Université Grenoble Alpes

7. Security protocols

7.1 IPv4 & IPv6, Security issues

7.2 security Protocols

- 7.2.1 Ipsec
- 7.2.2 SSL/TLS

7.3 Applications

- 7.3.1 VPN
- 7.3.2 RADIUS Server

Université Grenoble Alpes

7.1 IPv4 & IPv6, Security issues

7.1.1 IPv4

- Protocol: set of rules determining the format of the exchanged messages
- IPv4 (Internet protocol version 4, currently used) does not integrate any service for security
  - Does not allow the authentication neither of the source nor of the destination of a packet
  - Does not warranty the confidentiality of the data transported
  - Does not allow the confidentiality of implied IP addresses
- IPv4 is a protocol “without connection”, it does not guarantee:
  - The data has reached the destination (possible loss of data)
  - Delivery of data to the good destination
  - The correct scheduling (sequencing) of the data

7.1.1 IPv4

- No quality of service (no recovery after an error)
- => implementation of the TCP protocol (Transmission Control Protocol) at the 4th layer, TCP offers a reliable transport service in connected mode, but strictly speaking does not offer security services

7.1.2 IPv6

- The needs are taken into account in *IPnG* (Internet Protocol next Generation) or *IPv6*:
  - To handle a larger address range
  - To be able to make a dynamic allocation of bandwidth in order to be able to support multimedia applications
  - To take into consideration security aspects

7.1.2 Main IPv6 characteristics (RFC 2460)

- *(Recall: RFC = Request For Comment)*
- Support for a wide and hierarchically arranged addressing
- Addresses coded on 16 bytes (128 bits) instead of 4
- Representation in the form of hexadecimal numbers separated by two points every two bytes:
  - Example: 0123:: 4567:: 89ab:: cdef:: 0123:: 4567:: 89ab:: cdef
- Dynamic allocation of bandwidth for multimedia applications
- Creations of virtual IP networks
- Support procedures for authentication and ciphering
- Simplified headings of packets in order to facilitate and accelerate the routing

7.1.2 Difficulties for the use of IPv6

- Economic and technological problem for its deployment
- Modification of the address managements on internet
- Installation of systems supporting both IPV4 and IPV6 versions, synchronization of the migration of the versions

Université Grenoble Alpes

7.2 Security protocols

Université Grenoble Alpes

7.2.1 IPSec protocol

Security solution which is compatible with IPv4 and IPv6
Presentation
AH
ESP
IKE

IPSec strategies

7.2.1 IPSec (IP Security)

- IPSec is a set of protocols standardized by the IETF (Internet Engineering Task Force) which allows to ensure a data protection (IP layer of the TCP/IP model)
- The protection proposed by IPSec is based on cryptographic services and provides the following functions:
  - *"Anti-re-reading"*: an IP packet protected by IPSec and intercepted by a pirate could not be re-used in order to establish a new session
  - *Confidentiality*: enciphering of the data encapsulated in an IP packet in order to make sure that they cannot be read during their transfer
  - *Authentication*: allows to ensure that a received data comes from the expected IP host (with which the IP security was negotiated)
  - *Integrity*: the data were not modified during their transfer

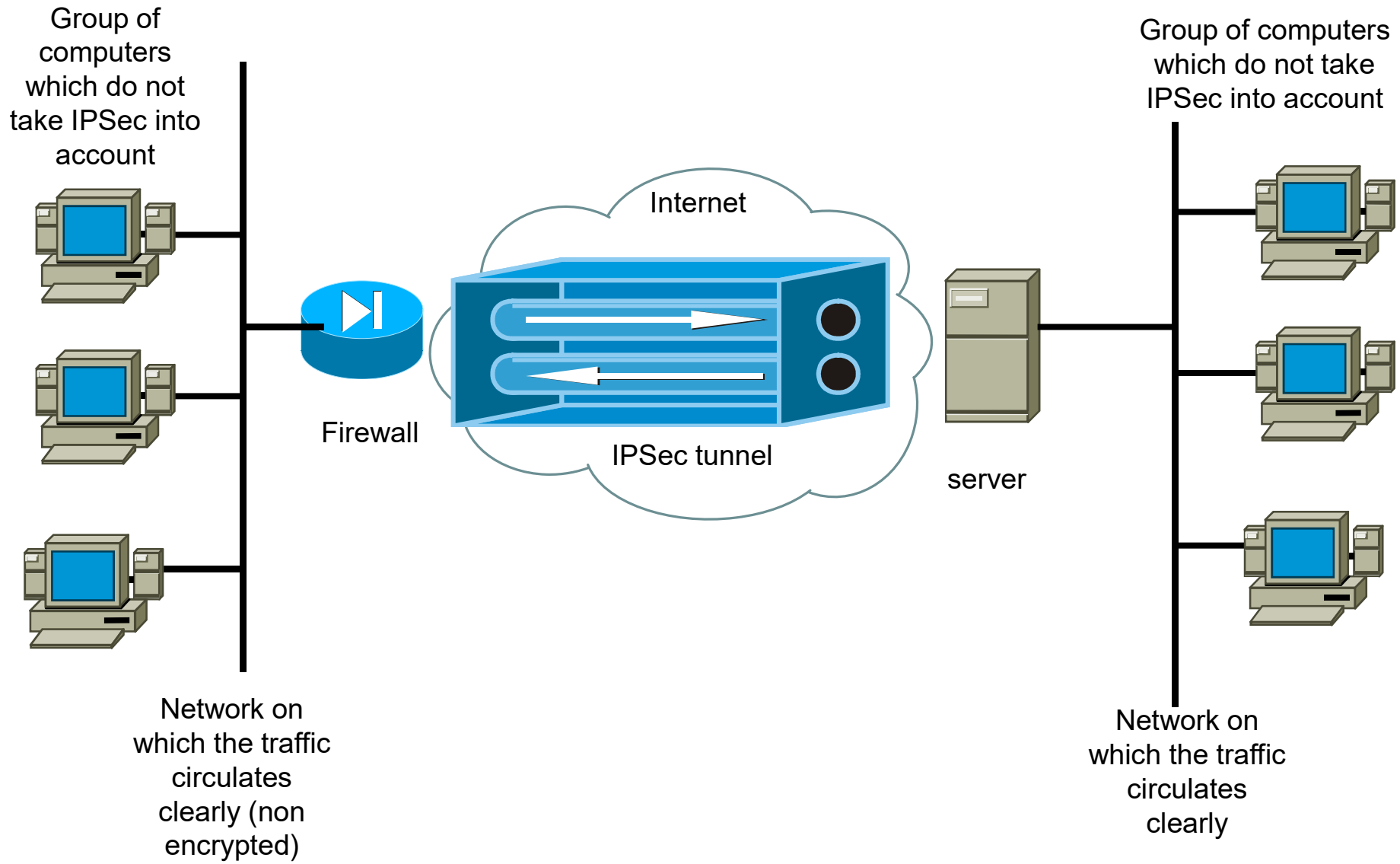
7.2.1 IPSec *Transport mode*

- Transport mode makes it possible to apply a security by IPSec from beginning to end
- Source and destination are the hosts taking charges of IPSec
  - Communication are safe from beginning to end
  - Blocking of certain types of traffic when the destination is open ports on a computer we would like to protect
    - Ex: a sensitive computer can have an IPSec strategy authorizing only a specific computer to reach this application, and blocking all the others

7.2.1 IPSec *Tunnel mode*

- Establishment of protected connections between two networks, when the gateways (firewall, router) are not able to use VPN technologies
- These are the gateways between the private network and the public network (Internet) which take the IPSec into account. The source and destination computers are not directly concerned

IPSec Tunnel mode, example



7.2.1 AH (Authentication Header) 1/3

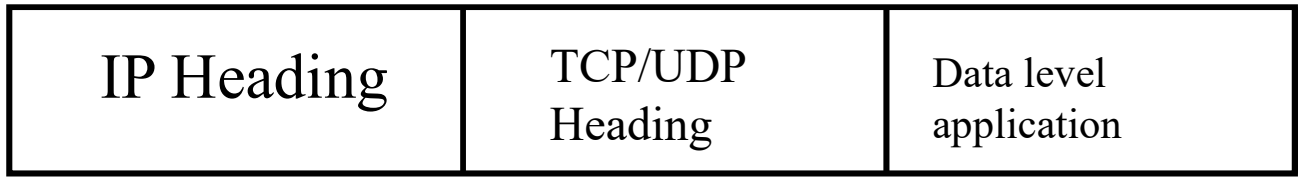
- Ensure the authentication, the integrity control and the anti-re-reading of the data encapsulated in an IP packet, as well as the IP heading itself

  $\Rightarrow$ It is so a protection against attacks using IP headings (ex: IP-spoofing)

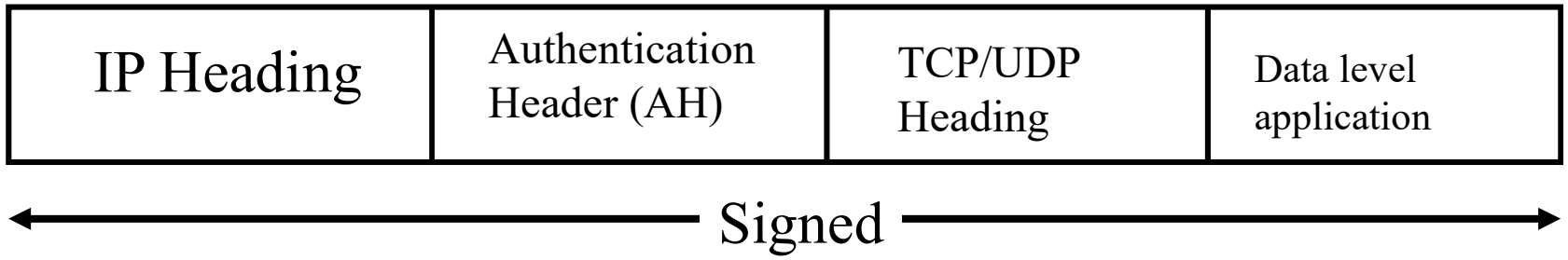
- N.B.: the integrity control does not take into account the bits of the IP heading since it is possible to modify them during their transit (ex: TTL field (lifespan) decremented when crossing a router)

7.2.1 AH 2/3

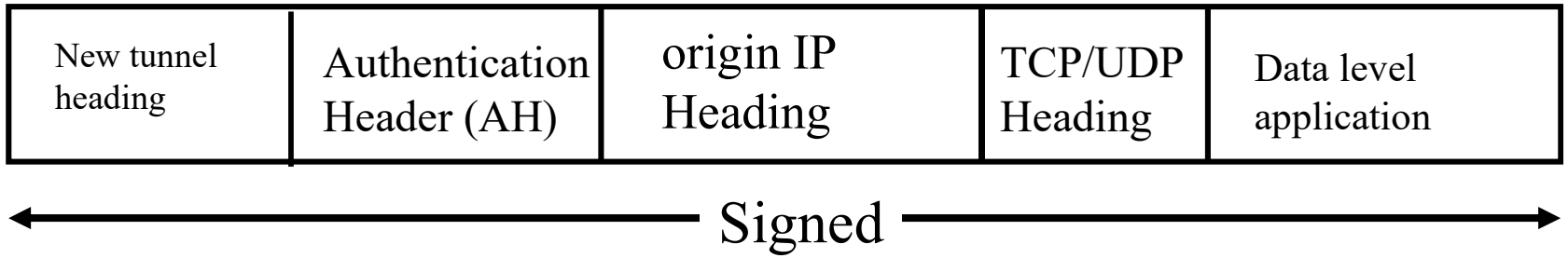
IPv4 packet



AH packet in transport mode



AH packet in tunnel mode



7.2.1 AH 3/3

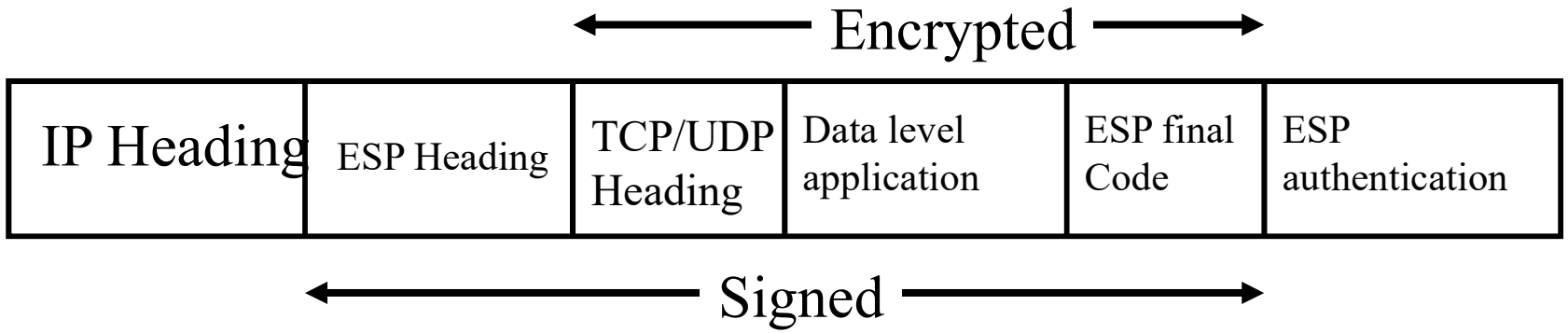
- AH uses the hashing algorithms according to
  - MD5 (Message Digest 5): 128 bits-hash
  - SHA1 (Secure Hash Algorithm): 160 bits-hash
- AH is defined in the RFC 2402

ESP (Encapsulating Security Payload)

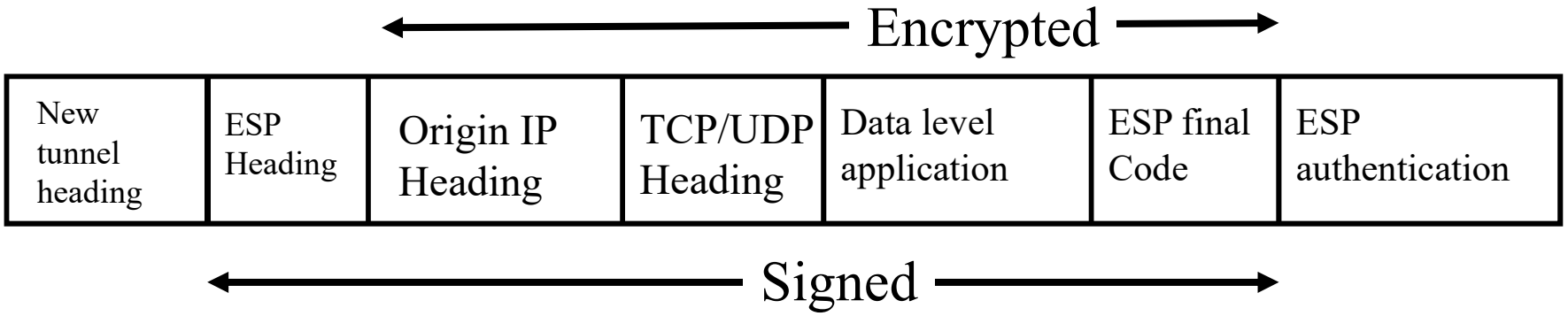
- Protocol ensuring the data confidentiality, by enciphering the contents of IP packets
  - N.B.: the headings are not encrypted, in order to be able to cross the routers!
- ESP can ensure an control integrity and an authentication, but only for the data encapsulated in IP packets
- ESP Protocol adds a heading in the IP packet

ESP

- Format of an ESP packet in transport mode



- Format of an ESP packet in tunnel mode



ESP

- Use the following hashing algorithms
  - MD5
  - SHA1
- Use the following encryption algorithms
  - DES
  - 3DES
- ESP is defined in RFC 2406

IPSec

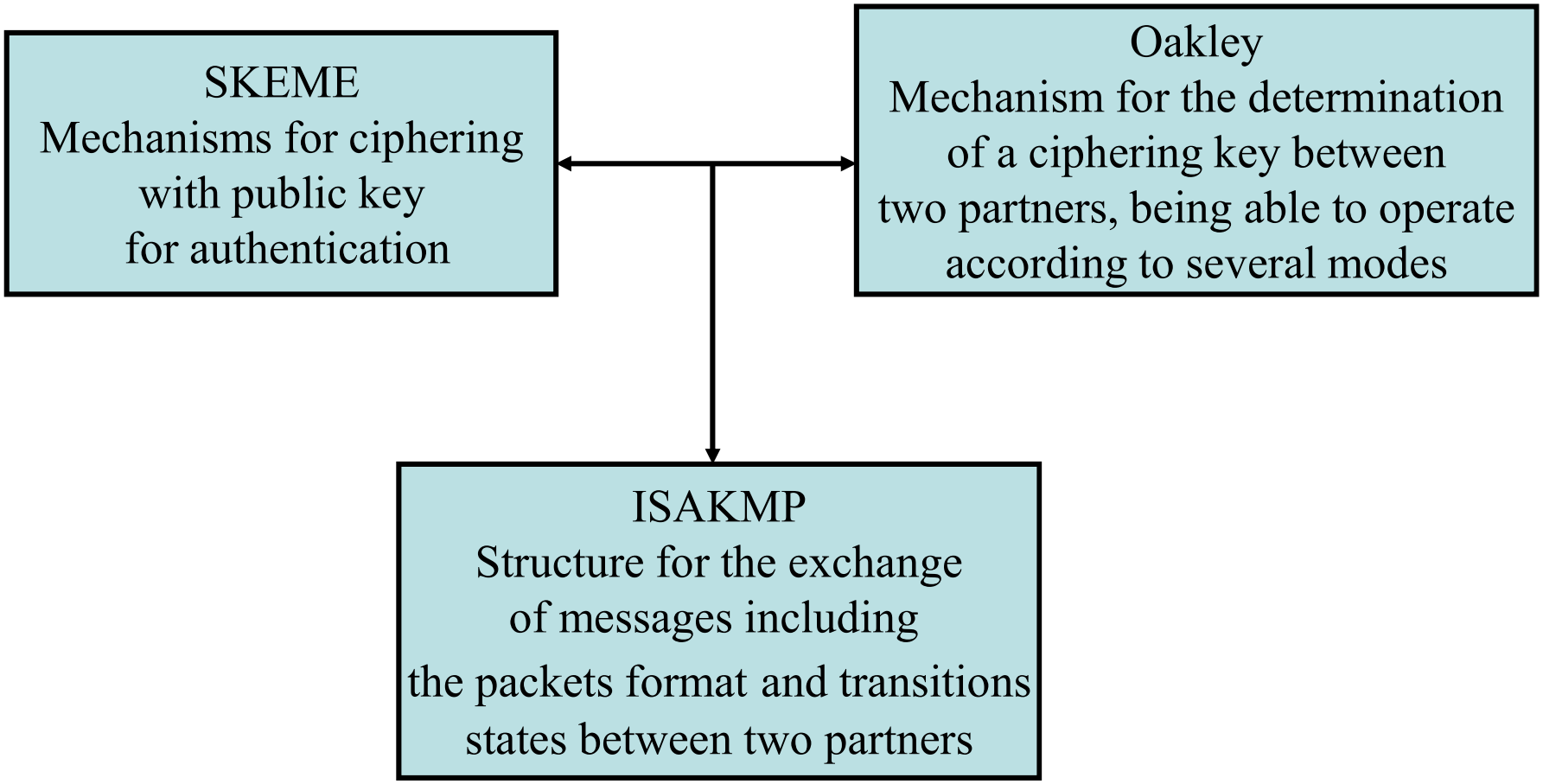
- In its most complex form (the most protected but also most consuming resources), an IPSec packet can use at the same time AH and ESP
- AH is an important consumer of CPU resources
- It is thus generally advised to use ESP alone, except if the integrity of the IP heading is a major element of the security policy
- There is hardware (accelerator cards) for IPSec implementation

Enciphering key management

- Oakley et SKEME (Secure Key Exchange Mechanism) : describes the way to exchange keys and defines services used by each exchange (based on Diffie-Hellmann exchange algorithm (RFC 2412)
- ISAKMP (Internet Security Association and Key Management Protocol) : this RFC (RFC 2408) defines procedures and packet formats to establish, negociate, modify, finish or cancel a security association. Formats are independent from key exchange protocols, from enciphering algorithms and from authentication mechanisms
- IKE (Internet Key Exchange) (RFC 2409) is an implementation of ISAKMP. IKE allows the realisation of key exchanges (authenticated keys) and the negociation of security services for security association

Protocols concerned by IKE

- IKE (Internet Key Exchange) (RFC 2409) is a hybrid protocol



IPSec strategy

- Set of parameters allowing to define how IP security must be applied to a data flow, and how the ciphering keys are generated
- One or more rules, each defining some filters, a method of authentication and filters actions

Default IPSec strategies

- Client (“simple response” strategy / *en réponse seule*)
  - Allows to forward the traffic normally, only one rule “default response rule” / “*règle de réponse par défaut*”, allowing to negotiate IPSec traffic if the distant host proposes it
- Server (ask for security / *demander la sécurité*)
  - Rule 1: negotiation for the entering and leaving IPSec traffic; if the distant computer does not use IPSec => non-protected communication
  - Rule 2: transmission of ICMP traffic without security negotiation
  - Rule 3: “default response rule” / “*règle de réponse par défaut*” (see above)

IPSec default strategies

- Server (requires security / *nécessite la sécurité*)
  - Rule 1: negotiation for the entering and leaving IPSec traffic; if the distant computer does not use IPSec => stopped communication
  - Rule 2: transmission of ICMP traffic without security negotiation
  - Rule 3: “default response rule” / “*règle de réponse par défaut*” (see above)
- “Default response rule” / “*règle de réponse par défaut*”
  - Allows to negotiate security with any host wishing to communicate in a protected way

Examination of the interaction between the rules

Direction of the traffic 	**No strategy**	**Client strategy** (simple response)	**Server strategy** (ask for security)	**Server strategy** (require security)
No strategy	Non-protected	Non-protected	Non-protected	No communication
Client strategy (simple response)	Non-protected	Non-protected	Secured	Secured
Server strategy (ask for security)	Non-protected	Secured	Secured	Secured
Server strategy (require security)	No communication	Secured	Secured	Secured

Université Grenoble Alpes

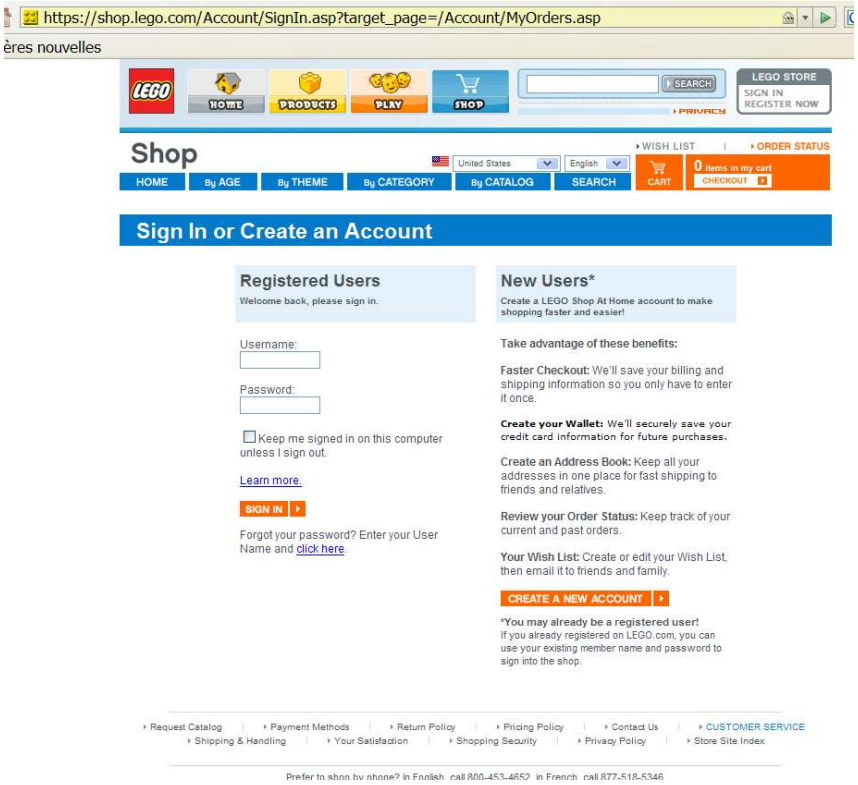
7.2.2 SSL/TLS

SSL (Secure Socket Layer)

- Data enciphering within the network protocol
- Guarantees
  - Identity of both parts
  - Data confidentiality from beginning to end
  - => data enciphering thus impossibility to read user names and passwords
  - data Integrity by the use of hash
- Generally based on TCP/IP
  - Allowing to guarantee the good arrival and the good schedule of data
- Web browsers equipped with SSL
  - Firefox, Konqueror, Internet Explorer, Safari…

SSL protocol

- SSL appeared in 1994 in Mosaic
- Web pages using SSL: HTTPS
- 1996: work for the formalization and standardization of SSL by the IETF



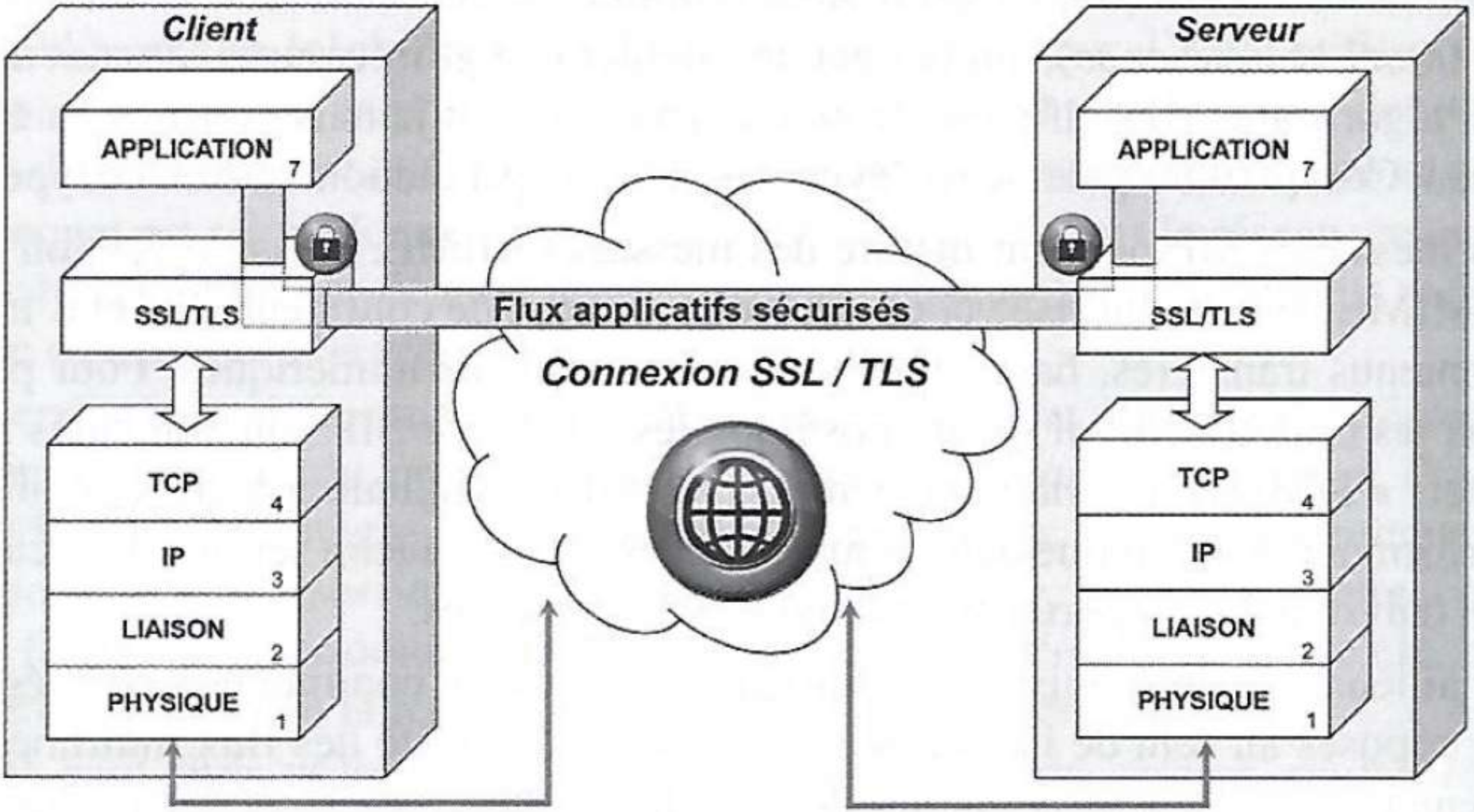


Figure 9.1 – La sécurité des flux applicatifs par SSL.

SSL: properties

- authentication
  - Proof of the client identity by certificates exchange
- Confidentiality
  - Encryption of the data by the use of a shared key and via the negotiation of the encryption algorithms
- Authentication and confidentiality phases take place during the stage of “negotiation”, also called “initialization” of SSL session
- Integrity
  - SSL checks that the data were not modified

SSL: facility of use

- Designed to be transparent for the end-user
  - The user needs only to be connected to the desired address (ex: https://...)
- RFC 1738 specifies the format
  - Web server port 80 but in SSL port 443
- A VPN based on SSL is easier to maintain than a VPN based on IPSec

Implementation of SSL

- A central server
- The client uses a communication software able to "speak" SSL
  - Browser
    - can use HTTPS
    - contains natively root SSL certificates coming from recognised certification authorities
- Possibilities to download additional software for the client computer
  - Plug-ins
  - Applets
- SSL may also be deployed on specific hardware solutions

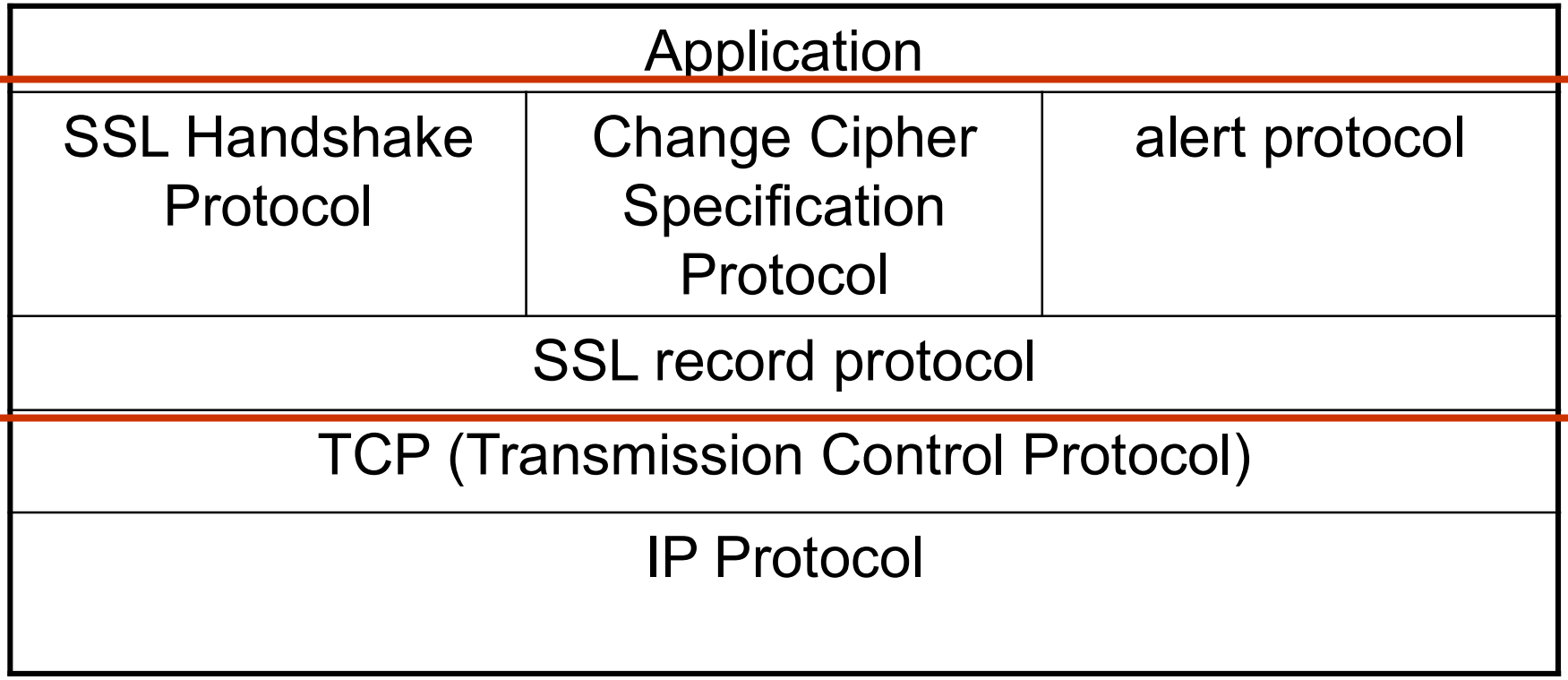
SSL: cryptography

- Symmetrical cryptography for data protection
  - Common Key (session key)
- Asymmetrical cryptography for the exchange of the session key

SSLv3

- More advanced version of SSL
  - Generator of keys
  - Hashing functions
  - Encryption algorithms
  - Management of the certificates
- Properties
  - Protocol for the change of specification: possible modification of the encryption algorithm during the communication to guarantee the confidentiality
  - Alert protocol allowing to send the alerts, accompanied by their importance (ex: unknown certificate, revoked, expired). High level alerts may cause the stop of the communication
  - Handshake protocol
    - authentication of the server by the client
    - negotiation of the protocol version
    - selection of the encryption algorithms
    - use of public-key encryption techniques for the distribution of secret keys
    - establishment of enciphered SSL connections
  - SRP recording Protocol (SSL Record Layer): encapsulation of the protocols located just above, like the Handshake protocol

Structure of the SSLv3 protocol



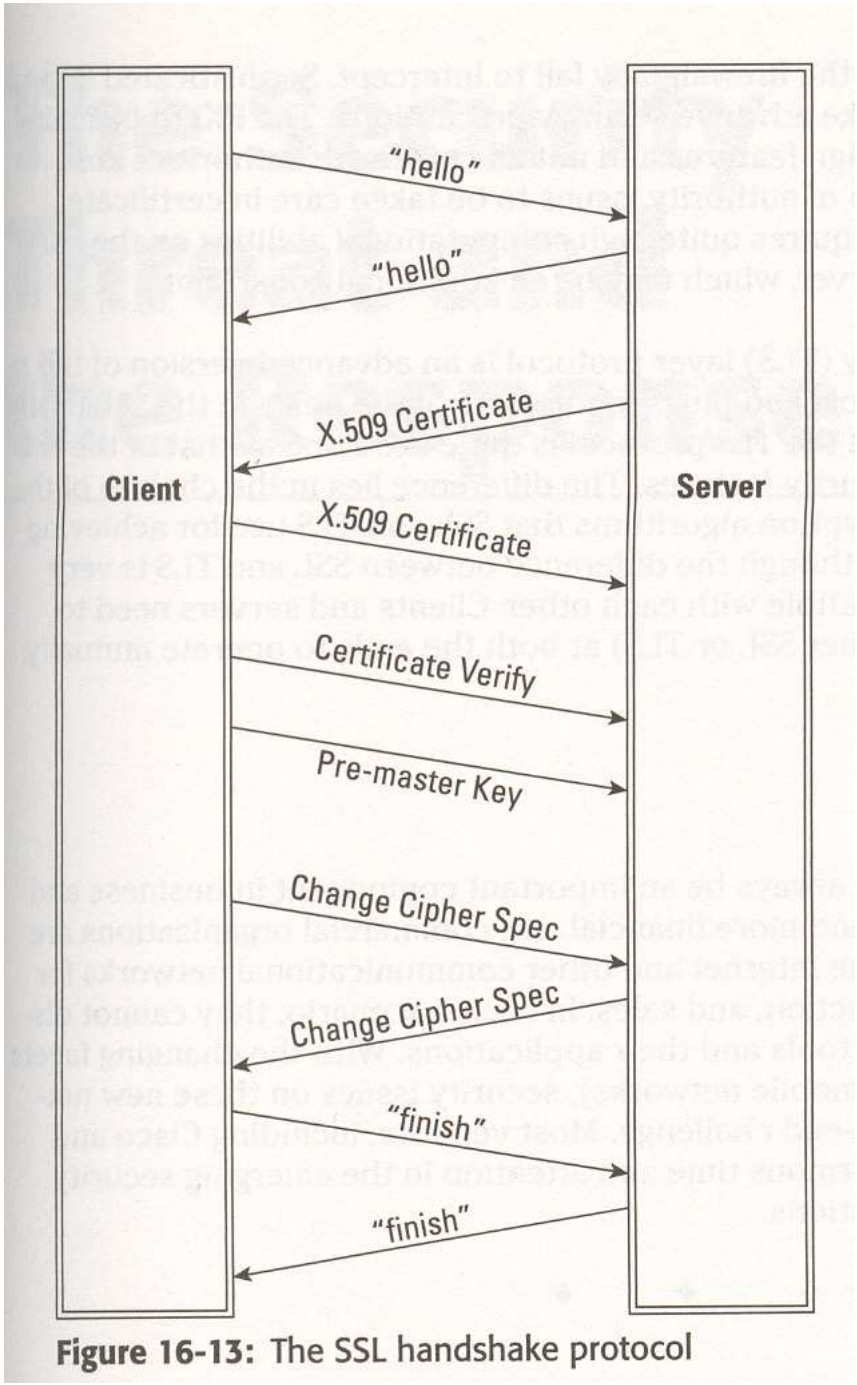


Figure 16-13: The SSL handshake protocol

SSL (Secure Socket Layer) et TLS (Transport Layer Security)

- SSL v2 and v3 obsolete since 2014 because of sevral security vulnerabilities
- TLS: new version, different algorithm, same functionalities (TLS ~ SSLv3)
- New version TLS 1.3 (June 2018) : abandonment of obsolete enciphering algorithms (MD5, SHA-224) to use Chacha20, Poly1305, Ed25519, x448 et X25519.
- BE CAREFUL about server configurations which allows retro-compatibilities with obsolete versions of cryptographic software (TLS 1.3 also forbids “downgrading”)
- TLS 1.3 is faster than previous versions
- Encryption of data within the network protocol
- Guarantees
  - Identities of both parts
  - End-to-end Confidentiality of data
  - => encryption of data so impossibility to read passwords and user names
  - Data integrity by using hash
- Is based generally on TCP/IP
  - Allows guaranteeing data order and controlling data arrival
- Web browser are equipped
  - Firefox, Konqueror, Internet Explorer, Safari, Chrome…

SSL/TLS

- Applications
  - Electronic Commerce
  - Communications Security with HTTPS
  - FTPs
  - Protected Copies
  - SSH
  - …

SSL/TLS Implementations

- OpenSSL the most widespread
- SChannel for Microsoft
- Secure Transport for Apple
- NSS for Mozilla and Chrome
- Cryptlib for banking
- GnuTLS for Open Source projects
- JSSE is an extension for Java applications to benefit SSL/TLS services
- MatrixSSL allows SSL/TLS services for embedded systems
- mbedSSL (previously PolarSSL), bought by ARM, for embedded systems

SSL/TLS Implementations

- OpenSSL the most widespread
- SChannel for Microsoft
- Secure Transport for Apple
- NSS for Mozilla and Chrome
- Cryptlib for banking
- GnuTLS for Open Source projects
- JSSE is an extension for Java applications to benefit SSL/TLS services
- MatrixSSL allows SSL/TLS services for embedded systems
- mbedSSL (previously PolarSSL), bought by ARM, for embedded systems

7.3 Applications

7.3.1 virtual private networks (VPN)

7.3.2 RADIUS servers

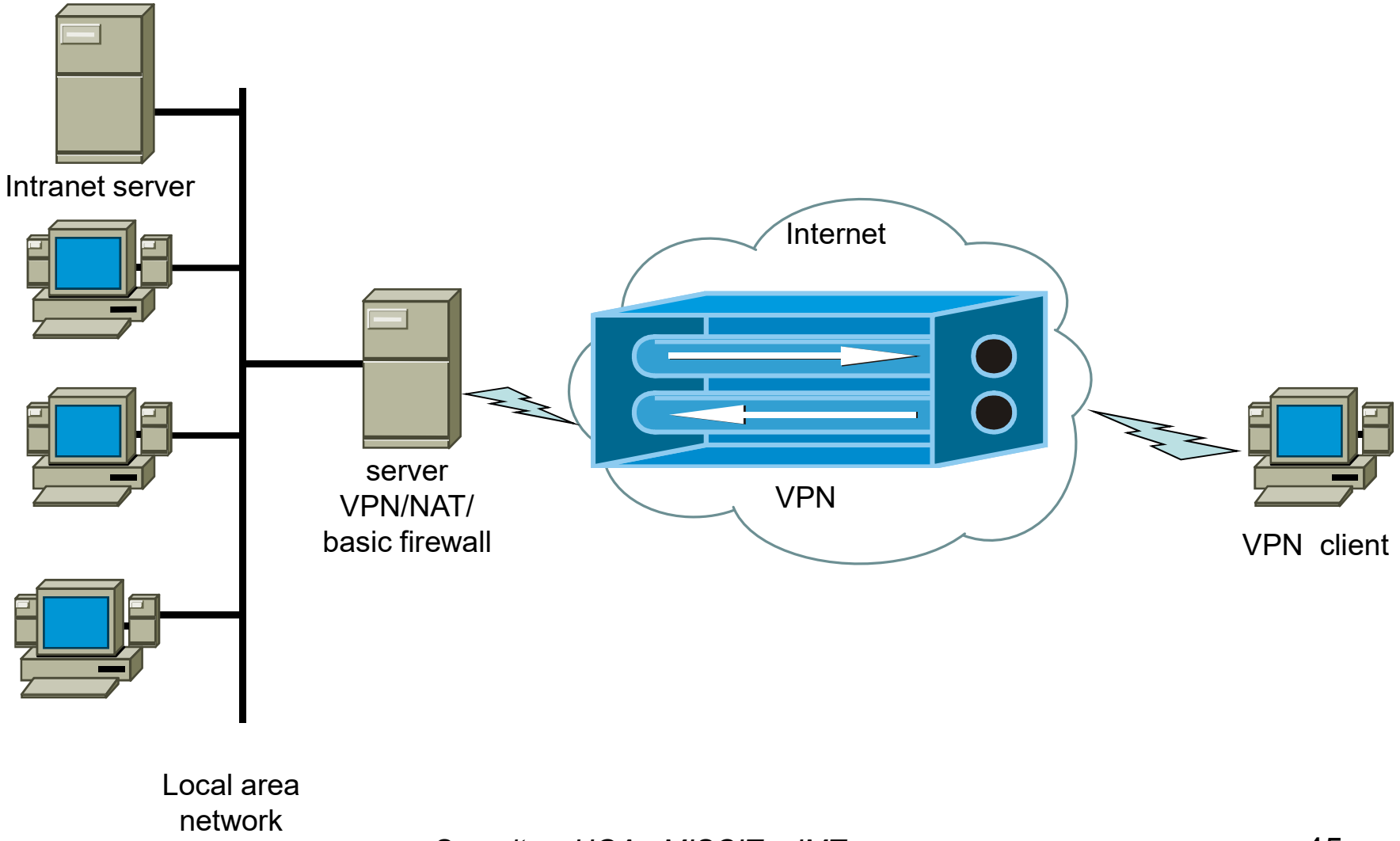
7.3.1 Some considerations about VPN

- VPN and distant access
  - To allow users located physically out of the corporate network of being able to connect itself to the corporate network
- VPN are considered as a particular class of shared networks
  - Resources of a real network shared between several sub-networks
- management Information to be taken into account
  - Topology: determination of the access points towards the sites which must be inter-connected by the VPN
  - Addressing: localization of the access points and the sites which must be inter-connected by the VPN
  - Routing: possibility of reaching the sites of the VPN
  - security Information: establishment and activation of the filters allowing or not the packets to cross them
  - quality of service Information: parameters for the control of the resources necessary for the quality of service

7.3.1 Some considerations about VPN

- level 2 VPN (frame): ex: VPN composed of Ethernet networks
- level 3 VPN (packet): ex: VPN composed of IP networks => the most widespread at the company level because integrating all IP functionalities
- level 7 VPN (application): ex: VPN set up for an application, such as HTTP
- VPN = extension of the ***private network*** of the company, ***virtually*** by the means of the public network
- ! The concept of security misses the basic definition of the VPN! => must be studied in particular (ex: use of IPSec, SSL)

7.3.1 VPN server in the periphery of the network (1/2)

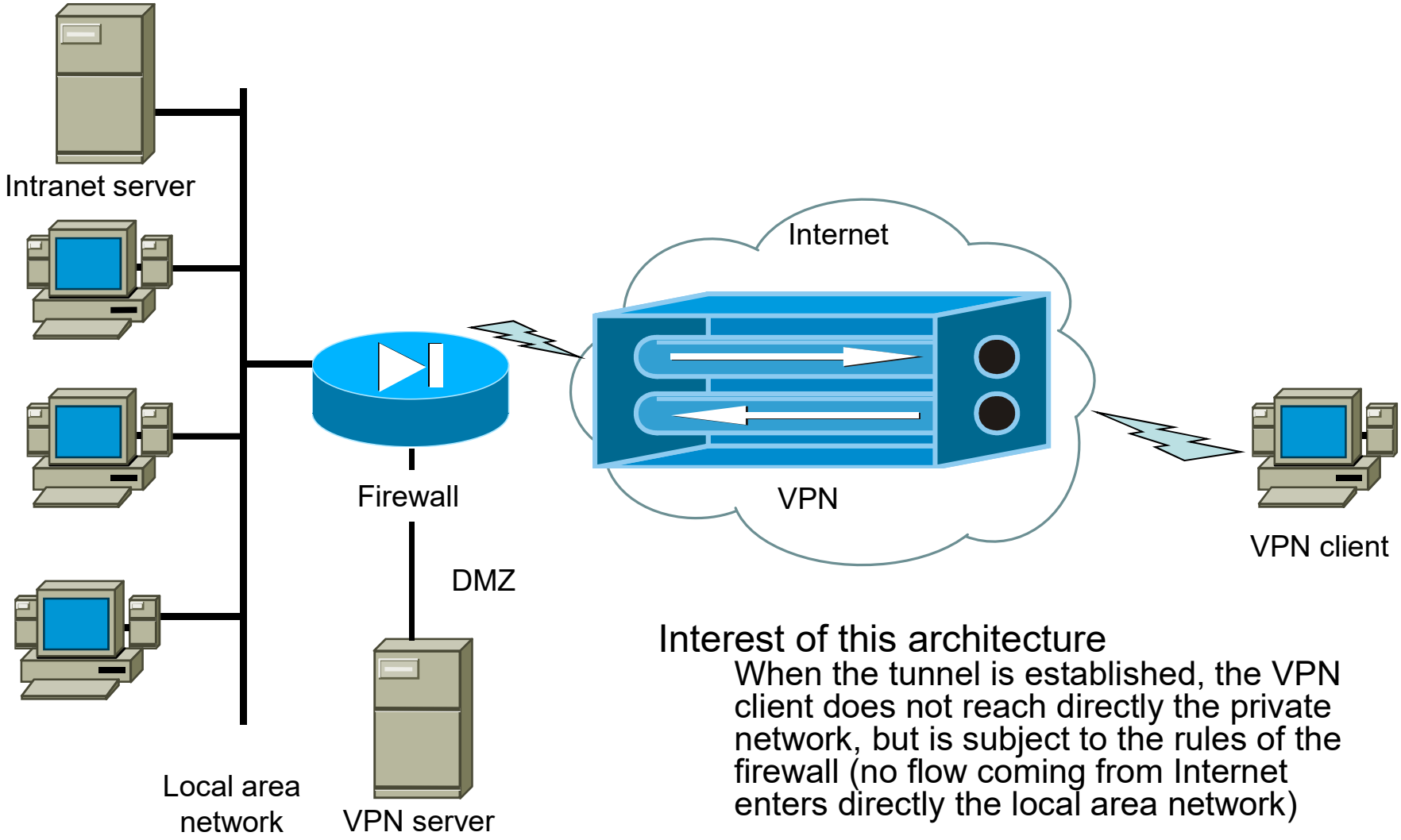


7.3.1 VPN server in the periphery of the network (2/2)

Necessary Pre-requisites for the installation of a VPN server

- VPN server must be connected to Internet (generally via the supplier of access Internet)
- VPN server must have a fixed IP public address or a corresponding DNS name
- VPN server must comply with the basic security rules
  - De-activate all the useless services on the server
  - Activate a firewall on the server
  - Use complex passwords strategies, or a “strong” authentication (smart card, biometric recognition)
- Check that the supplier of Internet access does not apply a filter to the router which connects you to Internet, and that the internet subscription allows to make flows enter

7.3.1 VPN server in a DMZ



Interest of this architecture

When the tunnel is established, the VPN client does not reach directly the private network, but is subject to the rules of the firewall (no flow coming from Internet enters directly the local area network)

7.3.1 Other aspects about VPN

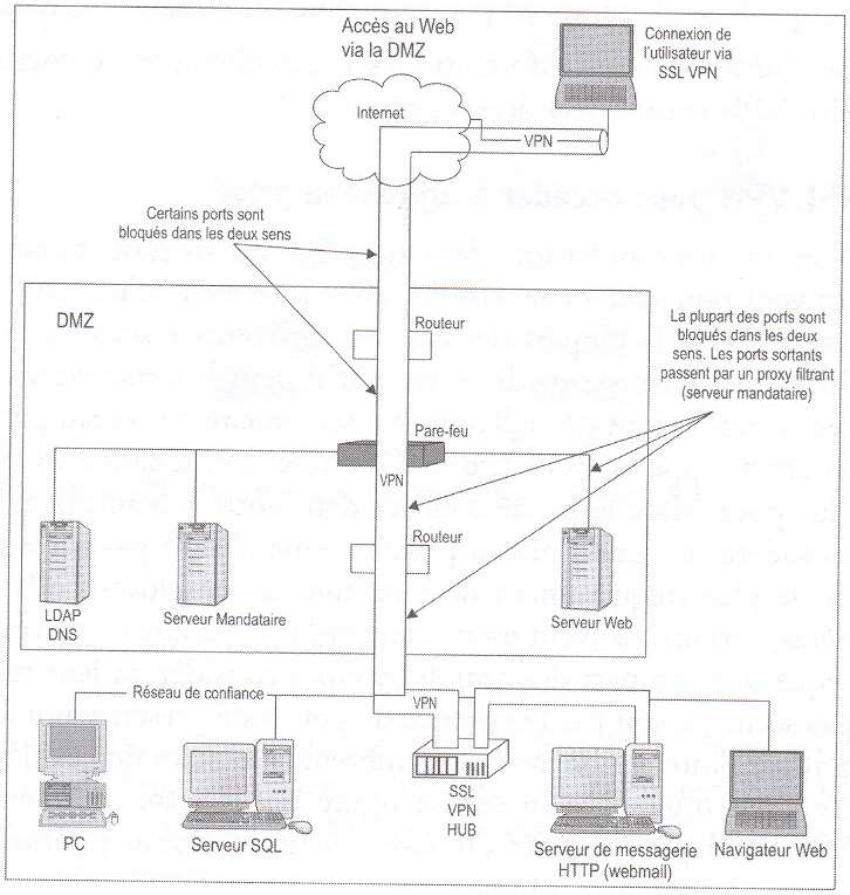
- It is possible to inter-connect two private networks through VPN
  - distant access VPN: relation between two sites of a company
  - intersite VPN : relation between a client and his supplier
- Use of other VPN-compatible devices: smart phone
- It is possible to use a secured phone (ex : VoIP SoftPhone application)

7.3.1 Advantages of VPNs

- Possibility for employees abroad to use a local connection to Internet and their VPN software client to be connected to the corporate network.
- Improvement of the productivity of the users because they connect in a protected way to the company resources independently of the geographical area where they are
- Cheapest costs thanks to the replacement of specialised WAN lines by direct broadband internet connections (distant computers can communicate through an intersite VPN)
- A large company can simplify the topology of its infrastructure by adding VPN to strategic sites

Models for the installation of SSL VPN: Access via a SSL VPN server to certain peripherals of the internal network

- Client connected via Internet (non-sure) to a SSL VPN server located in the internal network

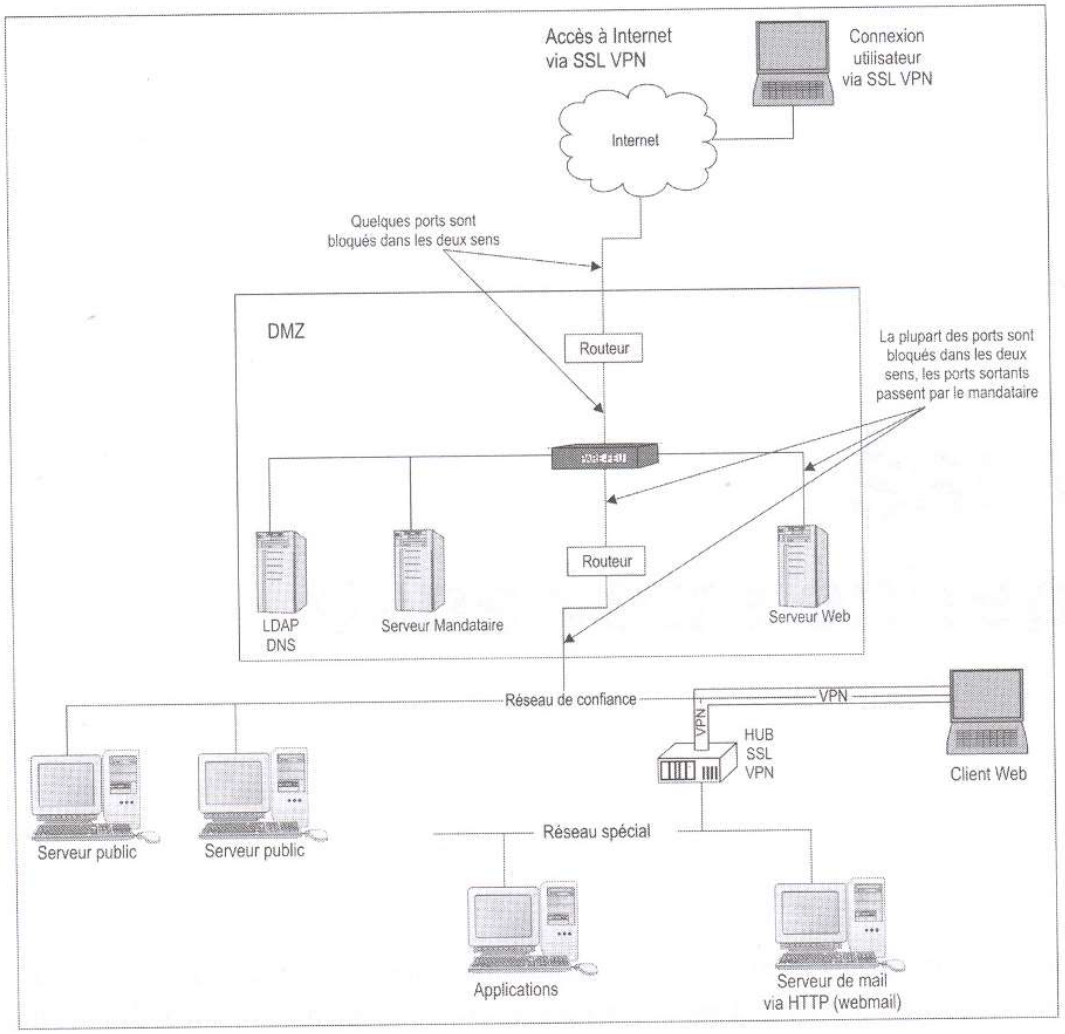


Models for the installation of SSL VPN: Access via a SSL VPN server to certain peripherals of the internal network

- Network frames routed in the DMZ
  - They arrive on the first router (border router)
  - The router will assign an IP of the DMZ to this connection
  - The DMZ checks then this connection
    - Inscription in the logs (history of connection)
    - Detection of the attacks of denial of service
    - …
- If all is correct, connection is transmitted to the router located between the DMZ and the internal network
  - The **destination** address is then modified again to use the internal SSL VPN server IP address (located within the internal network)
- The frame arrives to the internal SSL VPN server
  - SSL server will ensure additional checks, after deciphering the tunnel
    - authentication of the client
    - Negotiation of the encryption protocols
  - The communication could be transmitted to the required server (example: mail server)

Models for the installation of SSL VPN: Access via a SSL VPN server to a special network dedicated to the protected distant accesses

- SSL VPN to reach a private network



Models for the installation of SSL VPN: Access via a SSL VPN server to a special network dedicated to the protected distant accesses

- Example of the large companies
  - Several inter-connected private networks
  - Interconnection by several access suppliers (ISP: Internet Service Provider)
  - Use of POP (Point of Presence), access points to Internet => important security points
  - Protection against company employees
- Use of SSL VPN to provide a sure access to a special internal network from an internal network with limited confidence (hierarchy of internal networks)

SSL VPN at the application level

- Why?
- Many peripherals prohibit the creation of level-3 communication channels, but authorize the level-7 communications through a Web browser
- The most elementary security policy prohibit to connect to a corporate network a computer from a cybercafé or borrowed to anybody
- Disadvantage: very few widespread standards at the application level
- Communication at the layers 6 or 7 level => important impact for security

Advantages SSL VPN vs. proxy

- To reach non web applications
- Accesses to the files, printers and other resources
  - Mounting distant file
  - Web Interface for access to the files
- Access to the printers or other resources
- telnet access, access to terminals
  - Telnet, SSH, Putty…
- terminal servers
- Access to an Intranet
  - Via a non routable private address
  - Via a non published DNS domain (ex: gtr.iut)
- Coherent and ergonomic interface for distant access
- Access, if needed, with the internal network of the company (SSL VPN integrates security functionalities)

Access to the corporate internal network

- Establishment of a network connection through the SSL tunnel
  - Level 3
  - The SSL server sends a program to the client (ActiveX or Java applet) which creates a virtual network interface
  - The client receives an IP address from the internal network
  - Information frames are completely encrypted (from beginning to end)
- Two types of tunnel
  - Complete Tunnel: all the network flow passes through the tunnel => flow towards the internal network and flow towards Internet
  - Partial Tunnel: only the connections towards the internal network pass through the tunnel

Security of a SSL VPN access
1. Identification and authorizations

- Identification
  - Passwords
  - Single use passwords
    - From a passwords list
    - Hardware or software peripheral capable of generating single passwords (as a function of the time, a key…)
    - Challenge-response technique
  - Biometric information
  - Client digital certificates
    - Require a specific and “confident” peripheral
  - Smart cards or USB key
    - Contain a digital certificate which cannot be extracted. Only a digital signature is provided, proving the identity of the user

Security of a SSL VPN access
2. Client security

- Significant data in a non-secure place
  - Data coming from the corporate network on the laptop
  - Cache (browsers + files)
  - Non standard cache (used by some applications (software)…)
  - Temporary files (files attached to mail)
  - Memorization of e-mail addresses (when one fills a form by Internet) or Web addresses (in browser)
  - Cookies
  - Navigation History
  - Swap (exchange file, or auxiliary memory): can be used to store significant data (recovery is difficult, but not impossible)

Security of a SSL VPN access
2. Client security

- Possible corrections
  - Use NOCACHE command in the browser
    - NOCACHE avoids the storage of the received elements
    - Can bring dysfunctions (at the opening of a pdf or Word file for example)
  - To remove all the data at the end of the session, which is difficult:
    - Browser falls down
    - Closing the browser without disconnection
    - Bug of the computer…
  - To use an encrypted storage removed at the end of the session
    - Storage of all session information in a virtual disk
    - Removal of the virtual disk at the end of the session => if the system falls down, the disk can be re-initialised at boot; anyway, the encrypted contents cannot be read
    - Difficulty: this solution does not run with every programs

Security of a SSL VPN access
2. Client security

- Erasing of files
  - Simple “erase” on an operating system does not erase the file physically
  - Military standards: a physical erasing means that one rewrites on the file at least three times random suites of 0 and 1
- Automatic closing of session at the end of a certain time of inactivity
  - Prefer the solutions which consist in warning the user (ex: “are you still present? ” requiring to click on YES preventing connection from stopping) one or two minutes before the end of the session

Security of a SSL VPN access
2. Client security

- Virus entering the internal network via SSL VPN
- Solutions
  - Check the presence of anti-virus on the client computer (activation, last update)
    - Before giving access
  - Prohibit sending of files
  - To base on the corporate internal anti-virus
    - Files sent or attached to e-mail are scanned by the server on their arrival

Security of a SSL VPN access
2. Client security

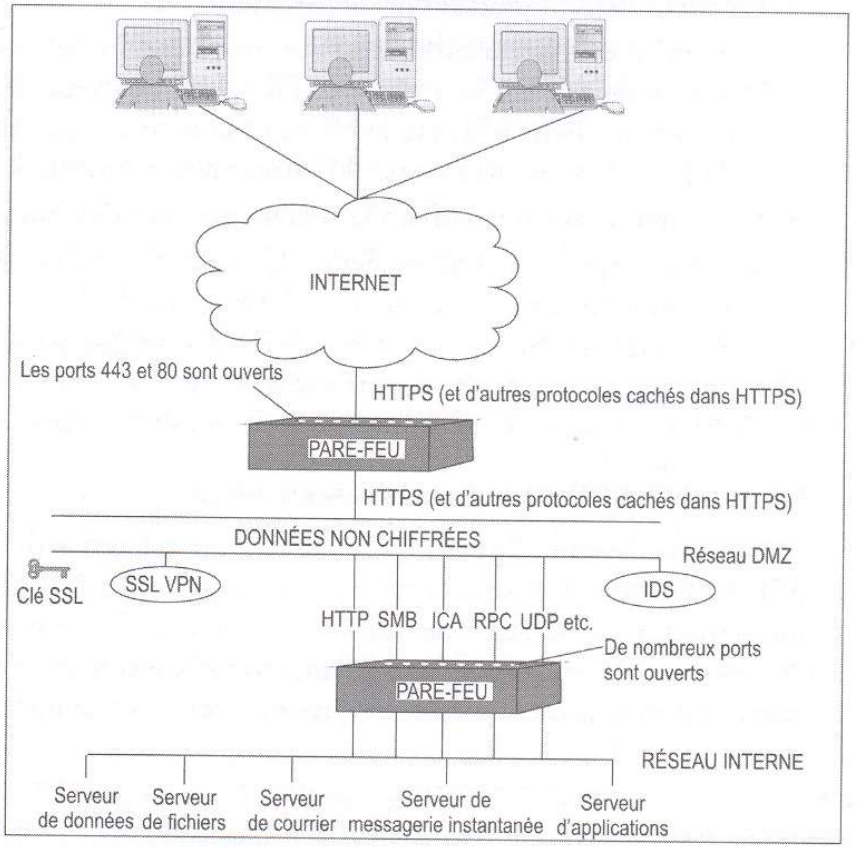
- A worm reaches the internal network via SSL VPN
- Solution: to prohibit connection to a computer which is not protected against the worms
  - Use of personal firewalls (do not let pass the non-desired network traffic, and so the worms)
  - Use of application firewall (with filtering rules)

Access rights according to the security of the distant peripheral

Security of the distant peripheral	Security of the distant peripheral	Security of the distant peripheral	Access rights on SSL VPN	Access rights on SSL VPN	Access rights on SSL VPN	Access rights on SSL VPN
Confidence computer?	**Installed and updated antivirus?**	**Possibility of removing the temporary files?**	**Authorization for e-mail consultation**	**Authorization for e-mail sending**	**Authorization for opening attached files**	**Authorization for sending attached files**
No	Yes	Yes	Yes	Yes	Yes	Yes
No	Yes	No	Yes	Yes	No	Yes
No	No	Yes	Yes	Yes	Yes	No
No	No	No	Yes	Yes	No	No
Yes, confidence level II	Yes	Yes/No	Yes	Yes	Yes	Yes
Yes, confidence level II	No	Yes/No	Yes	Yes	Yes	No
Yes, confidence level I	Yes/No	Yes/No	Yes	Yes	Yes	Yes

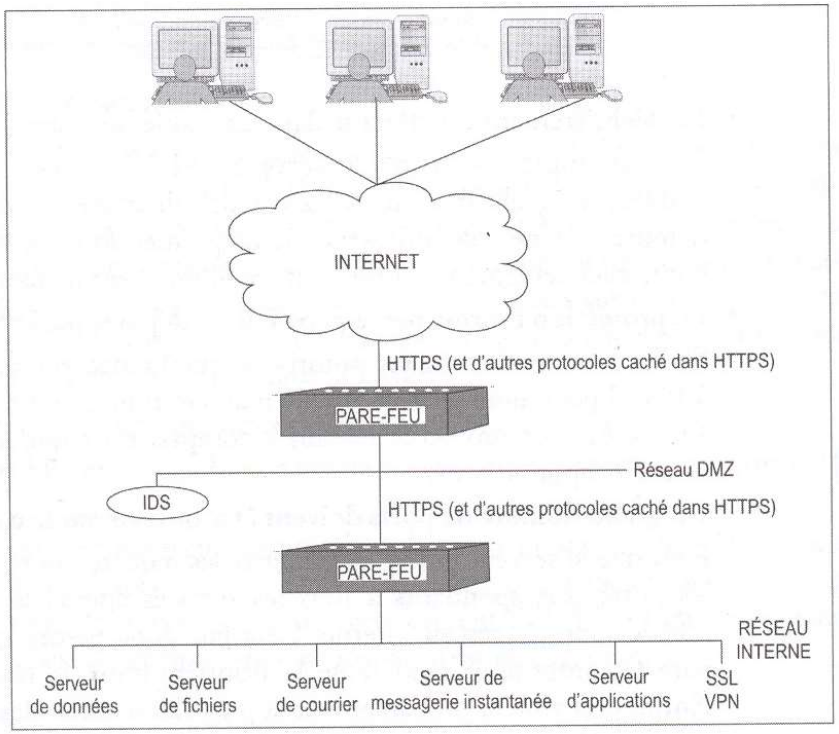
SSL VPN server security

- Firewall
  - Open communications for TCP/IP, and sometimes UDP and ICMP
- SSL VPN server located in the DMZ
  - Firewall must transmit port TCP 443 towards outside (often also port 80)
  - The SSL encrypting keys are stored in a non-secure environment (DMZ)
  - Ciphering is carried out in a non-secure zone (in particular, the communication between SSL VPN server and the internal network are not encrypted)
  - Protection provided by the firewall is thwarted by SSL VPN (it is possible to make pass through the tunnel some protocols which would have been prohibited by the firewall)
  - A large number of ports must be open on the internal firewall…
  - A distant (remote) client can be used as a gateway towards another network



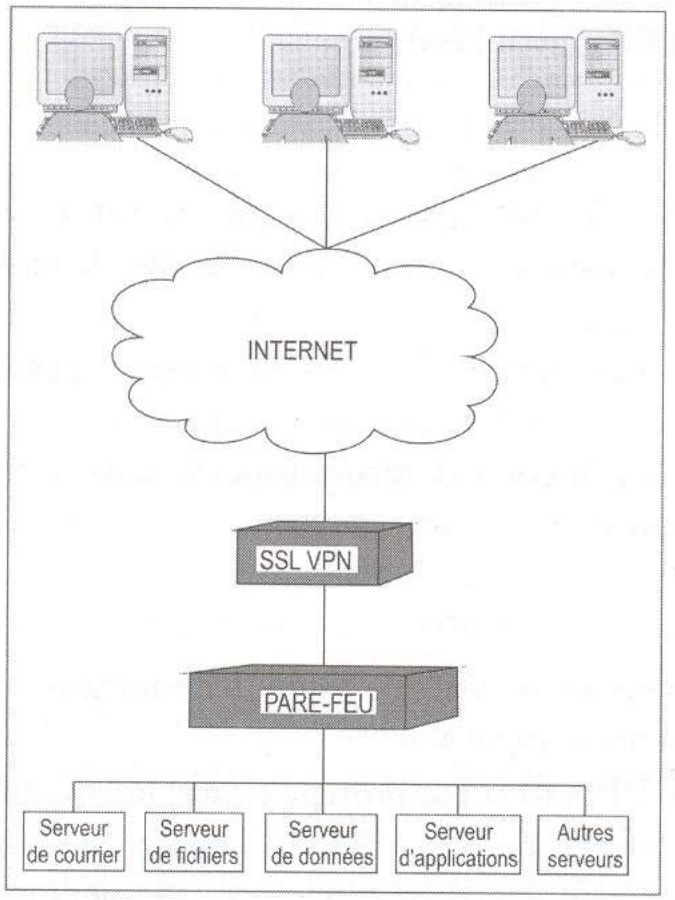
SSL VPN server security

- SSL VPN server located in the internal network
  - the firewall strategy is thwarted
  - Non identified users can send information into the internal network (ex: frames sent by users wishing to be identified)
  - The intrusion detection software (IDS) installed in the DMZ will be ineffective (because information passing through the tunnel is encrypted)



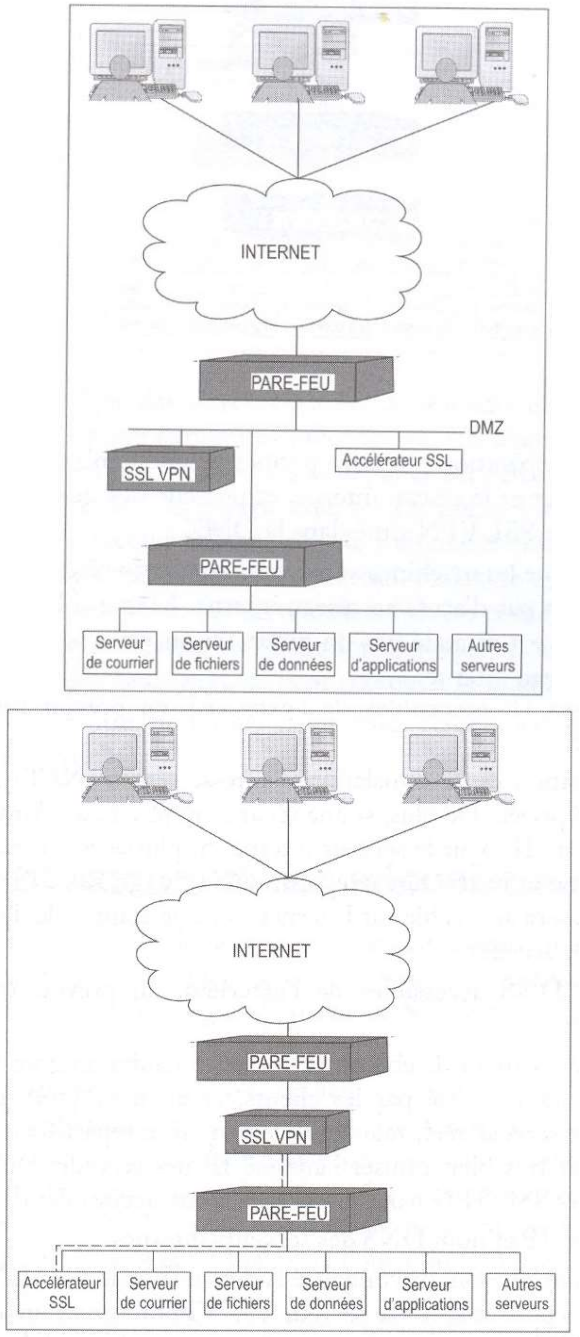
SSL VPN server security

- SSL VPN apart from the external firewall
- Advantages
  - Non - authorized protocols does enter **neither** in the internal network, **nor** in the DMZ
  - Non identified users does enter **neither** in the internal network, **nor** in the DMZ
  - IDS can detect the attacks, as well in the DMZ as in the internal network
- Disadvantages
  - SSL VPN server not protected from the attacks coming from the network
  - deciphering SSL keys are in a hostile environment
  - Need for opening many ports on the external and internal firewalls



SSL VPN server security

- Externalized SSL calculation
  - Discharge the main SSL VPN server by doing ciphering calculation to a dedicated external computer
- Caution: if one wants to install the calculation server in a network surer than the SSL VPN server itself, it is necessary to open ports on the intermediate firewalls, for ex:
  - discharge in the DMZ SSL calculation from a server located on Internet
  - discharge in the internal network SSL calculation from a server located in the DMZ
  - discharge in an internal DMZ SSL calculation from a server located on an external DMZ
- Advantages
  - Ciphering in a sure place
- Disadvantages
  - Opening of the port network

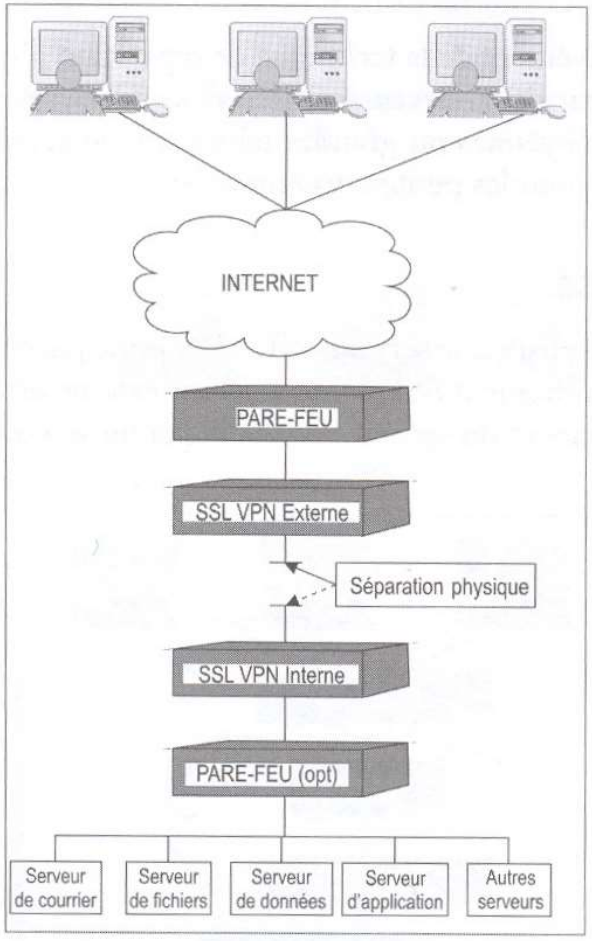


Solutions for the SSL VPN server security

- It does not exist a solution for everything
- Combine various security tools
- SSL VPN must make sure that it interacts well with the firewall and is integrated correctly in its infrastructure
- =>The possibility of network connection through a SSL VPN tunnel should be authorized only for computers which are authorized in the local area network (computers managed by the company)
- Be aware of the fact that even in this case, the firewall of the computer becomes indeed one of the firewall of the company => it is not necessarily dimensioned for that purpose…
- Prefer in general other distant (remote) accesses that the compkete access to the network (i.e. to avoid giving the possibility to a computer of going anywhere in the network while connecting itself by VPN), for example:
  - Route through the tunnel only necessary ports
  - Allow only a restricted access (whom? which application? which server? From which peripheral (a computer known with updated firewall and anti-virus…))

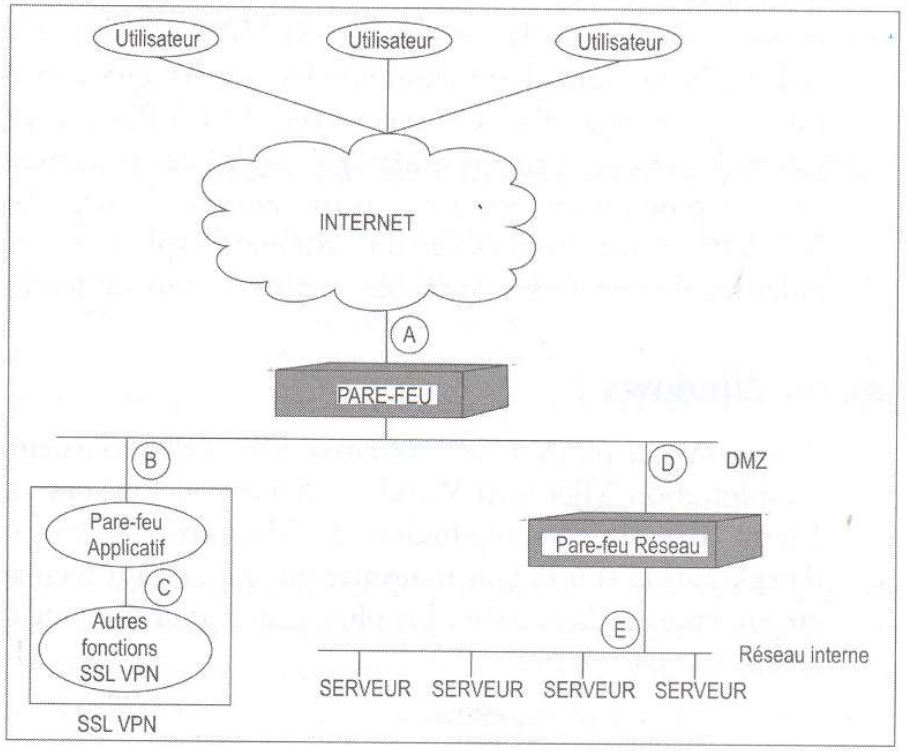
Solutions for the SSL VPN server security

- Problem of storage of SSL certificate
  - use an SSL accelerator => makes it possible to accelerate the processing times and to store the certificates in the protected environment of SSL accelerator
  - use a “physical separation”, called Air Gap Technology, which makes it possible to strore the certificate in the protected environment of the internal network. This technique consists in using two servers sharing a common memory (banks of memory allowing them to communicate)
    - a server is connected to Internet
    - a server is connected to the internal network and is running the whole SSL VPN functions
  - use both systems to protect even more effectively the certificates at the same time



Problem of the application faults

- Faults can be detected in the server application
- The operating system used by SSL VPN server can be vulnerable to security specific problems
- Protection to be considered
  - set up an application filtering to protect from the worms (on the right figure the data circulate according to ABCDE)
  - Filtering of the requests sent by a distant client to an internal server via SSL VPN



Other considerations on SSL VPN servers

- use an adequate ciphering strategy
- update the SSL VPN server software (bugs)
- Linux or Windows
  - No system is perfect
  - To be kept informed of security faults and failures and update the systems accordingly
- Consider the physical separation strategy
  - But expensive (two servers)
- Also do not to forget to make safe the SSL VPN server in the internal network
  - protect from any attack coming from the internal network
  - require a password for the access to the server administration functionalities
  - Configuration of the firewall between the internal network and SSL VPN server (to avoid the worms and spywares propagation)

Use of a SSL VPN server: determine the needs for the company

- Inter-sites communication (to give the illusion of a complete network)
  - Prefer IPSec
    - use technologies of virtual private networks between the sites, and inter-connect them
    - Equipment or dedicated software installed in the firewall in network edge
- Communication of a user towards an exploitation site
  - Distant access of the users to the resources of the internal network such as files, applications, databases, terminals services => SSL VPN is a suitable technology for this type of distant access

Use of a SSL VPN server: determine the user's needs

- E-mail distant access
  - Solutions of SSL VPN service dedicated to the e-mail
- Complete access to the network
  - prefer a solution containing IPSec + authentication of the client by digital certificate, with recognition of a specific computer => to be limited to some rare users
- Accesses for the customers and suppliers of the company
  - SSL VPN server which can deal with configurations with complexes rights of access management (accessible (reachable) applications are different according to the types of profiles and connected accounts)
- Distant access to a workstation for one or two users
  - prefer the use of a simple protected software for distant takeover such as PcAnywhere or a software from the VNC suite (UltraVNC, TightVNC, etc…) not very expensive and responding exactly to the the expected functionality

Models of SSL VPN servers

- http://www.aepnetworks.com
- www.arraynetworks.net
- fr.aventail.com
- www.checkpoint.com
- www.cisco.com
- citric.fr
- www.f5.com
- www.ipdiva.com
- juniper.net
- www.netsilica.com
- www.nokia.com
- nortel.com
- permeo.com
- portwise.com
- safenet-inc.com
- www.sonicwall.com/products/sslapp.html
- www.symantec.com/Products/enterprise?c=prodcat&refId=1006
- www.whalecommunications.com

Université Grenoble Alpes

7.3.2 RADIUS server

7.3.2 RADIUS server

- Remote Authentication Dial-In User Service: service of authentication for the users for on-the –request connections
- Allows to sub-contract the requests for session openings and the connections follow-up
- Service largely used by ISP (Internet Service Providers)
- RADIUS is not an official standard, but is maintained by a working group of the IETF

7.3.2 Introduction

- Protocol allowing to centralize the authentication and the authorization of distant users
  - Services and applications capable of taking into account RADIUS authentication are: routers, firewalls, wireless access points, etc…
  - Developed by Linvingstone Entreprise Inc
  - IETF (RFC 2865-2866 and 2869)
  - Client/server protocol functioning with UDP

7.3.2 Use of a RADIUS server (ex 1: Windows server)

- Use of Active Directory in order to authenticate the Internet accesses for the private networks users
  - The firewall which allows connection to Internet has rules forcing an authentication of the users in order to open or not the access to them
  - The firewall technology used deals with the RADIUS protocol

⇒ We can configure the firewall as a RADIUS client of a RADIUS server functioning under W. Server and member of the Active Directory domain to which the users belong

⇒ This offers an Internet accesses authentication for the users, without having to define a new accounts base for the firewall (and so having a complex management the use of the passwords)

7.3.2 Use of a RADIUS server (ex 2)

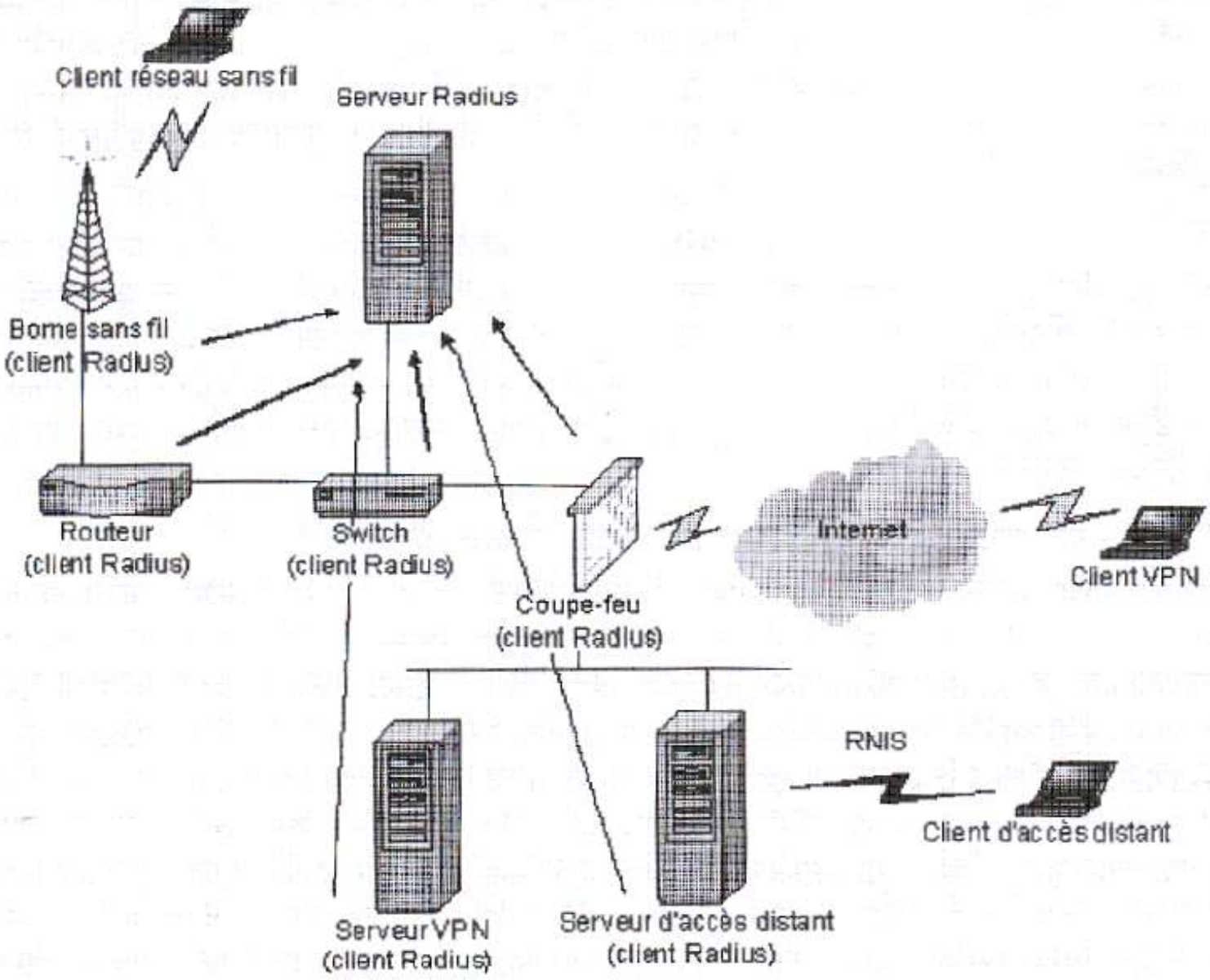
- The company owns several distant access and VPN servers
  - Creation of one or a set of strategies on the RADIUS server
  - Configuration of the distant accesses and VPN servers as RADIUS clients

Use of a RADIUS server (ex 3)

- One wishes to reinforce the access security at the borders of the wireless network. The RADIUS protocol can be used

7.3.2 Other interests to use a RADIUS server

- Centralization of the authentication
- Authentication of VPN clients in a domain which VPN server does not belong to
- Ex:
  - Installation in the DMZ of a VPN server in a working group
  - Configure in such a way that the authentication of VPN clients is done in their domains, by re-directing authentication requests towards a RADIUS server which is a member of this domain


Client réseau sans fil
Serveur Radius
Borne sans fil
(client Radius)
Routeur
(client Radius)
Switch
(client Radius)
Coupe-feu
(client Radius)
Internet
Client VPN
RNIS
Client d'accès distant
Serveur VPN
(client Radius)
Serveur d'accès distant
(client Radius)

7.3.2 Configuration of the RADIUS server

- Creation of distant access strategies
- clients authentication
- Definition of the Radius clients for whom the Radius server will operate
- Use of the MMC “authentication Internet Service” / *"Service d'authentification internet"*

7.3.2 Configuration of the RADIUS client

- Use of the “Routing and distant access” console / *"Routage et accès distant"*
- “Properties of the server” / *"Propriétés du serveur"*
- “Supplier for authentication” / *"Fournisseur d'authentification"*
- “RADIUS authentication ” / *"Authentification RADIUS"*
- “configure” / *"Configurer"*

References

- VPN, mise en œuvre sous Windows Server 2003, P. Mathon, 2004.
- La sécurité des réseaux-First steps, Tom Thomas, Cisco Press, 2005.
- SSH, le shell sécurisé, D. J. Barrett et R.E. Silverman, O'Reilly, 2001.
- SSL VPN, Understanding, evaluating and planning secure, web-based remote access – J. Steinberg & T. Speed, 2005.
- Les réseaux, édition 2005, G. Pujolle, Eyrolles 2004
- Présentation de Eric WIESS, 2005
- S. Ghernaouti-Helie – *Sécurité informatique et réseaux, 4ème édition* – Dunod, 2013
- E. Cole, R. Krutz, JW Conley - *Network security bible* – Wiley, 2005
- L. Bloch & al. – Sécurité informatique pour les DSI, RSSI et administrateurs, Eyrolles, 2016.