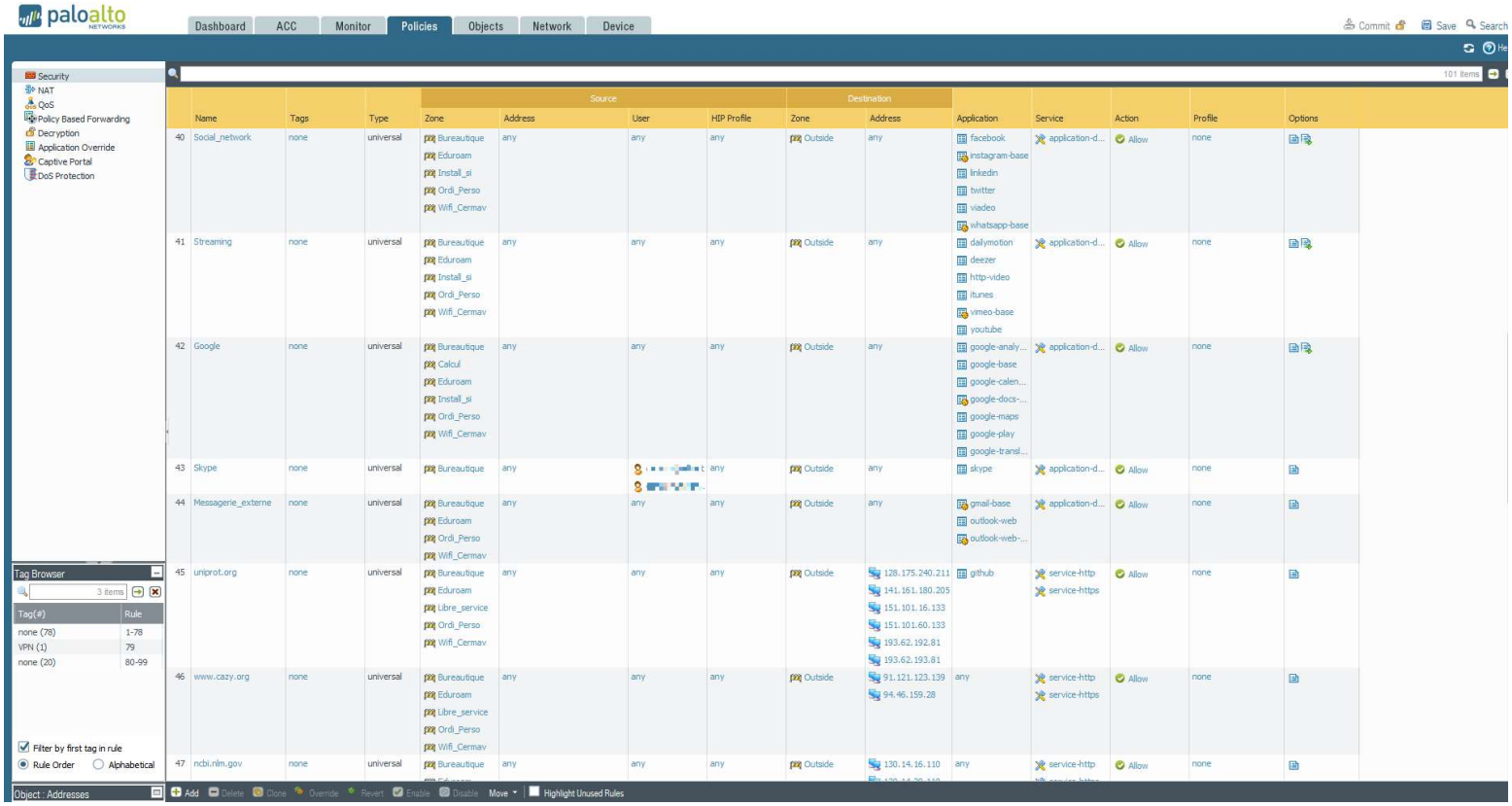
4.3.3 Rules of filtering/firewalls

- Rules swept in the ascending order
  - Need to insert the most used rules at the beginning (performance)
  - Need to inserts the most restrictive rules before the others (e.g.: if a machine has certain rights and the network to which it belongs does not have them)
- To prohibit any traffic towards the firewall
- Implicit rule prohibiting any traffic not corresponding to an explicit rule

NO.	SOURCE	DESTINATION	IF VIA	SERVICE	ACTION	TRACK	INSTALL ON	TIME	COMMENT
1	* Any	ip330	* Any	* Any	drop	Log	* Policy Targets	* Any	
2	Lan_privé	* Any	* Any	TCP http	accept	None	* Policy Targets	* Any	
3	Lan_privé	serveur_dmz	* Any	UDP domain-udp TCP ftp	accept	None	* Policy Targets	* Any	
4	* Any	Lan_privé	* Any	* Any	reject	Log	* Policy Targets	* Any	
5	serveur_dmz	* Any	* Any	dns	accept	None	* Policy Targets	* Any	
6	* Any	serveur_dmz	* Any	dns TCP http	accept	None	* Policy Targets	* Any	
7	* Any	serveur_dmz	* Any	FTP ftp->ftp_get	accept	None	* Policy Targets	* Any	
8	* Any	* Any	* Any	* Any	drop	Log	* Policy Targets	* Any	

4.3.3 Rules of filtering/firewalls

- Rules can act at application level
  - For each application we could allow or not a specific action
- Rules can be applied to specific users



4.3.3 Disadvantages (insufficiencies)

- Some firewall don’t inspect at the application level
- No states of connections for some protocols
  - Ex: ICMP, UDP

4.3.4 NAT function (network address translation)

- Internet Addresses (IPv4)
  - Theory, 2^{32} addresses (~4,3.10^9 addresses)
  - Practical
    - Public addresses: ~3,2.10^9
    - Reserved addresses: test…
    - Private addresses: reserved for the internal networks (non accessible from outside)
      - 10.0.0.0 to 10.255.255.255 (prefix 10/8)
      - 172.16.0.0 to 172.31.255.255 (prefix 172.16/12)
      - 192.168.0.0 to 192.168.255.255 (prefix 192.168/16)
- NAT ensures the conversion between public and private addresses, between the internal network and the outside accesses
  - firewall,
  - sometimes a router or a computer

4.3.4 NAT

- Static NAT
  - Always the same public IP address to a given private IP address
  - Ex: Web server
- Dynamic NAT
  - Association of a random public address drawn from a group, to a private IP address
- PAT (Port Address translation)
  - Associate only one public address to several private addresses by using various ports
  - *Let's remember*: 65.535 TCP ports are supported by an IP address

4.3.4 Security with NAT

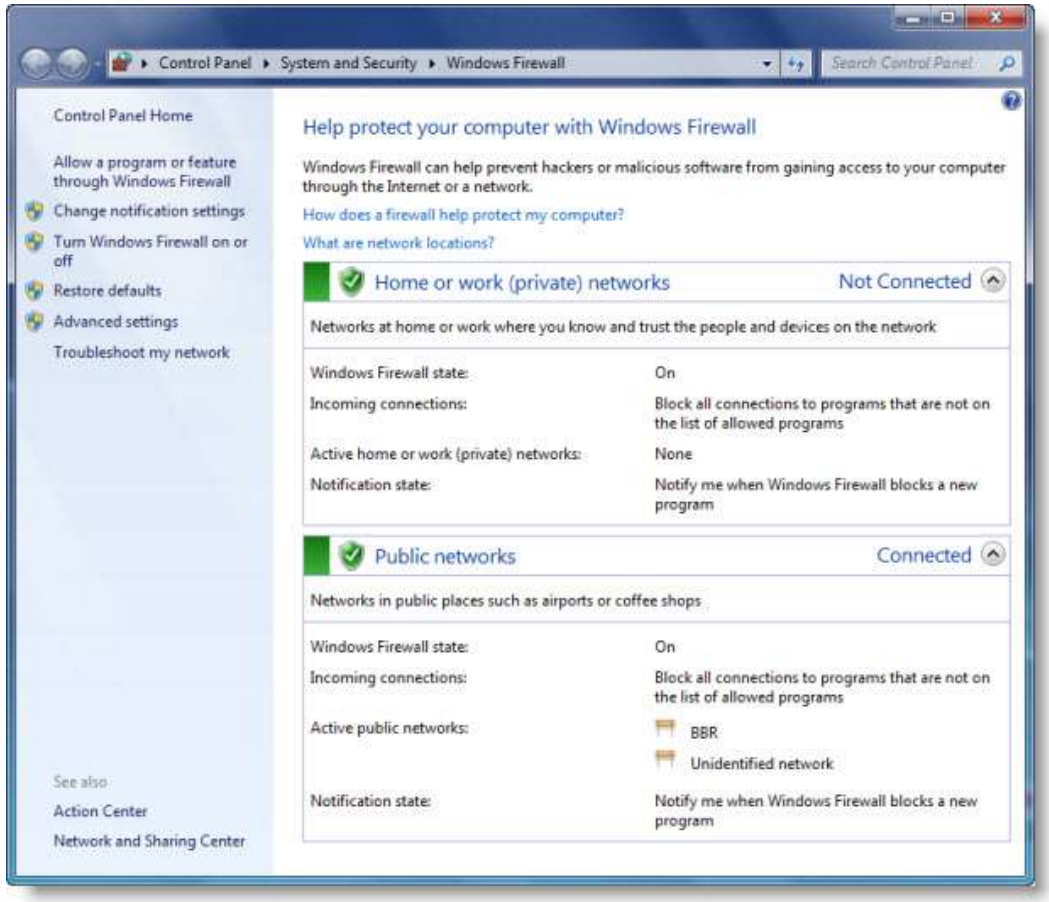
- More difficult for an attacker to:
  - Determine the topology of the network and the type of connectivity of the target company
  - Identify the number of systems which are running on the network
  - Identify the type of machines and their operating systems
  - Carry out attacks such as denial of service (Ex: SYN Flood, scan of ports, packets injection)

4.3.4 Disadvantages of NAT

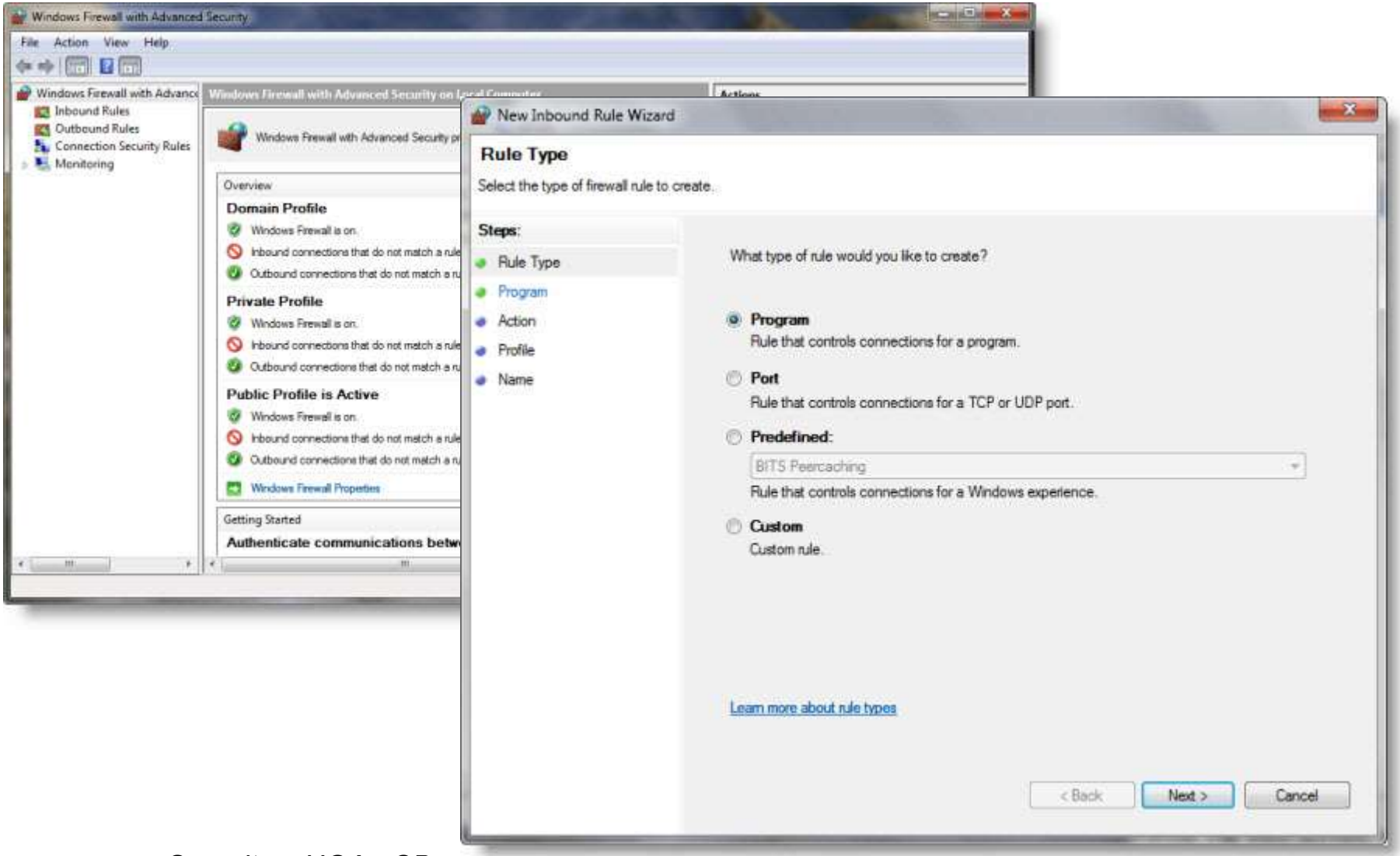
- Bad management of UDP connections
  - Difficult estimation of how many time must the connection remain open
- Other protocols are badly managed
  - Kerberos, X Windows, rsh (remote shell), SIP (Session Initiation Protocol)
- Systems of ciphering and authentication
  - These systems are based on the integrity of the packets
  - However NAT modifies these packets
- Journalizing is complicated
  - Analyzing the correlation between journals requires to take into considerations the NAT
- Problem with the sharing of address with PAT
  - Authentication by a protected external resource (all the users sharing the same address are likely to be able to use this resource)

4.3.5 Types of firewalls

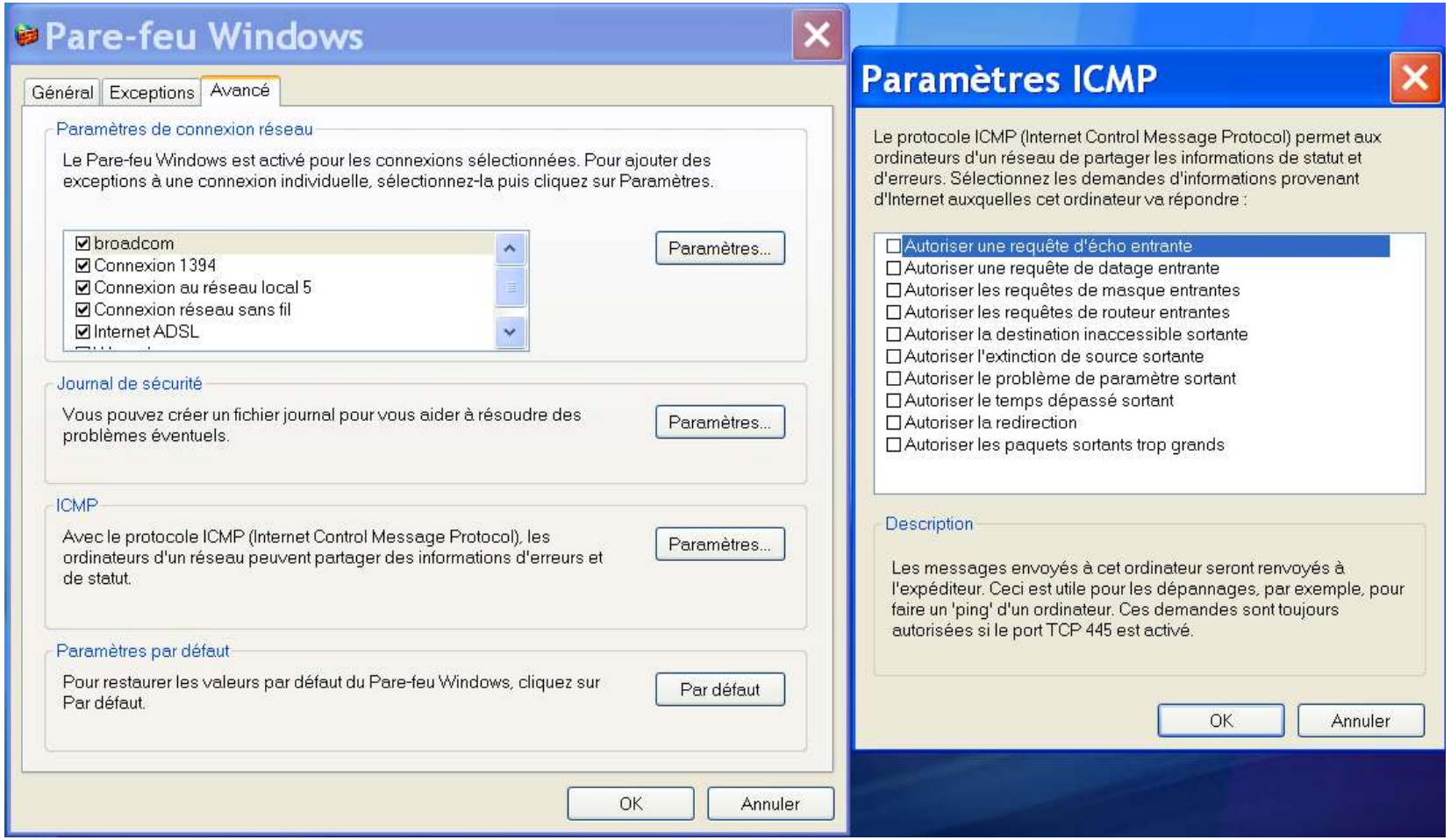
- Personal firewalls
  - Could be integrated into the system (Windows, Mac, Linux…)
  - Ex: Windows 7 => in the control panel



4.3.5 Personal firewalls (2/4)



4.3.5 Personal firewalls (3/4)



4.3.5 Personal firewalls (4/4)

- Personal firewalls websites
  - www.comodo.com
  - www.zonelabs.com
  - tinywall.pados.hu
  - www.online-armor.com
  - …

4.3.5 Next generation firewalls

- Application level inspection
- Rules defined at user level
- Encrypted traffic analyze

- Example : Palo Alto Firewall

4.3.5 Next generation firewalls

Address translation

			Original Packet						Translated Packet	
	Name	Tags	Source Zone	Destination Zone	Destination Interface	Source Address	Destination Address	Service	Source Translation	Destination Translation
1	Afficheur_bureautique	none	Afficheur	Bureautique	ethernet1/2.2	any	any	any	none	none
4	Afficheur_DMZ	none	Afficheur	DMZ1	any	any	any	any	none	none
5	Afficheur_outside	none	Afficheur	Outside	ethernet1/13	192.168.15.50	any	any	static-ip 195.83.29.4 bi-directional: no	none
6	Bureautique-Afficheur	none	Bureautique	Afficheur	ethernet1/4.3	any	any	any	none	none

4.3.5 Next generation firewalls

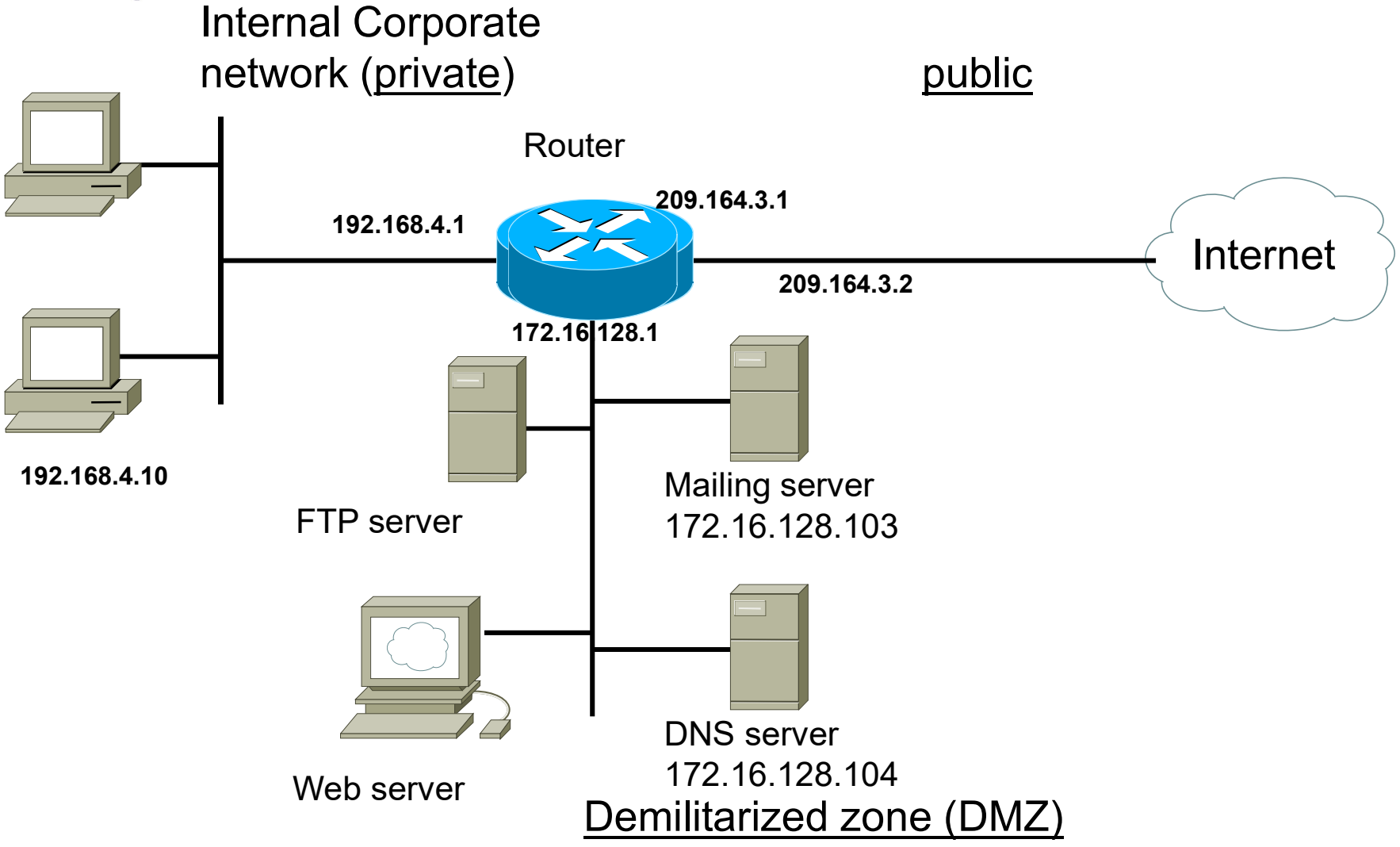
Filtering rules

18	Kali	none	universal	Bureautique	17	any	any	Outside	any	any	any	Allow	none	
19	connect.univ-rouen.fr	none	universal	Bureautique	any	any	any	Outside	193.	any	any	Allow	none	
20	*DMZ_download*	*none*	*universal*	*DMZ1* *DMZ2*	*any*	*any*	*any*	*Outside*	*any*	*any*	*service-http* *service-https*	*Allow*	*none*	
21	VPN_UGA	none	universal	Bureautique Eduroam Wifi_Cermav	any	any	any	Outside	193.	dtls	application-d...	Allow	none	
22	ESRF	none	universal	Bureautique	17	any	any	Outside	193.	any	SSH_ESRF	Allow	none	
23	UPS	none	universal	Bureautique DMZ1 DMZ2 TOIP	17 17 17 17 17 19 19 more...	any	any	IDRAC	192.	any	service-http service-https	Allow	none	
24	Supervision	none	universal	Bureautique	17	any	any	Administra... DMZ1 DMZ2 IDRAC Imprimantes TOIP	any	ping snmp	application-d...	Allow	none	
25	UPS-client	none	universal	IDRAC	19	any	any	Bureautique DMZ1 DMZ2 TOIP	17 17 17 17 17 19 19 more...	apc-powerch...	application-d...	Allow	none	
26	UPS-Ping	none	universal	IDRAC	19	any	any	IDRAC	19	ping	application-d...	Allow	none	
27	Skype	none	universal	Bureautique	any	any	any	Outside	any	ms-lync ms-lync-online skype windows-azure	application-d...	Allow	none	
28	Skype-ip	none	universal	Bureautique	17	any	any	Outside	any	skype	application-d...	Allow	none	
29	VPN_Portal	none	universal	Eduroam	any	any	any	Outside	19	any	service-https	Allow	none	

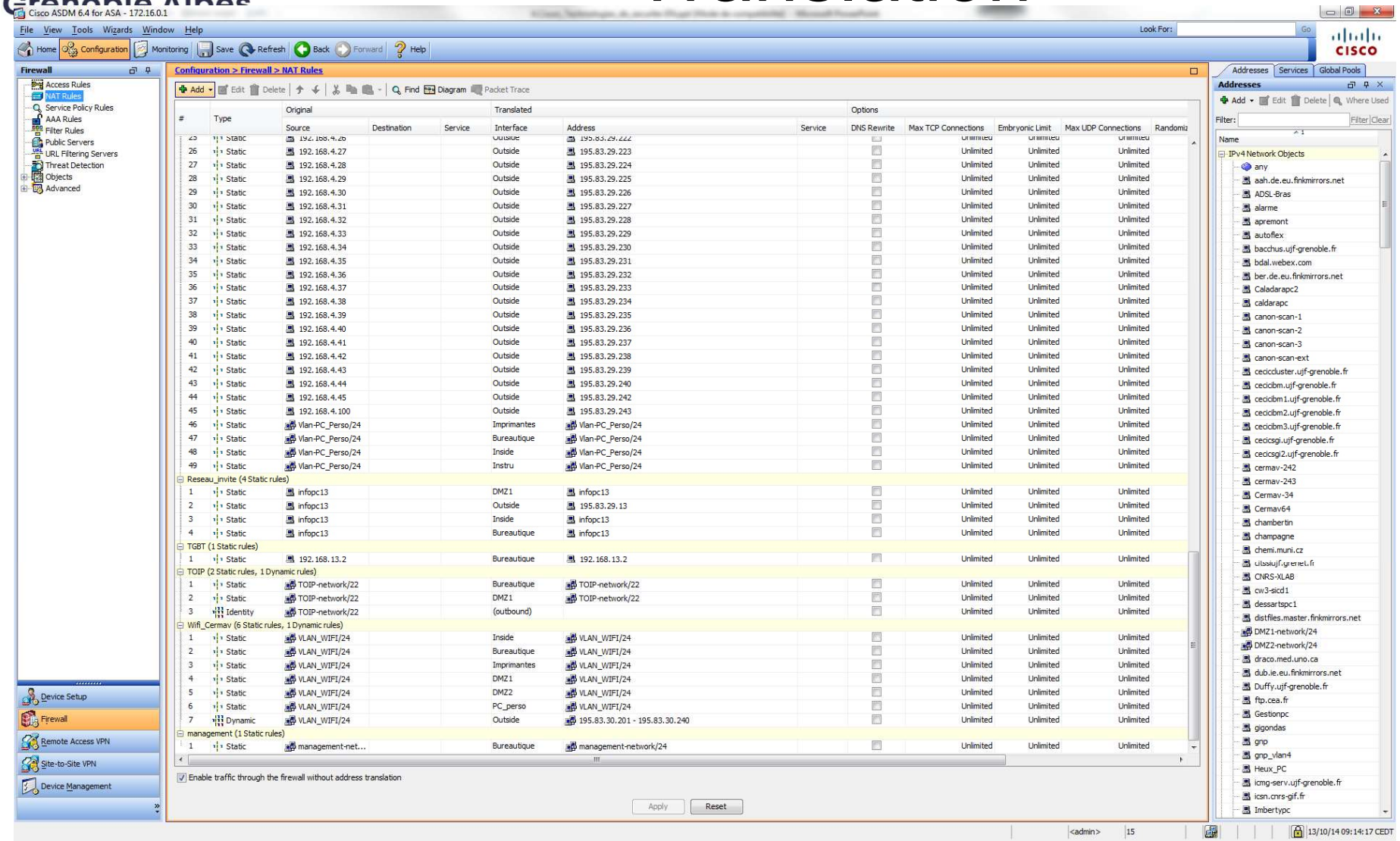
Université Grenoble Alpes

Type of firewall
Cisco ASA

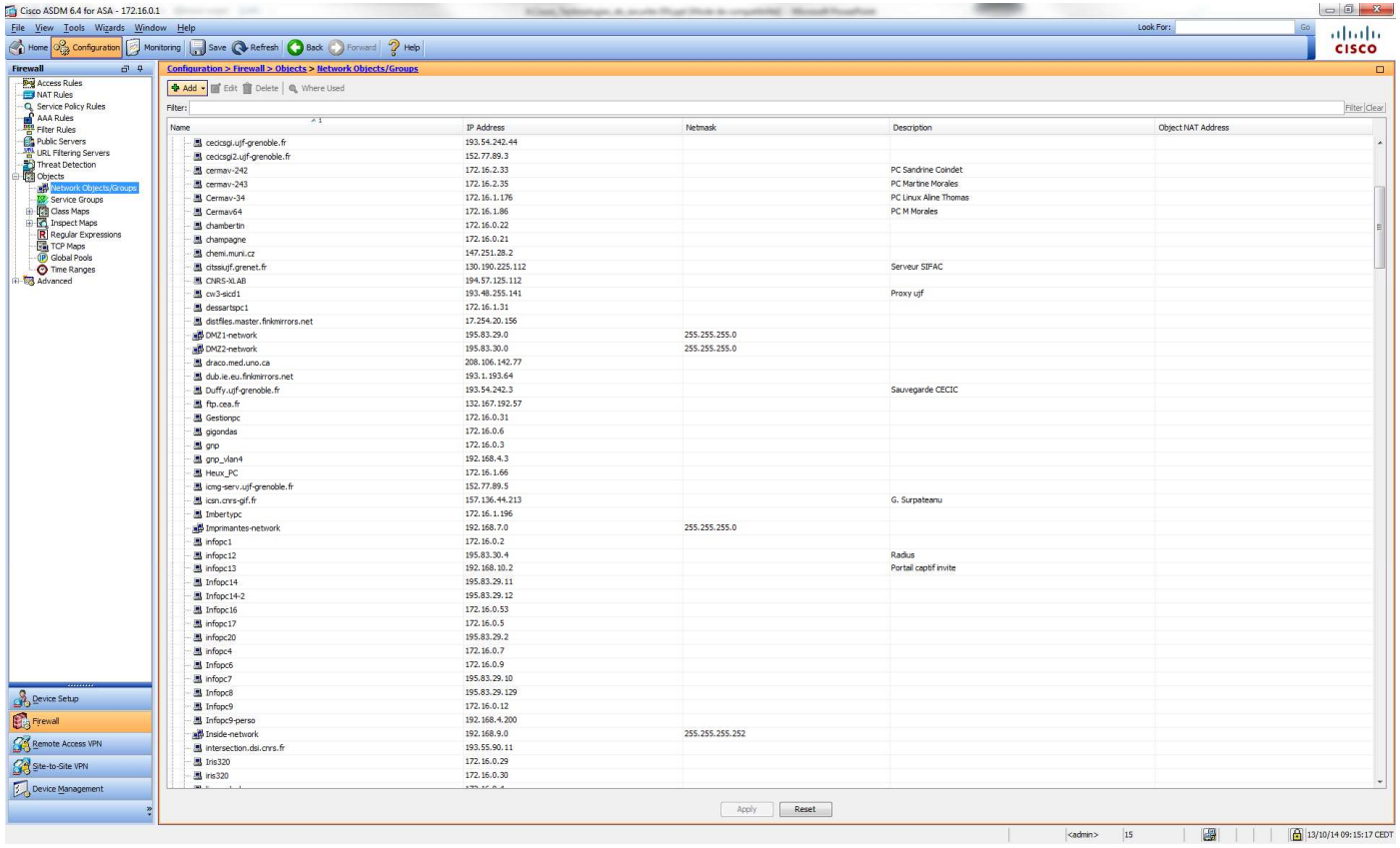
A network…


Internal Corporate network (private)
public
Router
192.168.4.1
209.164.3.1
209.164.3.2
Internet
172.16.128.1
192.168.4.10
FTP server
Mailing server
172.16.128.103
Web server
DNS server
172.16.128.104
Demilitarized zone (DMZ)

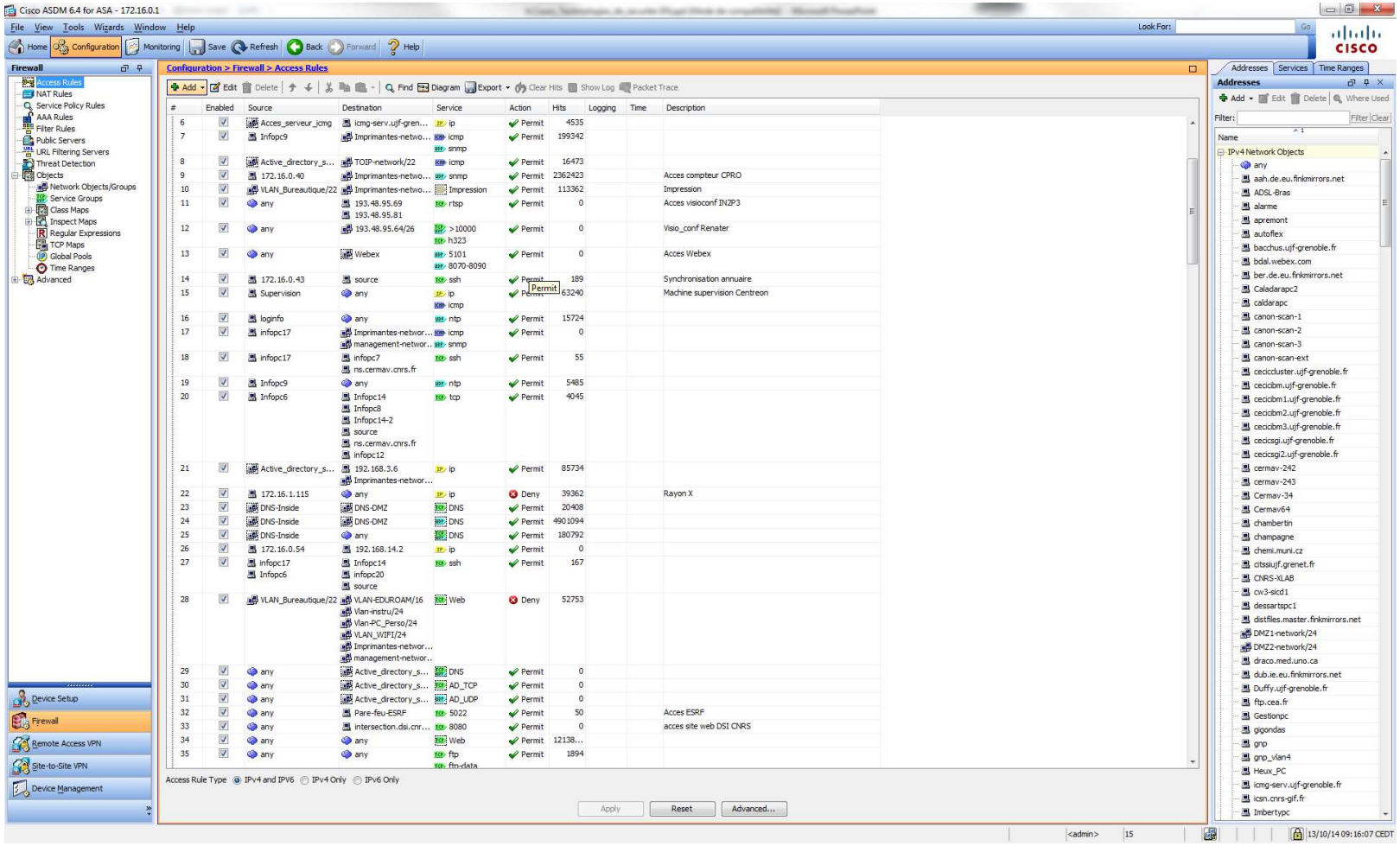
Translation



Cisco ASA firewall



Filtering rules



4.3.5 Types of firewalls

- Firewall all in one
  - Integrates the following functionalities:
    - Router
    - Ethernet switch
    - Wireless Access point
    - Firewall
- Firewall for office of middle size
- Firewall for companies
    - Differences between the ranges of firewall
  - Number of supported connections
  - Capacity

4.3.5 Place of the firewalls

- Where should we put the firewalls?
  - At the connection interface between internal network and outside (Internet)
  - Between various portions of internal networks (large companies)

4.3.6 Firewalls limitations

- Cannot prevent users or attackers using modems to reach inside the network
- Cannot prevent a misuse of the passwords (non respect of the passwords strategy by the users)
- Concentration of the traffic in only one point = bottleneck = source of fatal breakdown

Guiding principles for the configuration of a firewall

- – Less privilege: do not grant the users with a higher level of rights that they need; to prohibit for example the peer-to-peer protocol within a company
- – Default Prohibition: To prohibit everything by default: everything which is authorized should be explicitly authorized
- – In-depth defense: to use the protection means at all the possible levels, for example by analyzing and filtering everything which can be analyzed at the level of the firewall. This principle prevents letting enter the network undesirable communications, even if another method of control is used more in-depth in the network
- – Bottleneck: all the communications incoming and outgoing of the network must forward by the firewall. Other paths are strictly forbidden, such as for example unauthorized modems or access points
- – Simplicity: the firewall filtering rules must be the simplest and most comprehensible possible in order to avoid any error on behalf of the administrator or his successors (every rule should be documented and traceable)
- – Participation of the users: the users must be involved in the firewall definition. They must indeed express their needs and receive in exchange the reasons and the objectives of the installation of such a device; the constraints related with the firewall will be accepted thus better.

Université Grenoble Alpes

4.4 proxy firewalls

4.4.1 Proxy: its role

- Cache for Web and FTP
- Allows the control and record of all the requests towards outside of the private network
- Only the proxy can cross the router, the other computers cannot
- Feedback => the router communicates only towards the proxy

4.4.1 Proxy: by-pass

- If bad configuration of the router
  - It answers to other computers (other than the proxy)
  - Bad configuration of the clients (access rights)
- The router identifies the proxy
  - Replaces it on the network

4.4.1 Proxy: counter-measures

- Correct configuration of the router and clients
- Protection against proxy spoofing
  - Update of the system
  - SSL Connection with the router
  - Setting of a private network (proxy with two network cards (interfaces))
- Use of probes (*sondes*) to detect if a tunnel is installed
  - High traffic on a specific site
  - Take care of tunnels with multiple targets

4.4.2 Reverse-proxy (Rproxy): its role

- Same function as the proxy but for entering traffic
  - Internal servers in cache for the consultation coming from internet
- Purpose
  - It receives all the attacks
  - Filtering of HTTP requests (or other services)
  - Protection of internal servers

4.4.2 Reverse-proxy (Rproxy): by-pass

- To find the address of the real server (if there is a fail in the router for example)
- Saturation of the RProxy
  - Constant sending of a request flow
  - To stop the Rproxy to answer to the computers
  - Sending of reset packets
- Sending of « pirated » HTTP requests
  - Depends on the proxy functions
- Corruption of a computer on the local network
  - Allows to access to the servers

4.4.2 Reverse-proxy (Rproxy): counter-measures

- Check the configurations
  - Routers
  - Computers in the local network
- Configure a « compulsory » proxy
  - For accesses coming from outside
  - For access coming from the local network
  - Example in Grenoble: www-cache.ujf-grenoble.fr, port 3128
- Isolate the network from the servers
  - To hide the servers for everybody
  - Rproxy with 2 network cards (interfaces)

4.4.3 Proxy

- Firewall at the application level, or proxy firewall
- Analyze packets on the high-layer levels
  - Able to make the difference between e-mail and Java data, for example
- Serves as a “barrier” between outside and inside
- Standard proxy firewalls
  - Transmission of the packets at the TCP/IP level
  - No connection from outside towards inside by PCs
- Dynamic proxy firewalls
  - Propose a new level 3 packets filtering after having processed the application level
- Functioning of the proxy
  - Separation of the headings and the data
  - Inspection of information
  - If the packet is authorized
    - Storage of information about connection; this information is contained in the heading
    - Rewriting of the headings
    - Transmission of the packet
- Proxy limitations
  - Degradation of the performances
    - Very sure but slow
  - Insufficient actualization

Université Grenoble Alpes

4.5 DMZ, demilitarized zone (concept of perimetric security)

4.5 Demilitarized zone (perimetric security) (DMZ)

- Specific isolated zone of the internal network (between the public zone and the private zone)
  - Web server
  - Mailing server
  - FTP server
  - …
- This strategy allows the traffic coming from Internet to go in this zone, but not to penetrate elsewhere in the internal network
- Possibility of audit traffic exchanged with the DMZ
- Possibility of placing an intrusion detection system (IDS)

4.5 DMZ: its role

- To propose a zone
  - Receiving requests from outside
  - Does not allow direct communication from outside
  - Using its own addressing policy
- Access to the zone
  - Through the router from outside
  - Through the router + NAT from inside
- To realise a buffer zone
  - Can be corrupted
  - Does not reveal the presence of the local network

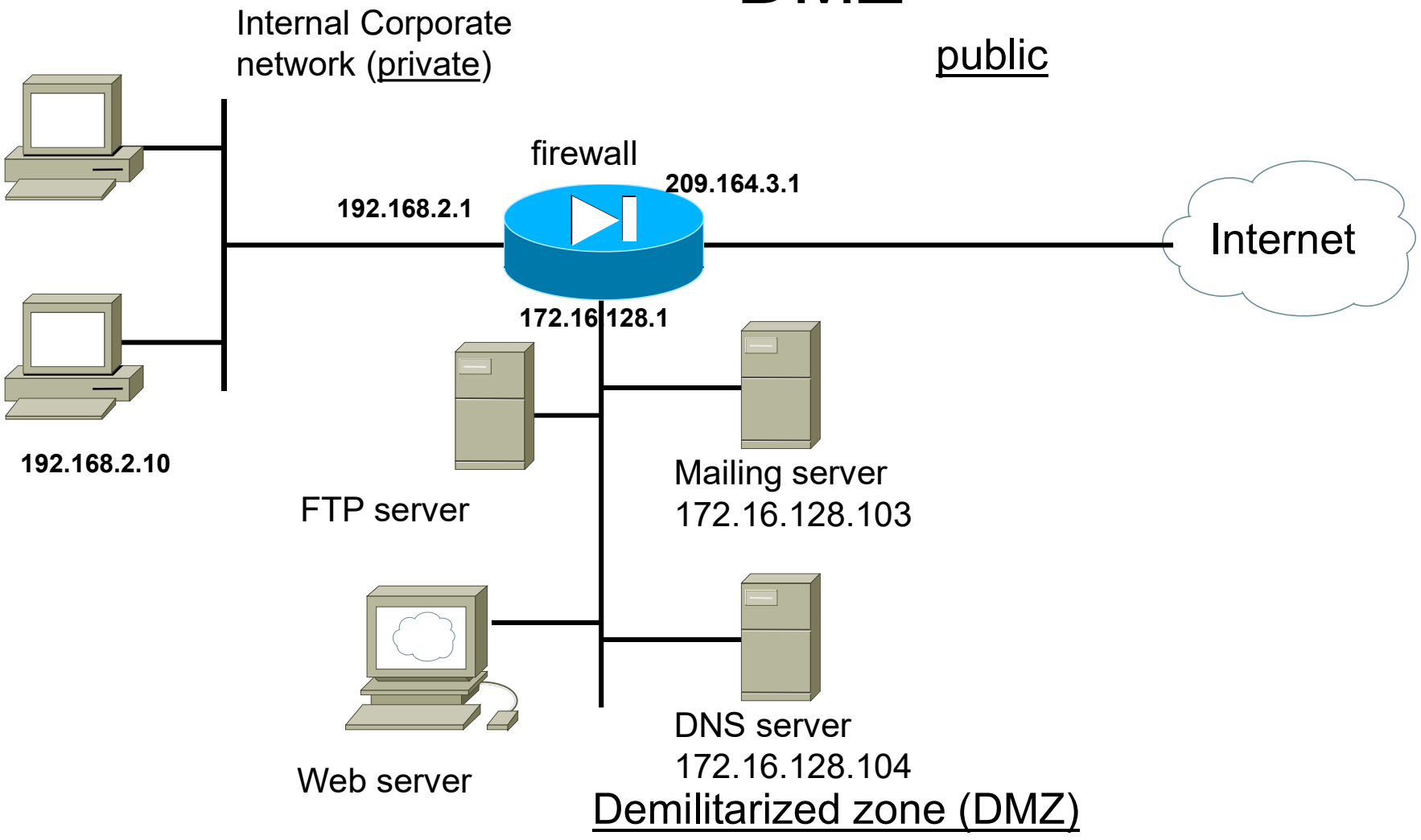
4.5 DMZ: by-pass

- To corrupt the DMZ server
  - Security failure, code injection
- Setting of a sniffer
  - Decoding of higher layers
  - Allow to know the local network
- Use some technics to cross the firewall
  - Corruption of the computers of the local network
- Use the fails of the DMZ design
  - => to have 2 mail servers

4.5 DMZ: counter-measures

- Access strictly forbidden
  - DMZ => local network
- NAT access compulsory
  - Local network => outside
  - Local network => DMZ
  - Take care of the internal hacking
- Network probe
  - To see if the DMZ is corrupted
- If 2 mail servers
  - The internal server should get the mails from the external server

4.5 Localization and function of a DMZ

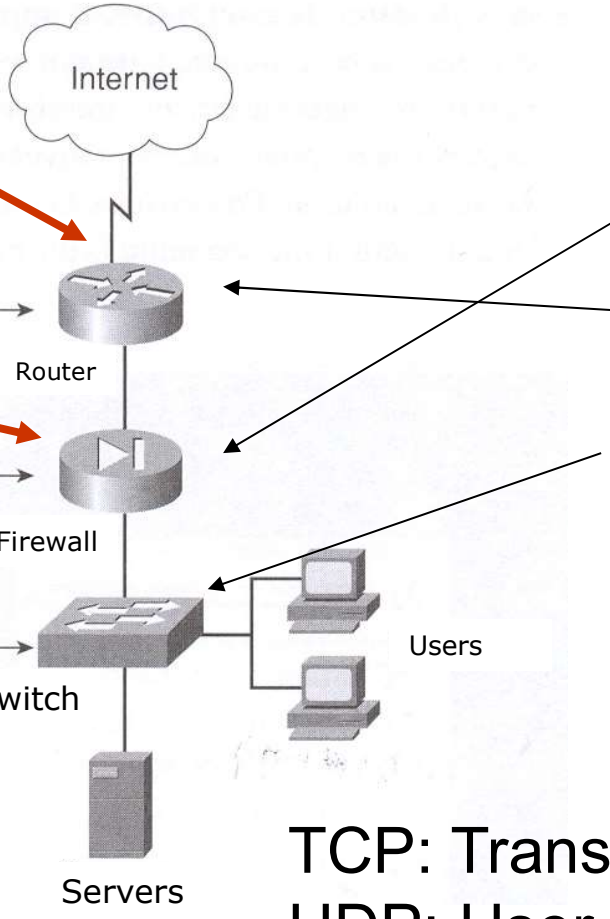


Security in layers (TCP/IP layers) implemented in several points of the network

Filters for entering packets (router, layer 3)

Functions SPI and NAT (firewall, layer 4)

Security is implemented at every level



7. Application
4. TCP & UDP (transport)
3. IP (network)
2. Data link
1. Physics

TCP: Transport Control Protocol
UDP: User Datagram Protocol

4.6 Conclusion

- Packets layer (3)
  - Filters of packets (router)
    - Eliminate undesirable addresses
- Transport layer (4)
  - Inspection of SPI packets (firewall)
    - Identify authorized connections (solicited)
  - Address translation
    - The internal network is invisible outside
- Application layer
  - Inspection of data (proxy firewall)
- Each method alone is insufficient

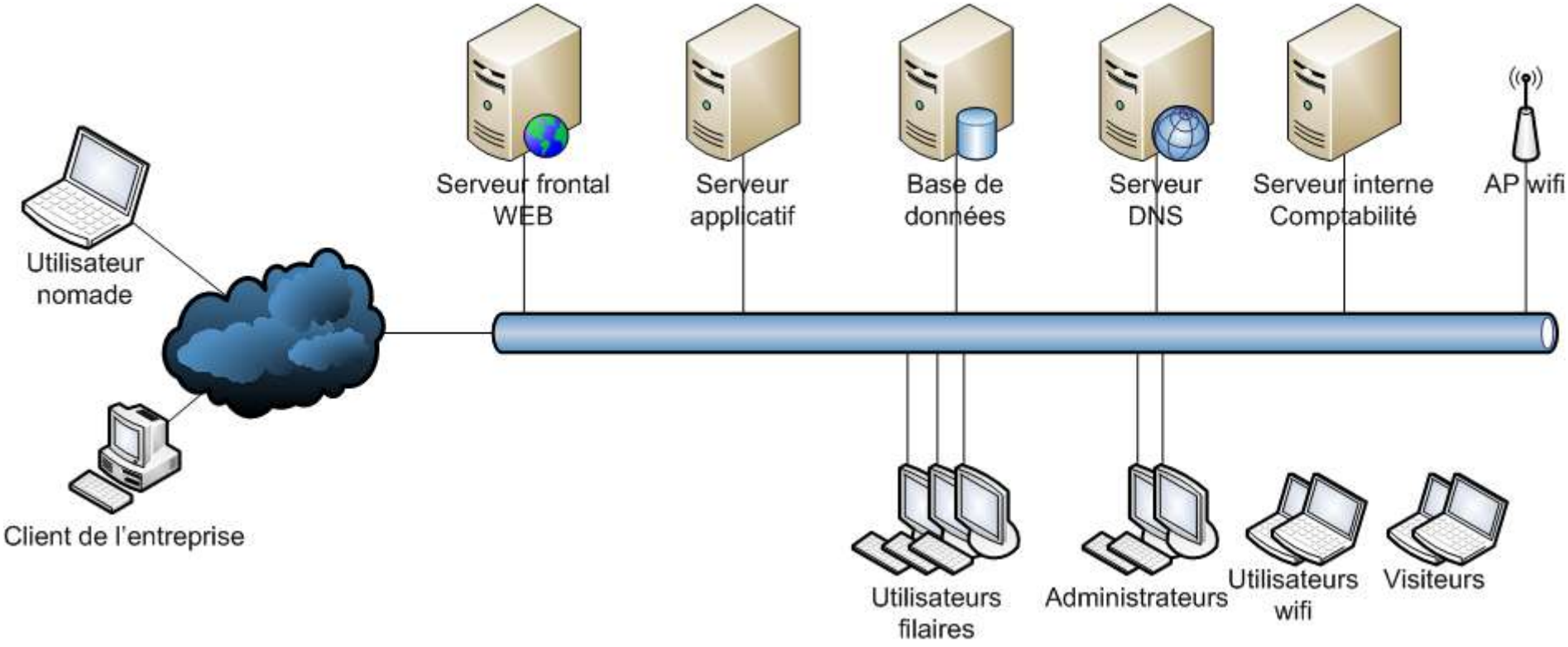
=> Their combination offers a good level of protection

Practical example of securing a simple network

Let's take the example of a "flat" corporate network. Characteristics of this company :

- It provides an e-commerce web site ;
- Some employees connect to the wired LAN, others connect to wifi ;
- Some employees are nomadic and therefore have to connect remotely ;
- There are two main categories of users: "standard" users and IT administrators ;
- In order to function, the company also has internal servers (accounting, wiki, etc.) ;
- The company wants to allow its visitors to connect the wifi in order to browse the internet.

Practical example of securing a simple network



Réseau « à plat », avant sécurisation

Practical example of securing a simple network

Let's see how we can secure this network.

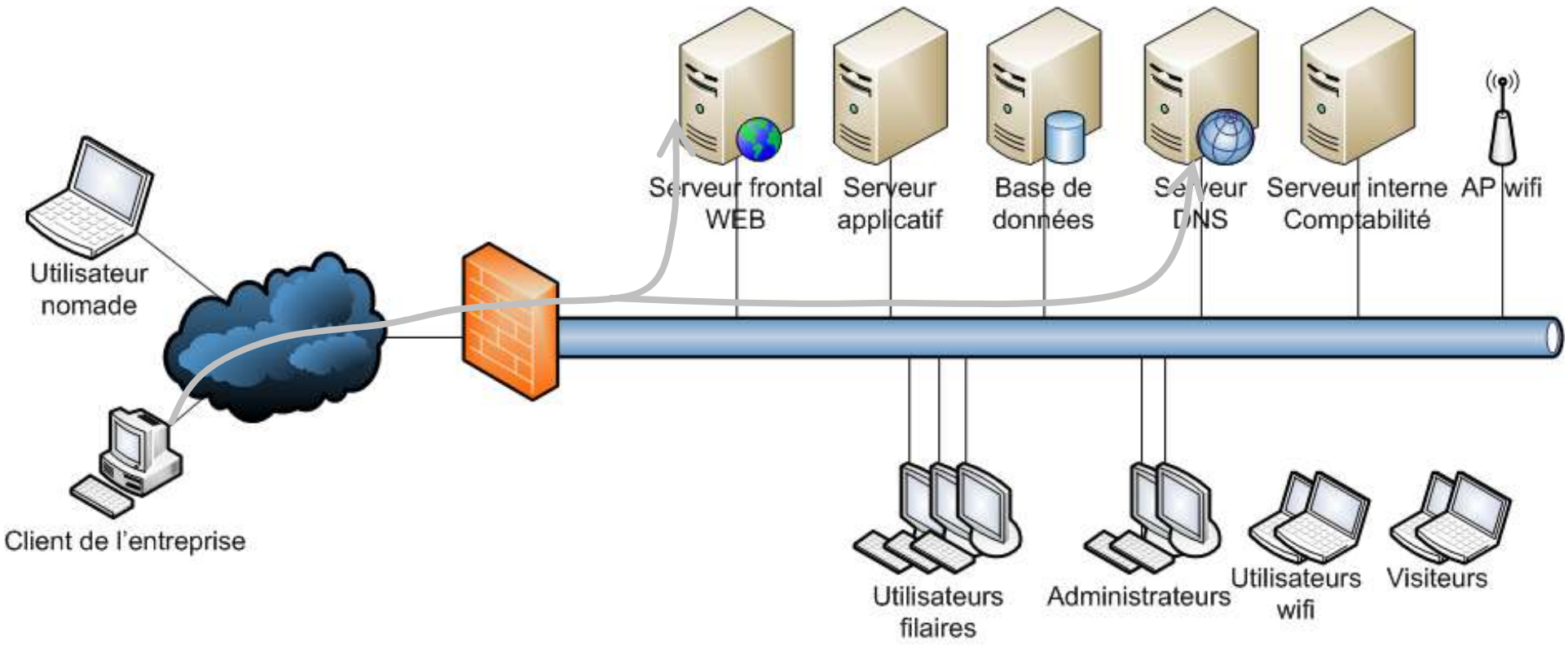
Note: there are several ways to improve the security of this network, we present here only the main lines. This exercise is neither exhaustive nor the only possible solution.

Among the many architectural weaknesses of this network, we can identify at least the following problem :

•The network is directly connected to Internet, i.e. all systems and users and systems can communicate with outside (beware of data leakage!) and all Internet can connect on our internal network.

Fix this by implementing a front-end firewall that will allow only incoming traffic to the WEB server (TCP / 80 and TCP / 443) and the DNS server (UDP / 53 and TCP / 53). Thus, Internet will no longer be able to access the rest of the internal network.

Practical example of securing a simple network



« Flat » network with a frontend firewall

Practical example of securing a simple network

The firewall prevents - the direct connection between the Internet and the internal network, but:

In case the WEB server presents a **vulnerability**, a hacker present on the Internet can potentially take **control of this server** and then **rebound on the internal network.**

We will therefore **segment** our network into **different zones of criticality**, in particular :

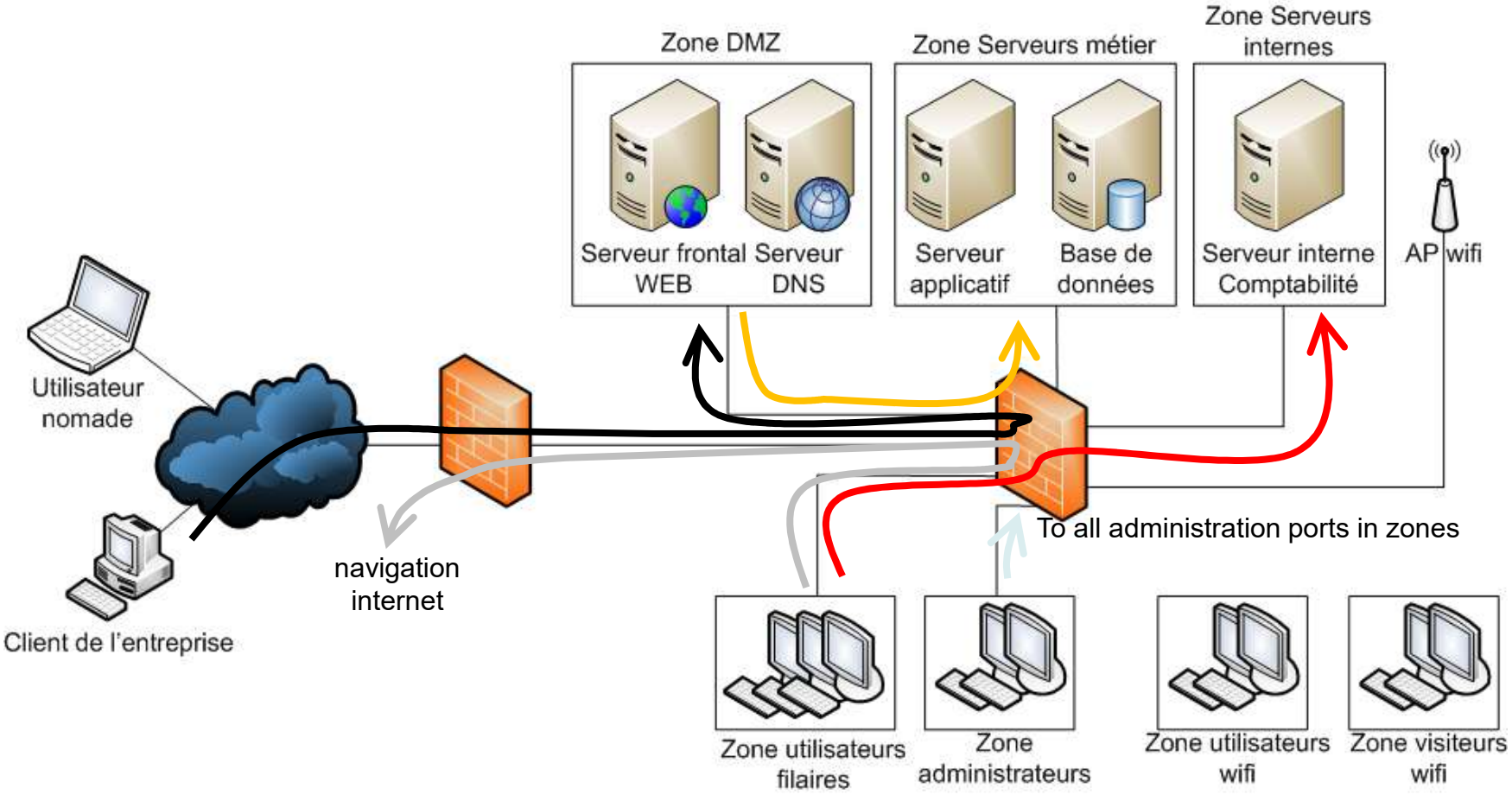
A **DMZ (demilitarized zone)** intended to host all the servers that must be accessible from the Internet, and only these. Thus, in the event of a fault in the web server, an attacker would have more difficulties to rebound on the internal network ;

- An area for the **company's internal servers** ;
- An area for **users' wired workstations ;**
- An area for **users' wifi workstations ;**
- A zone for the **visitors wifi stations ;**
- An area for **administrators' workstations**, because they need access to administrative interfaces (RDP, SSH ...).

In order for this network segmentation to be efficient, we **pass all (including internal) streams** through a second **(internal) firewall** so that only the streams we are going to configure are allowed.

Note: Segmented but unfiltered networks are unfortunately often observed. This is useless in terms of security, because all zones can communicate with one another.

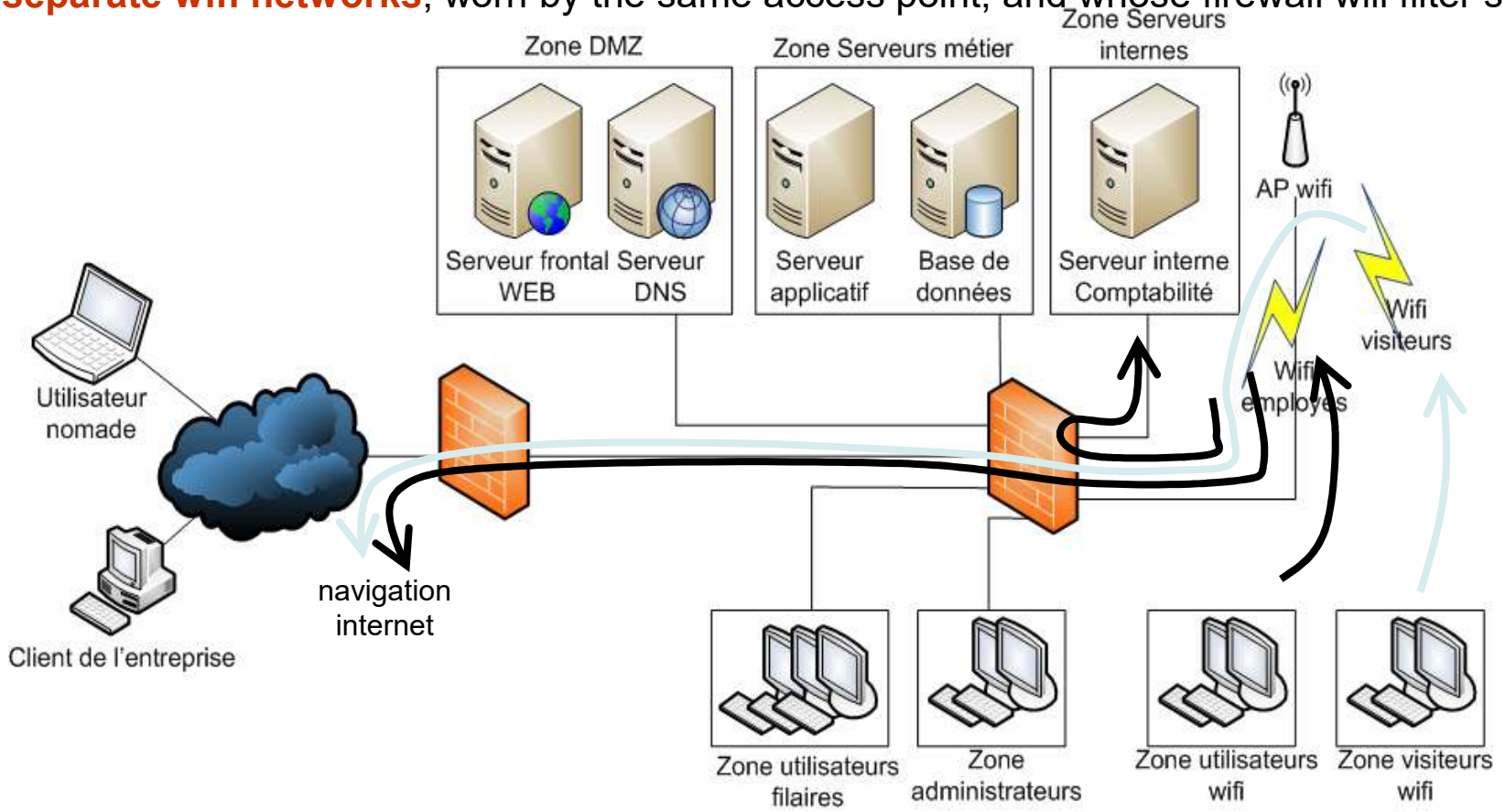
Practical example of securing a simple network



Network with segmented areas, and systematic filtering via the firewall, including internal streams.

Practical example of securing a simple network

The wifi access point must be accessible to visitors and internal employees. Since the need for access to resources is different for these two populations, we will implement two SSIDs (**two separate wifi networks**, worn by the same access point, and whose firewall will filter streams).



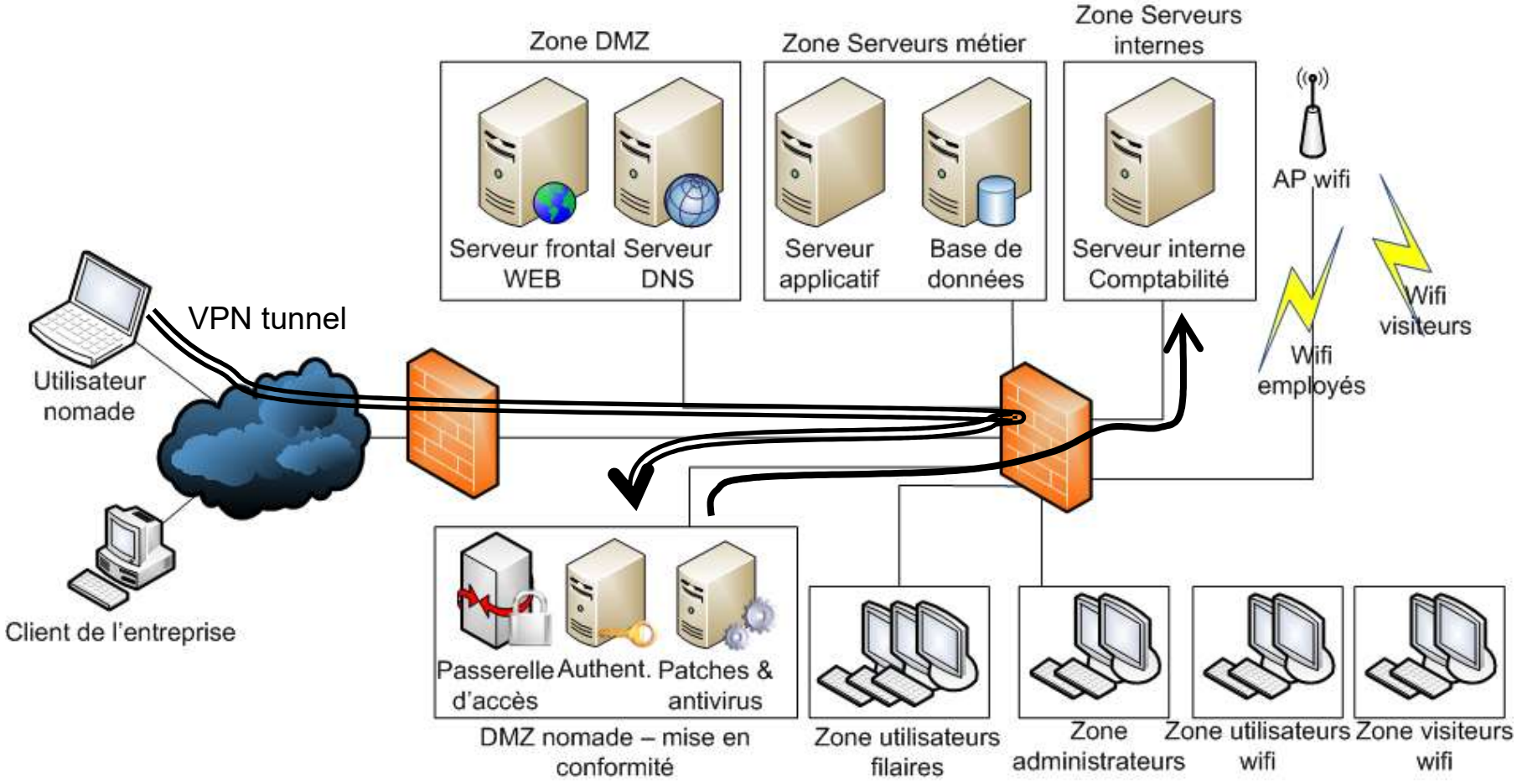
Two wifi networks, whose streams are filtered differently.

Practical example of securing a simple network

We must also allow **mobile users to connect to the internal network from the Internet**. This is done via a specific DMZ, called a compliance zone, whose role is the following :

- Provide the interface for access to the internal network from the Internet, usually via a **VPN tunnel**;
- **Check that the roaming station and its user are allowed** to connect remotely ;
- **Check the security level of the workstation** before allowing connection (**patches and anti-virus** updates in particular) ;
- If everything is OK, then **allow flows to the internal zones** (and only those that are necessary for the craft), **always passing through the firewall**.

Practical example of securing a simple network



Network with DMZ compliance for mobile workstations.

Practical example of securing a simple network

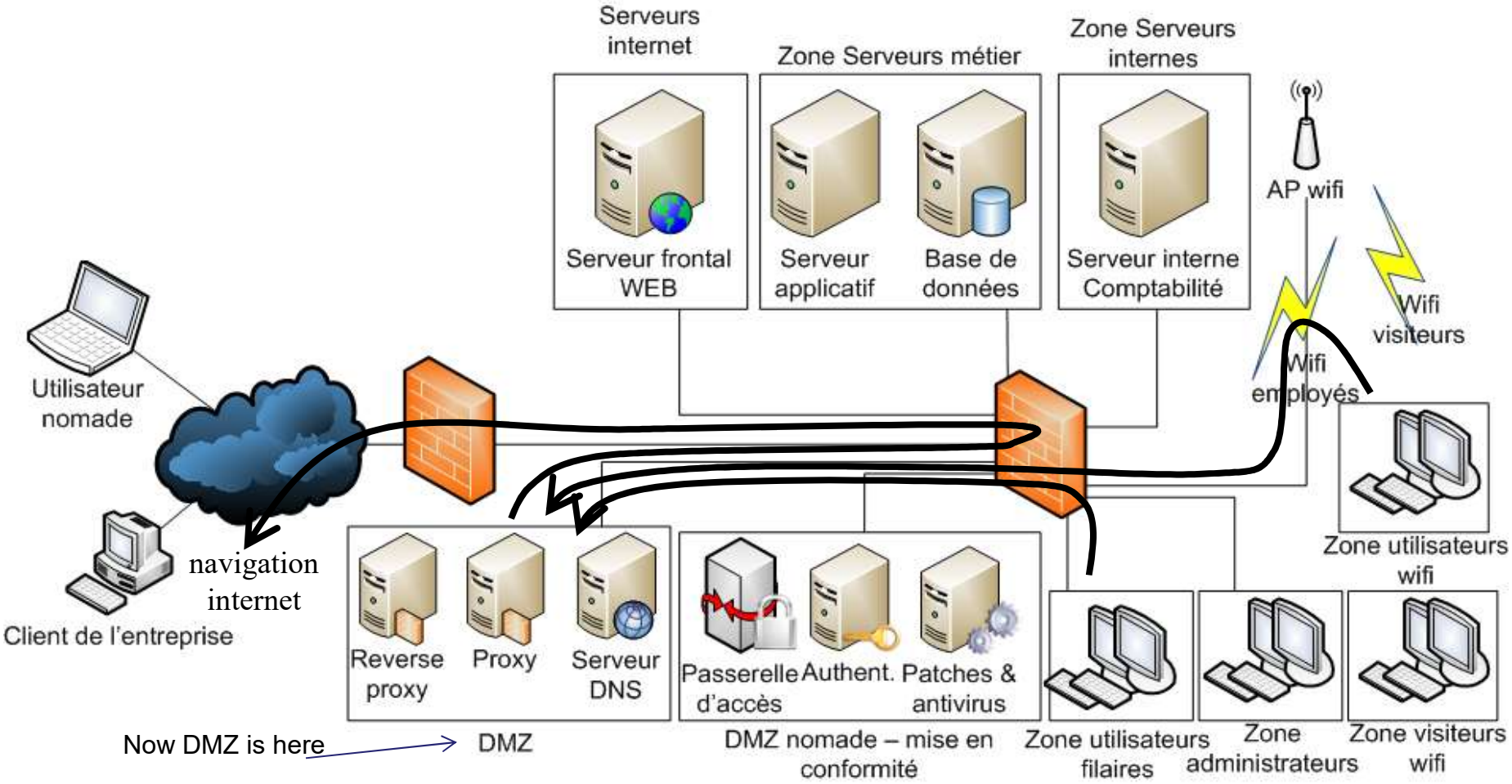
Finally, it would be desirable to **better filter inbound and outbound WEB traffic** :

- **Outbound traffic**: define the categories of WEB sites that employees are allowed to navigate, implement a black or white list of allowed / forbidden sites ;
- **Inbound traffic**: analyze WEB requests from the internet to the e-commerce server in order to intercept malicious requests (injection, malware, etc.).

We will therefore use **a proxy to analyze the outgoing flows**, and a **reverse-proxy to analyze the incoming flows**. As these devices are cut, they prevent users' workstations from being directly connected to the Internet while allowing them to navigate the authorized sites. The same remark for the WEB server: it is no longer connected directly on the Internet, it is the reverse-proxy that is now frontal.

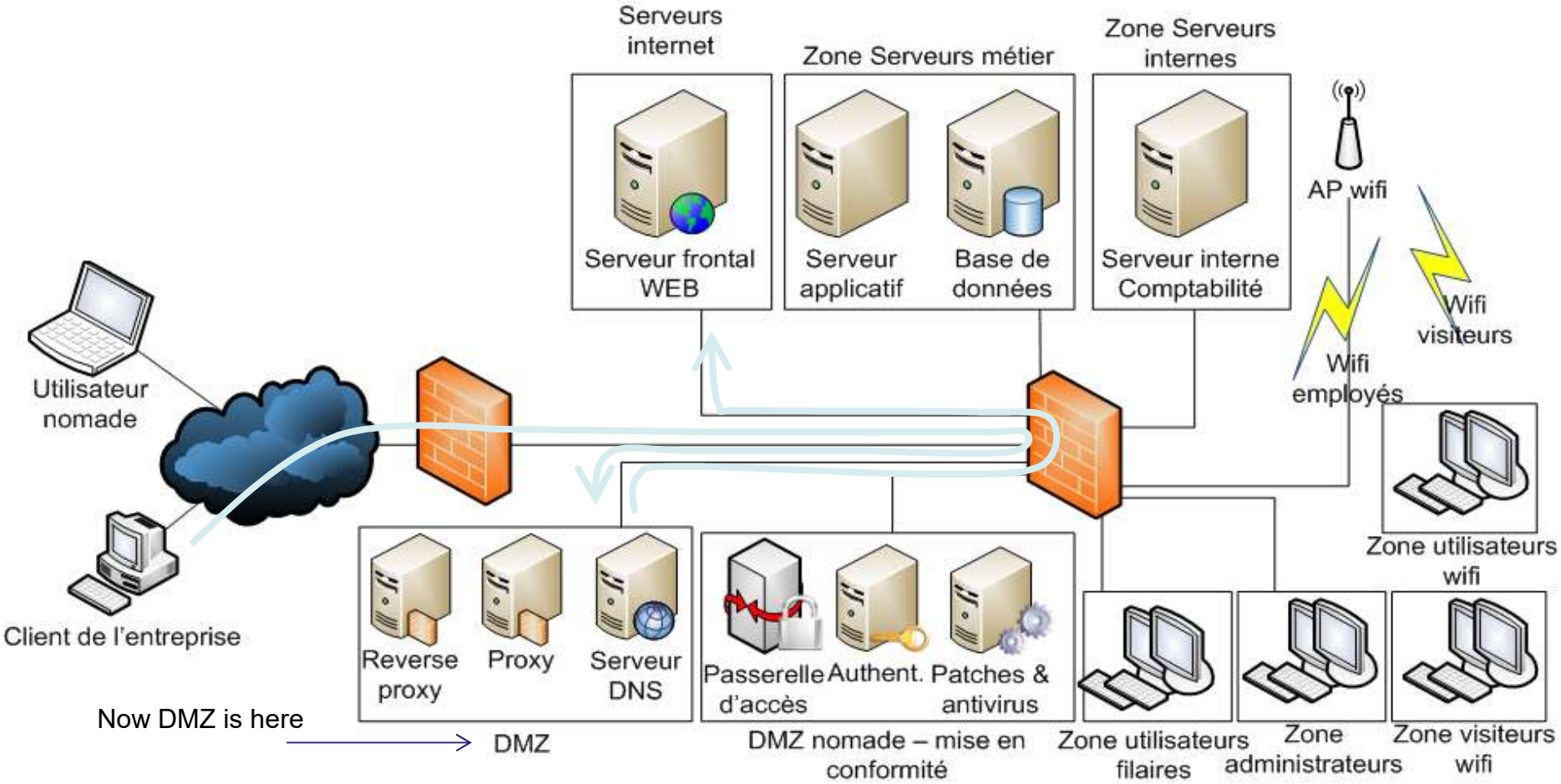
Since proxies and reverse-proxies are on the Internet front, they must be **placed in the DMZ**.

Practical example of securing a simple network



Network with a proxy and a reverse-proxy cutting the flows from / to Internet

Practical example of securing a simple network



Network with a proxy and a reverse-proxy cutting the flows from / to Internet

References

- Presentation of Eric WIESS
- La sécurité des réseaux-First steps, Tom Thomas, Cisco Press, 2005
- Les réseaux, édition 2005, G. Pujolle, Eyrolles 2004
- Cours de Jean-Luc Noizette, ESSTIN, Nancy, 2005
- S. Ghernaouti-Helie – *Sécurité informatique et réseaux* – Dunod, 2005

Exercises

- What is a firewall? Whose are its roles and functions?
- A firewall is a necessary but not sufficient security tool, why?
- Define the concept of perimetric security (demilitarized zone)
- Step 4 of the report on security: what kind of security technologies are we planning to implement? For what purpose ?
  - Compare with the results of the reflection at the end of step 3

Adress translation

- Network address translation(NAT) allows a private network to use public addresses to reach Internet network
  - Explain with some sentences how NAT works.
  - What it is the difference between static NAT and dynamic NAT ?
  - What are the advantages and disadvantages of NAT ?

Mail header

- Following a SPAM header. Could you explain why there are two different IP adresses in the header?

```
Received: from
  gw_05[192.168.227.29]
(cust-90-62.as01.chcg.eli.net
  [209.210.90.62]) by
  ns.tsp.co.kr with SMTP id
  LAA29540; Fri, 10 Oct 2008
  11:45:27 +0900
```