Université Grenoble Alpes

Cours de sécurité
M25-4. Les protocoles de sécurité

4.1 Généralités
4.2 IPSec
4.3 TLS/SSL
AUTRES ASPECTS
4.a IPv4 & IPv6, aspects sécurité
4.b L2TP
4.c SSH
4.d VPN
4.e RADIUS Server

4.1 Généralités

- Les algorithmes de cryptage peuvent être utilisés à différentes couches du modèle OSI
- Protocoles de sécurité
- La sécurité est native dans IPV6, elle doit être ajoutée dans IPV4
- Utilisé pour le VPN (Virtual Private Network)

Sur les différentes couches…

- Couche 3 : VPN de couche réseau: **IPSec**, MPLS (Multi-Protocol Label Switching, RFC 2547)
- Couche 4 : VPN de couche transport **: SSL/TLS**
  - Permet d'établir un tunnel entre deux stations
- Couche 7 : VPN de couche applicative : SSH

Voir aussi

- Couche 2 : VLAN (Virtual local networks) peut être considéré comme un VPN de couche liaison
  VPN : L2TP

Université Grenoble Alpes

4.2.3 Protocole IPSec

Solution de sécurité compatible avec IPv4 et IPv6

Présentation
AH
ESP
IKE
Stratégies IPSec

IPSec (IP Security)

- IPSec est un ensemble de protocoles standardisés par l'IETF (Internet Engineering Task Force) et permettant d'assurer une protection des données au niveau de la couche IP du modèle TCP/IP
- La protection apportée par IPSec se base sur les services cryptographiques et assure les fonctions suivantes :
  - *Anti-relecture* : un paquet IP protégé par IPSec et intercepté par une personne mal intentionnée ne pourra pas être réutilisé afin d'établir une nouvelle session
  - *Confidentialité* : chiffrage des données encapsulées dans un paquet IP afin de s'assurer qu'elles ne peuvent être lues lors de leur transfert
  - *Authentification* : une donnée reçue provient bien de l'hôte IP avec lequel la sécurité IP a été négociée
  - *Intégrité* : les données n'ont pas été modifiée lors de leur transfert

Transport du protocole IPSec

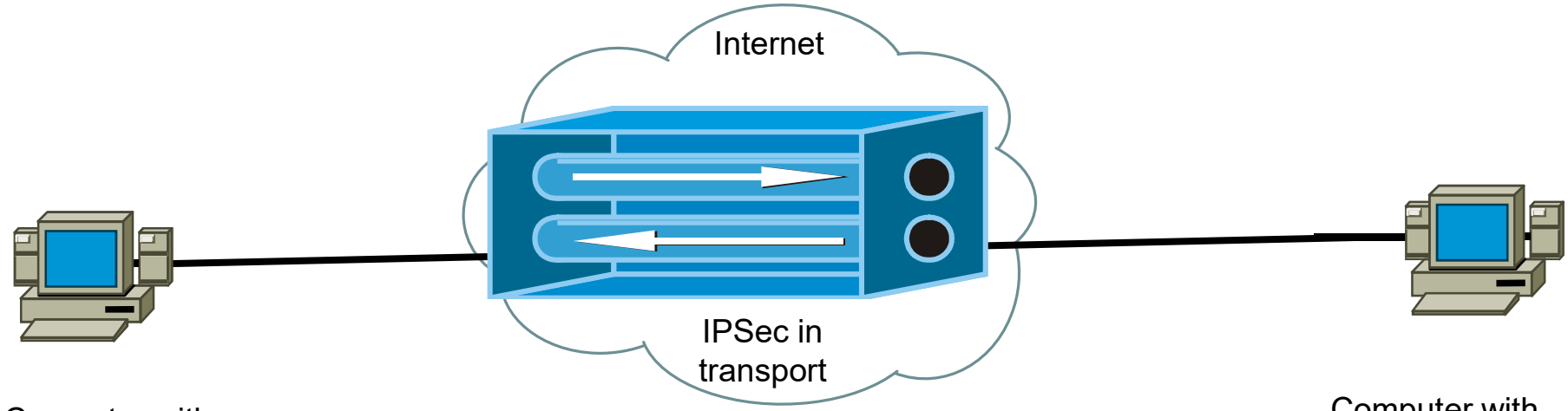
- Le protocole IPSec fonctionne de bout en bout => seules la source et la destination doivent les prendre en main
- Plusieurs équipements réseau tels que routeurs peuvent être traversés
- Attention aux équipements filtrants
  - Routeurs filtrants ou pare-feu

  => Certains ports seront à ouvrir
- Certaines implémentations IPSec acceptent de traverser les équipements faisant de la translation d'adresse (NAT)
- IPSec est un ensemble de trois protocoles principaux : AH, ESP et IKE

Mode transport de IPSec

- Le mode transport permet d'appliquer une sécurité par IPSec de bout en bout
- Source et destination sont les hôtes prenant en charge IPSec
  - Communication sécurisée de bout en bout
  - Blocage de certains types de trafic à destination de ports applicatifs ouverts sur la machine que l'on souhaite protéger
    - Ex : une machine sensible peut avoir une stratégie IPSec autorisant uniquement la machine en question à accéder à cet applicatif, et bloquant toutes les autres

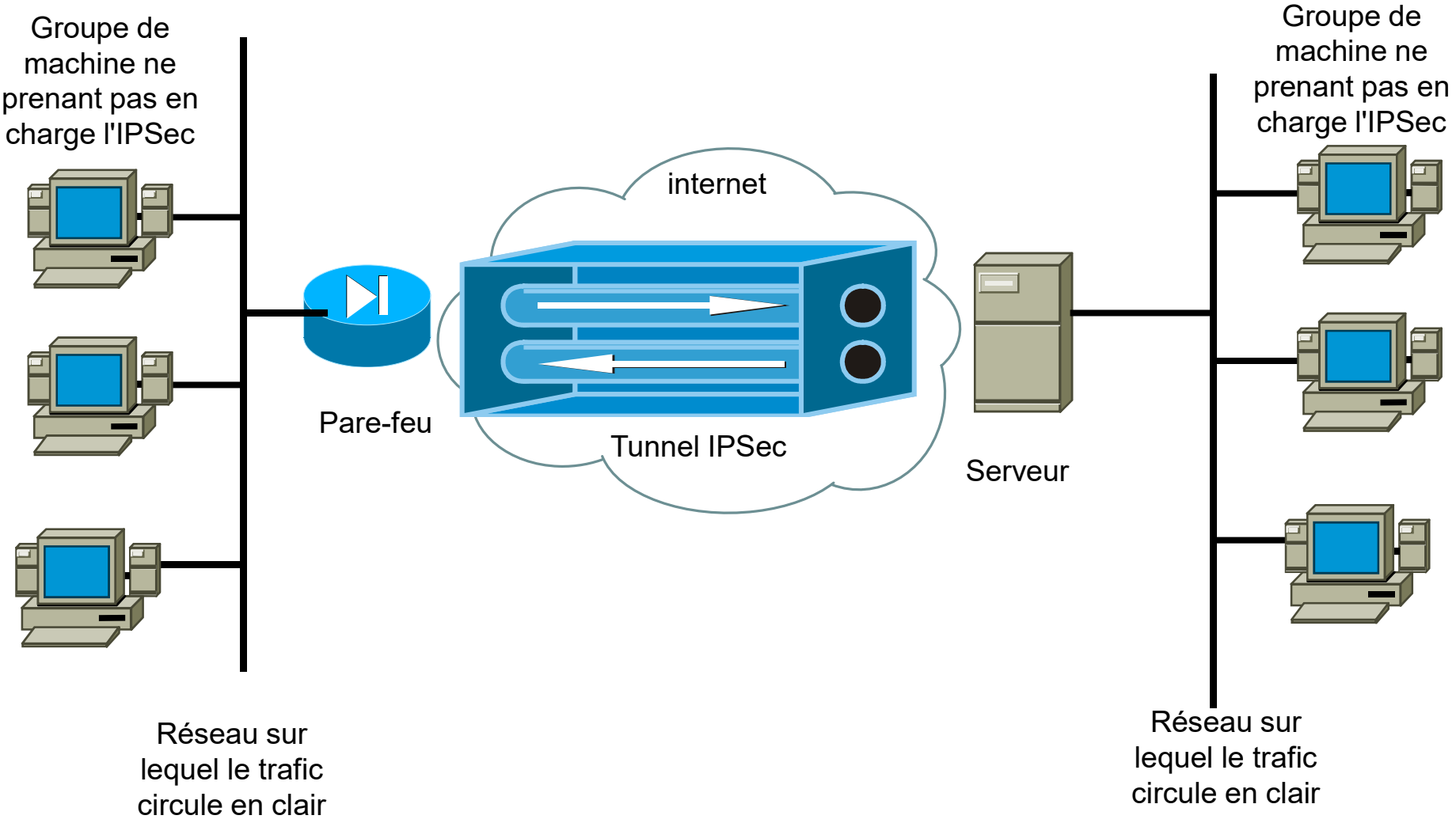
IPSec Transport mode, example



Mode tunnel de IPSec

- Etablissement de connexions sécurisées entre deux réseaux, lorsque les passerelles (pare-feu, routeur) ne prennent pas en charge une technologie VPN
- Ce ne sont pas les machines source et destinataires mais les passerelles entre les réseaux privés et le réseau public (internet) qui prennent en charge l'IPSec

Ex de Mode tunnel de IPSec



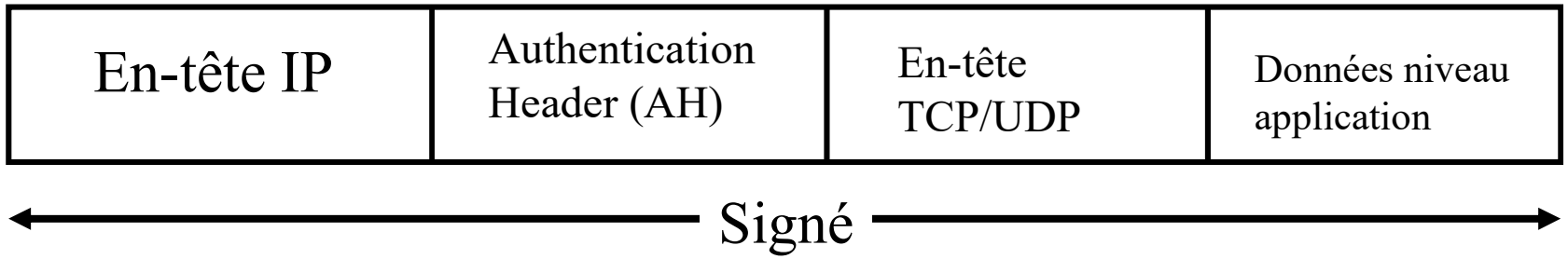
AH (Authentication Header) 1/3

- Assure l'authentification, le contrôle d'intégrité et l'anti-relecture des données encapsulées dans un paquet IP, ainsi que de l'en-tête IP elle-même
  ⇒Bloque donc les attaques utilisant les en-têtes IP (ex : IP-spoofing)
- Rem : le contrôle d'intégrité ne prend pas en compte les bits de l'en-tête IP autorisés à être modifiés lors de son transit (ex : le champ TTL (durée de vie) décrémenté lors de chaque passage dans un routeur)

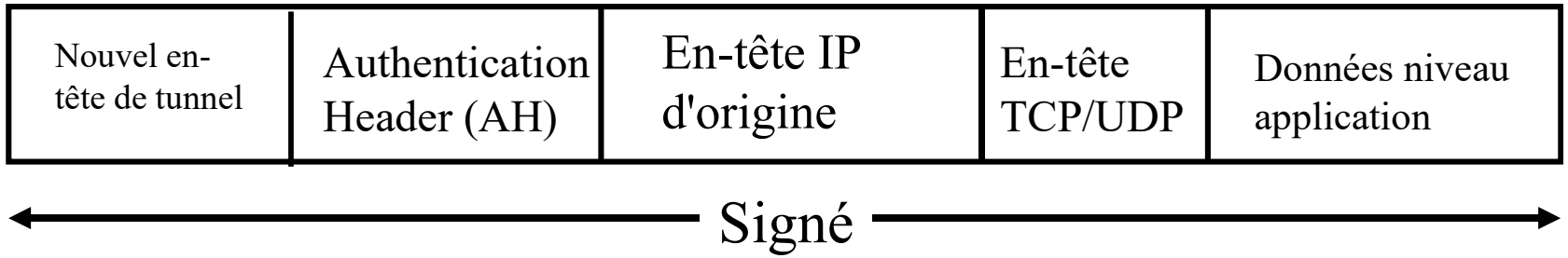
AH 2/3

paquet IPv4

paquet AH en mode transport



paquet AH en mode tunnel



AH 3/3

- AH utilise les algorithmes de hashage suivant
  - MD5 (Message Digest 5) : hash sur 128 bits
  - SHA1 (Secure Hash Algorithm): hash sur 160 bits

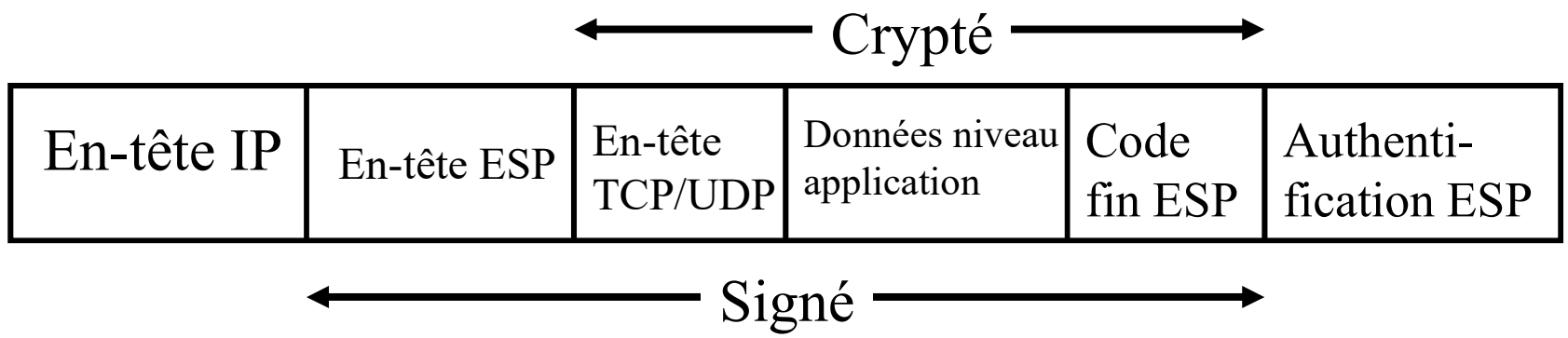
- AH est défini dans la RFC 2402

ESP
(Encapsulating Security Payload)

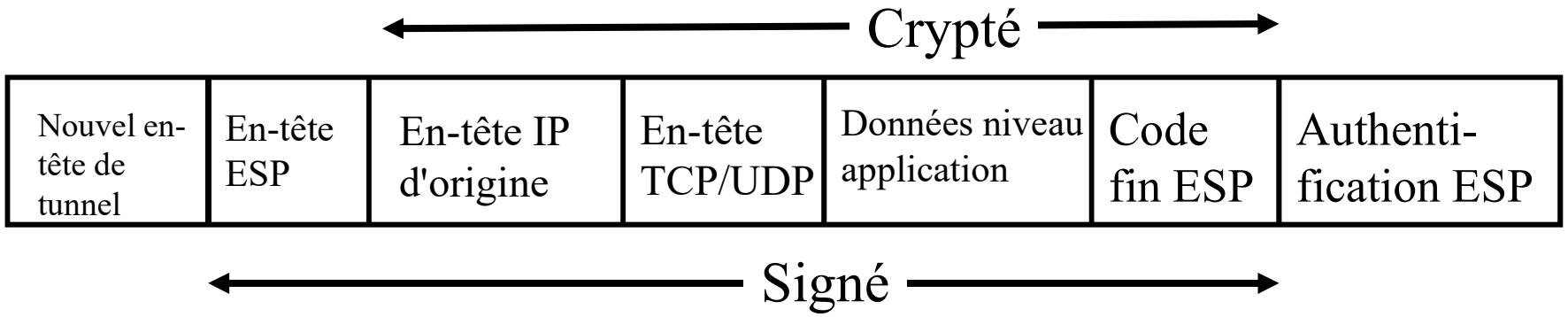
- Protocole assurant la confidentialité des données, en chiffrant le contenu du paquet IP
  - Rem : en-tête non crypté, pour pouvoir traverser les routeurs !
- ESP peut assurer un contrôle d'intégrité et une authentification, mais uniquement pour les données encapsulées dans le paquet IP
- Le protocole ESP ajoute un en-tête dans le paquet IP

ESP

- Format d'un paquet ESP en mode transport



- Format d'un paquet ESP en mode tunnel



ESP

- Utilise les algorithmes de hashage suivants
  - MD5
  - SHA1
- Utilise les algorithmes de chiffrement suivants
  - DES
  - 3DES
- ESP est défini dans la RFC 2406

IPSec

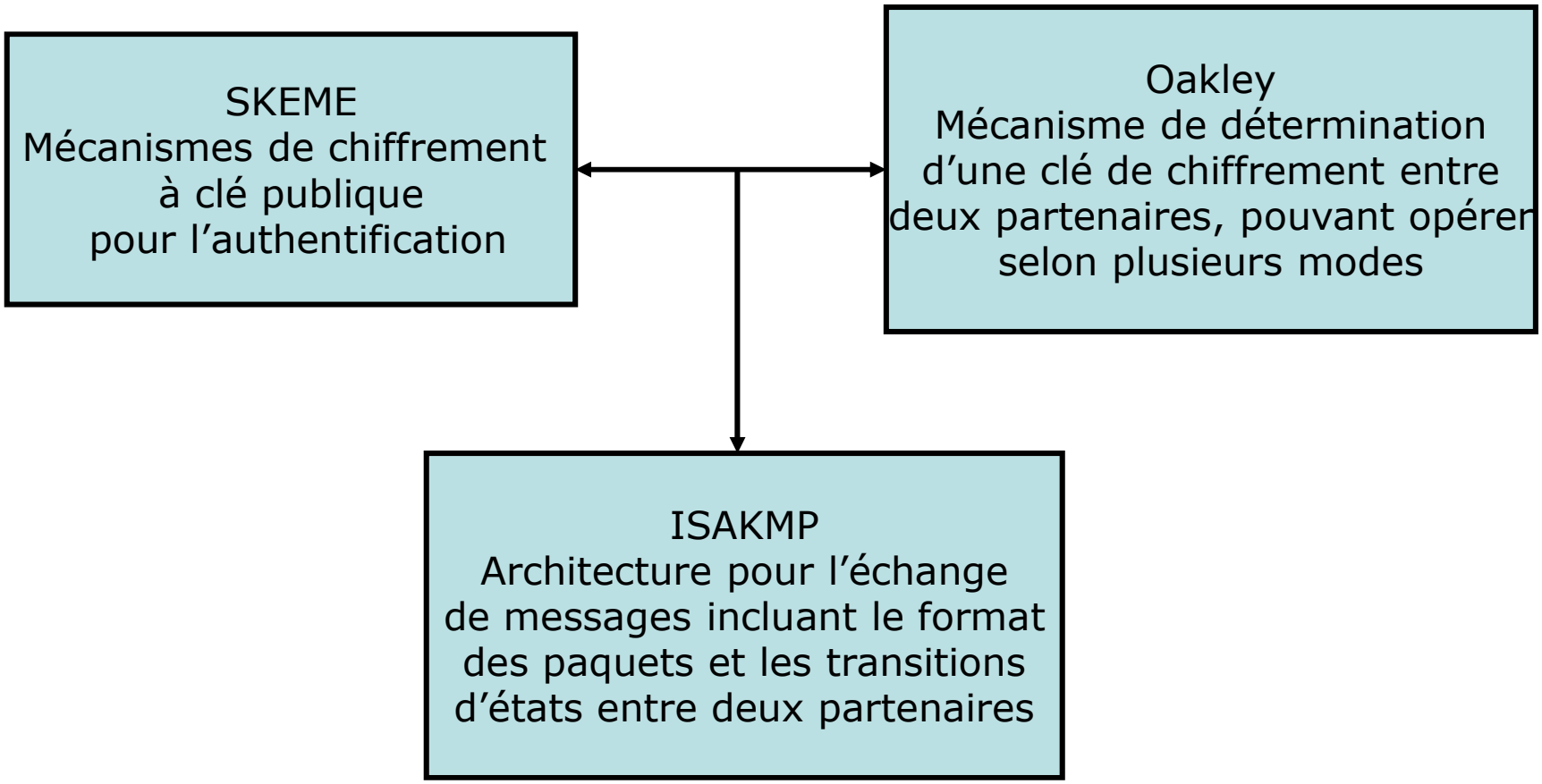
- Dans sa forme la plus complexe (la plus protégée mais aussi la plus consommatrice de ressources), un paquet IPSec peut utiliser à la fois AH et ESP
- AH est très consommateur de ressource CPU
- Il est donc généralement conseillé d'utiliser ESP seul, sauf si l'intégrité de l'en-tête IP est un élément important de la politique de sécurité
- Il existe des cartes matérielles (cartes d'accélération) pour IPSec

Gestion des clés de chiffrement

- Oakley et SKEME (Secure Key Exchange Mechanism) : décrit la façon d'échanger les clés et définit les services utilisés par chaque échange (basé sur l'algorithme d'échange de Diffie-Hellmann (RFC 2412)
- ISAKMP (Internet Security Association and Key Management Protocol) : cette RFC (RFC 2408) définit les procédures et les formats des paquets pour établir, négocier, modifier, terminer ou détruire une association de sécurité. Les formats sont indépendants des protocoles d'échange de clé, des algorithmes de chiffrement et des mécanismes d'authentification
- IKE (Internet Key Exchange) (RFC 2409) est une implémentation de ISAKMP. IKE permet de réaliser l'échange de clés (clés authentifiées) et de négocier les services de sécurité pour une association de sécurité

Protocoles intervenant dans le cadre de l'IKE

- IKE (RFC 2409) est un protocole hybride



Stratégie IPSec

- Ensemble de paramètres permettant de définir comment la sécurité IP doit être appliquée à un flux de données, et comment les clés de chiffrement sont générées
- Une ou plusieurs règles, définissant chacune des filtres, une méthode d'authentification et des actions de filtres

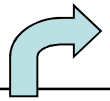
Stratégies IPSec par défaut

- Client (en réponse seule)
  - Permet de faire transiter le trafic normalement, une seule règle "règle de réponse par défaut", permettant de négocier le trafic IPSec si l'hôte distant le propose
- Serveur (demander la sécurité)
  - Règle 1 : négociation pour le trafic IPSec entrant comme sortant ; si la machine distante ne prend pas IPSec => communication non sécurisée
  - Règle 2 : transmission du trafic ICMP sans négociation de sécurité
  - Règle 3 : règle de réponse par défaut (voir ci-dessus)

Stratégies IPSec par défaut

- Serveur (nécessite la sécurité)
  - Règle 1 : négociation pour le trafic IPSec entrant comme sortant ; si la machine distante ne prend pas IPSec => communication interrompue
  - Règle 2 : transmission du trafic ICMP sans négociation de sécurité
  - Règle 3 : règle de réponse par défaut (voir ci-dessus)
- Règle de réponse par défaut
  - Permet de négocier la sécurité avec tout hôte désirant communiquer de façon sécurisée

Examen de l'interaction entre les règles

Sens du trafic 	**Aucune stratégie**	**Stratégie client (en réponse seule)**	**Stratégie serveur (demander la sécurité)**	**Stratégie serveur (nécessite la sécurité)**
Aucune stratégie	Non sécurisé	Non sécurisé	Non sécurisé	Echec
Stratégie client (en réponse seule)	Non sécurisé	Non sécurisé	Sécurisé	Sécurisé
Stratégie serveur (demander la sécurité)	Non sécurisé	Sécurisé	Sécurisé	Sécurisé
Stratégie serveur (nécessite la sécurité)	Echec	Sécurisé	Sécurisé	Sécurisé

Conclusion : IPSec

- Authentification de l'origine des données par paquet
  - Le récepteur peut identifier la source des paquets. Ce service est dépendant du service d'intégrité des données
- Intégrité des données
  - Possibilité de vérifier que les paquets envoyés par l'émetteur n'ont pas été altérés durant la transmission
- Protection contre le rejeu (protection contre la capture et la reproduction d'un flot de paquets)
  - Le récepteur peut détecter et rejeter les paquets reproduits
- Confidentialité des données (protection contre la lecture possible de données sans la clé de chiffrement lors d'une interception)
  - Les paquets sont chiffrés avant d'être expédiés sur le réseau. Même s'ils sont capturés durant leur transport, ils ne seront d'aucune utilité à l'intercepteur s'il ne peut les lire
- Inconvénient : nécessite d'installer un logiciel spécialisé à chaque extrémité de la transmission

Université Grenoble Alpes

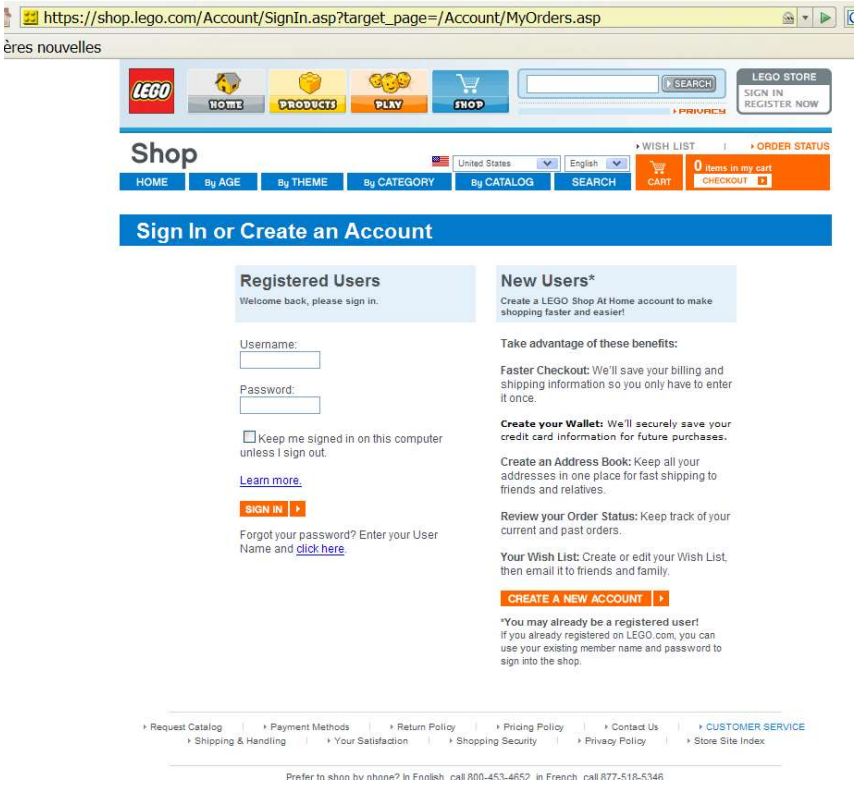
4.3 SSL/TLS

SSL (Secure Socket Layer)

- Chiffrage des données au sein du protocole réseau
- Garantit
  - Identité des deux parties
  - Confidentialité des données de bout en bout
  - => chiffrage des données donc impossibilité de lire les noms d'utilisateur et mots de passe
  - Intégrité des données par l'utilisation de sommes de contrôle (hash)
- Se base généralement sur TCP/IP
  - Permettant de garantir la bonne arrivée et l'ordre des données
- Navigateurs web équipés de SSL
  - Firefox, Konqueror, Internet Explorer, Safari…

SSL protocol

- SSL est apparu en 1994 dans Mosaic
- Pages web utilisant SSL : HTTPS
- 1996 : travail de formalisation et de standardisation de SSL par l'IETF



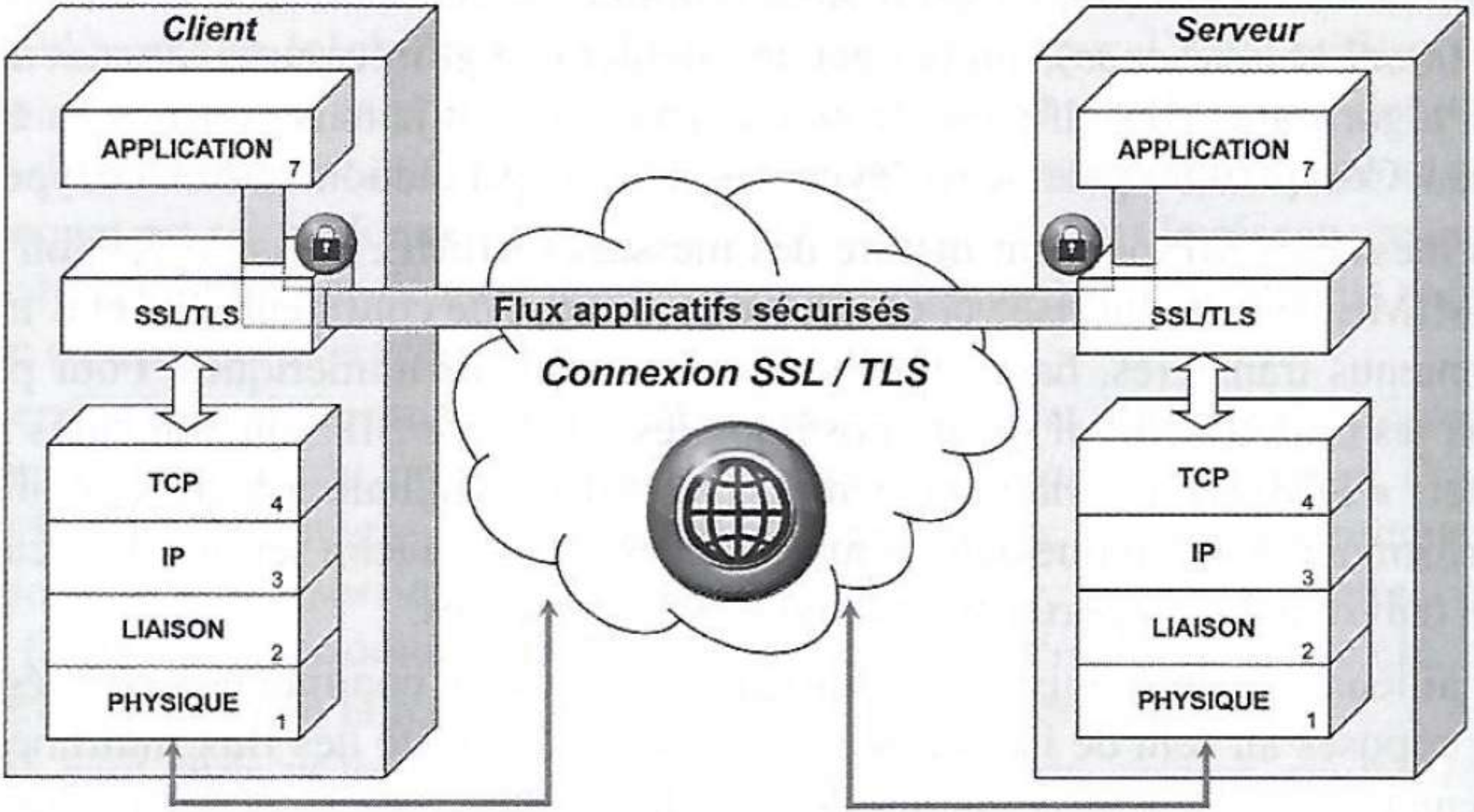


Figure 9.1 – La sécurité des flux applicatifs par SSL.

SSL : propriétés

- Authentification
  - Preuve de l'identité du client par échange de certificats
- Confidentialité
  - Données chiffrées par l'utilisation d'une clé partagée et via la négociation des algorithmes de chiffrement
- Les phases d'authentification et de confidentialité ont lieu pendant l'étape de « négociation », appelée aussi « initialisation » de la session
- Intégrité
  - vérifie que les données n'ont pas été modifiées

TLS/SSL : facilité d'utilisation

- Conçu pour être transparent pour l'utilisateur final
  - Il suffit pour l'utilisateur de se connecter à l'adresse désirée (ex : https://...)
- RFC 1738 précise le format
  - Serveur web port 80 mais en SSL port 443

Mise en œuvre de SSL

- Un serveur central
- Client utilisant un logiciel de communication sachant parler SSL
  - Navigateur
    - savent parler HTTPS
    - contiennent nativement des certificats SSL racines issus d'autorités de certification reconnues
- Possibilités également de faire télécharger des logiciels additionnels au client
  - Plug-ins
  - Applets
- SSL peut également être déployé sur des solutions matérielles spécifiques

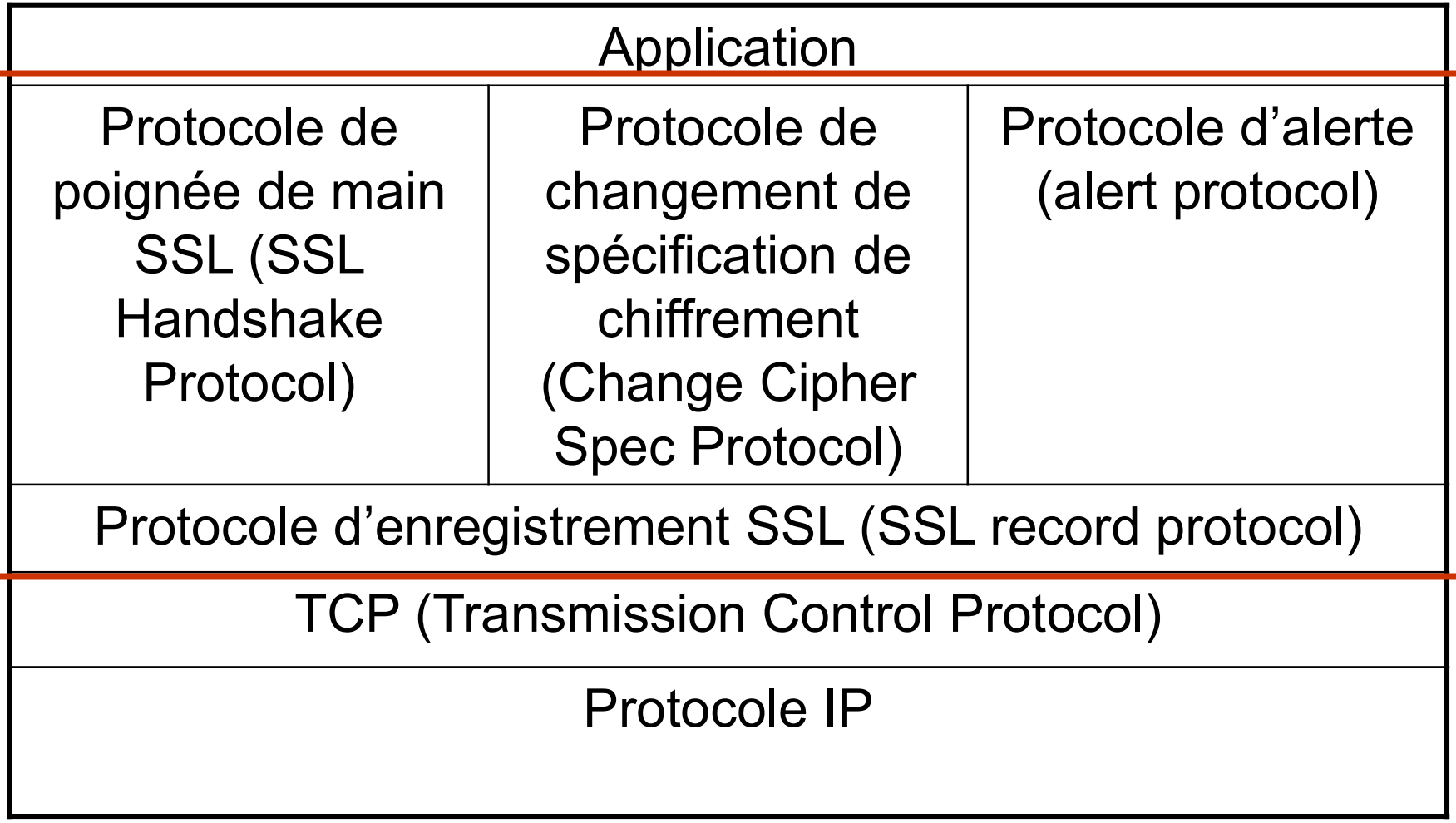
SSL: cryptographie

- Cryptographie symétrique pour la protection des données
  - Clé commune (clé de session)
- Cryptographie asymétrique pour l'échange de la clé de session

SSLv3

- Version plus évoluée de SSL
  - Générateur de clés
  - Fonctions de hashage
  - Algorithmes de chiffrement
  - Gestion des certificats
- Propriétés
  - Protocole de changement de spécification : modification possible de l'algorithme de chiffrement en cours de communication pour garantir la confidentialité
  - Protocole d'alerte permettant d'envoyer des alertes, accompagnées de leur importance (ex : certificat inconnu, révoqué, expiré). Les alertes de haut niveau entraînent l'arrêt de la communication
  - Protocole Handshake
    - authentification du serveur depuis le client
    - négociation de la version du protocole
    - sélection des algorithmes de chiffrement
    - utilisation de techniques de chiffrement à clé publique pour générer et distribuer des clés secrètes
    - établissement de connexions SSL chiffrées
  - Protocole d'enregistrement SRP (SSL Record Layer) : encapsulation des protocoles situés juste au-dessus, comme le protocole Handshake

Architecture du protocole SSLv3



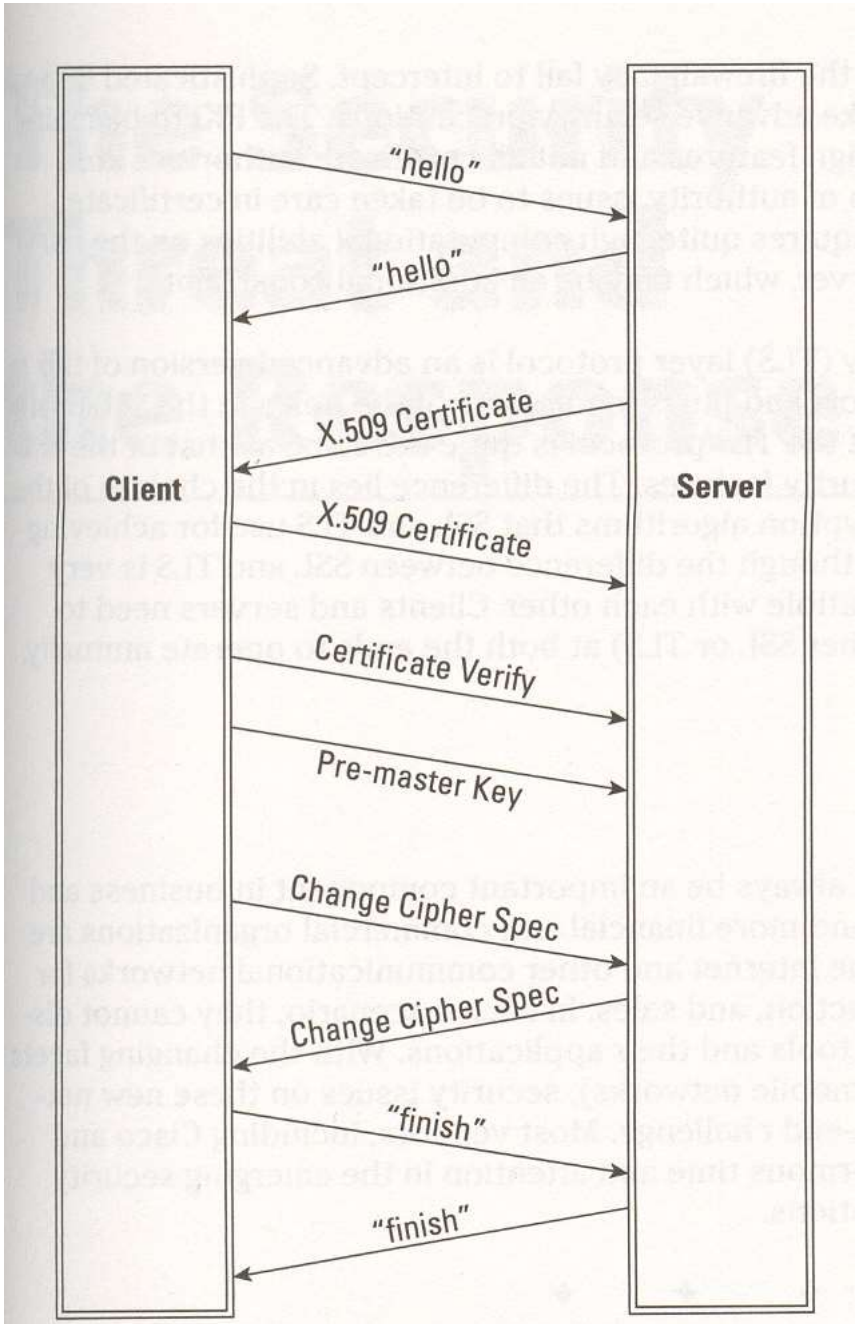


Figure 16-13: The SSL handshake protocol

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

- SSL v2 ou v3 mis à l'index depuis 2014 à cause de nombreuses failles de sécurité qui ont montré ses faiblesses.
- TLS: nouvelle version, algorithme différent, mêmes fonctionnalités (TLS ~ SSLv3)
- Nouvelle version TLS 1.3 (juin 2018) : abandon d'algorithmes de chiffrage obsolètes (MD5, SHA-224) pour passer à Chacha20, Poly1305, Ed25519, x448 et X25519.
- ATTENTION aux configurations de serveurs permettant des rétro-compatibilités avec des versions obsolètes de logiciels cryptographiques (mais TLS 1.3 interdit le "downgrading")
- TLS 1.3 est aussi plus rapide de que les versions antérieures
- Chiffrage des données au sein du protocole réseau
- Garantit
  - Identité des deux parties
  - Confidentialité des données de bout en bout
  - => chiffrage des données donc impossibilité de lire les noms d'utilisateur et mots de passe
  - Intégrité des données par l'utilisation de sommes de contrôle (hash)
- Se base généralement sur TCP/IP
  - Permettant de garantir la bonne arrivée et l'ordre des données
- Navigateurs web équipés
  - Firefox, Konqueror, Internet Explorer, Safari, Chrome…

TLS/SSL

- Applications
  - Commerce électronique
  - Sécurisation des communications sous HTTPS
  - FTPs
  - Copies sécurisées
  - (connexion sécurisée à un système SSH)
  - …

Implémentations de SSL/TLS

- OpenSSL la plus répandue
- SChannel sur Microsoft
- Secure Transport sur Apple
- NSS sur Mozilla et Chrome
- Cryptlib dans le secteur bancaire
- GnuTLS pour les projets Open Source
- JSSE est une extension du langage permettant aux applications Java de bénéficier des services SSL/TLS
- MatrixSSL permet de fournir des services SSL/TLS à des environnements embarqués
- mbedSSL (a remplacé PolarSSL), racheté par ARM, pour environnements embarqués

Références Bibliographiques

- 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, accès web et extranets sécurisés – J. Steinberg & T. Speed, Eyrolles, 2006.
- 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

D’AUTRES ASPECTS

Université Grenoble Alpes

4.a IPv4 & IPv6, aspects sécurité

4.a IPv4

- Protocole : ensemble de règles déterminant le format des messages échangés
- IPv4 (version 4 du protocole internet, actuellement utilisée) n'intègre aucun service de sécurité
  - Ne permet pas l'authentification ni de la source ni de la destination d'un paquet
  - Ne permet pas la confidentialité des données transportées
  - Ne permet pas la confidentialité des adresses IP impliquées
- IPv4 est un protocole en mode sans connexion, il ne garantit pas
  - La remise de données (perte possible de données)
  - La livraison de données au bon destinataire
  - L'ordonnancement (séquencement) correct des données

4.a IPv4

- Pas de qualité de service (pas de reprise sur erreur)
- => implémentation du protocole TCP (Transmission Control Protocol) en couche 4, TCP offre un service de transport fiable en mode connecté, mais n'offre pas de services de sécurité à proprement parler

4.a IPv6

- Besoins pris en compte dans *IPnG* (Internet Protocol next Generation) ou *IPv6*:
  - Manipuler une plage d'adresse plus importante
  - Pouvoir faire une allocation dynamique de bande passante pour pouvoir supporter les applications multimedia
  - Intégrer des aspects sécurité

4.a Principales caractéristiques d'IPv6 (RFC 2460)

- *(Rappel : RFC = Request For Comment)*
- Support d'adressage étendu et hiérarchisé
- Adresses codées sur 16 octets (128 bits) au lieu de 4
- Représentation sous forme de nombres hexadécimaux séparés par des deux points tous les deux octets:
  - Exemple : **0123::4567::89ab::cdef::0123:: 4567::89ab::cdef**
- Allocation dynamique de bande passante pour le support d'applications multimedia
- Créations de réseaux IP virtuels
- Support de procédures d'authentification et de chiffrement
- En-têtes de paquets simplifiés afin de faciliter et accélérer le routage

4.a Difficultés d'utilisation de IPv6

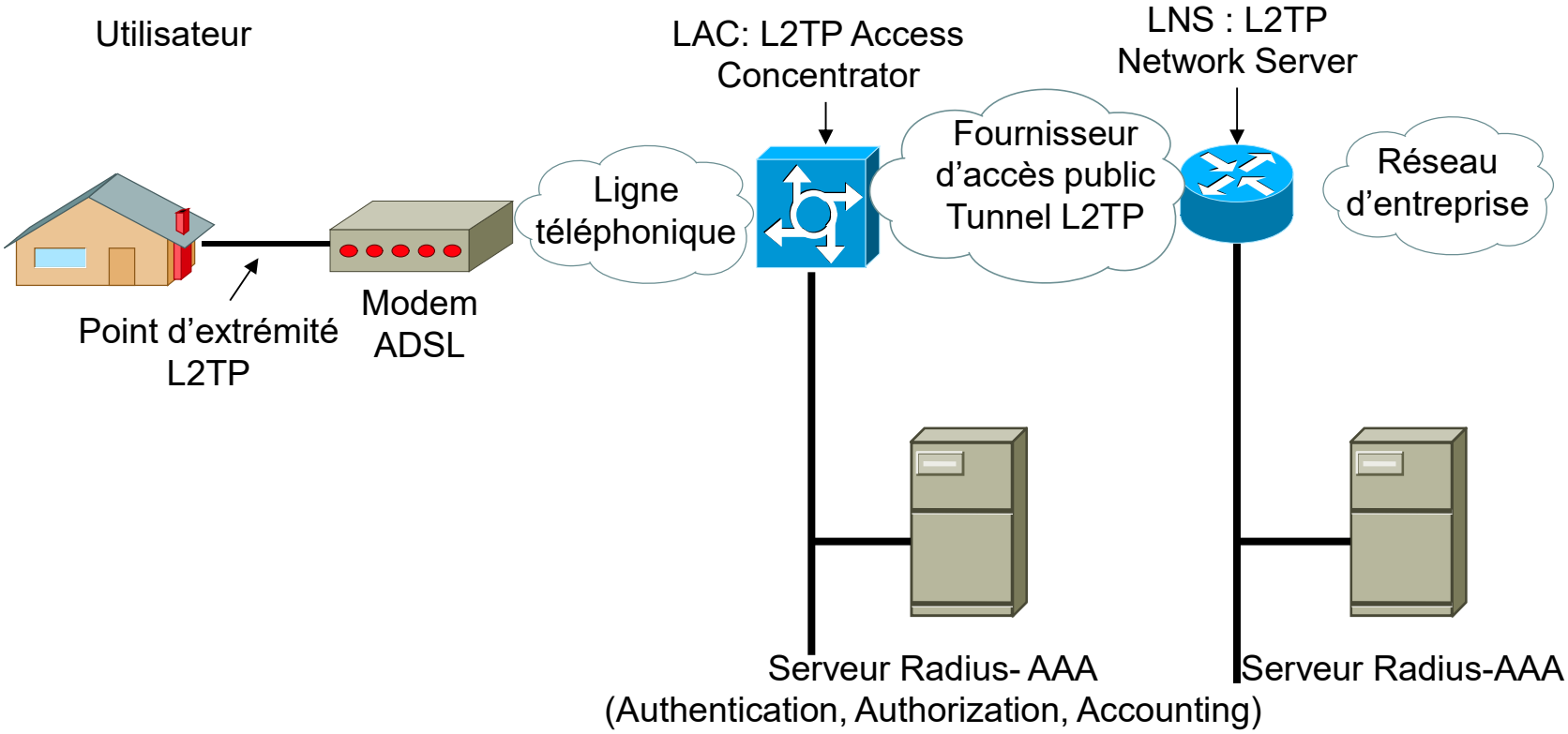
- Problème d'ordre économique et technologique lié à son déploiement
- Modification du schéma d'adressage et de la gestion des adresses
- Mise en place de systèmes supportant les versions 4 et 6, synchronisation de la migration des versions

4.b L2TP (Layer 2 Tunneling Protocol)

- Combinaison de deux protocoles
  - PPTP (Point-to-Point Tunneling Protocol) de Microsoft
  - L2F (Layer-2 Forwarding) de Cisco
- Couche 2, basé sur le protocole PPP
- RFC (Request for Comments) 2661
- Ou RFC 3193 (emploi sécurisé au moyen de la suite de protocoles IPSec)
- Paquets L2TP échangés par l'intermédiaire du port UDP (User Datagram Protocol) 1701
- Peut envoyer des données à travers divers réseaux (IP, Frame relay (relais de trames), MPLS (MultiProtocol Label Swiching), ATM (Asynchronous Transfer Mode)

4.b Architecture de réseau L2TP (1/2)

Un serveur (LNS : L2TP Network Server) et des clients (LAC : L2TP Access Concentrator)



AAA: http://www.ietf.org/html.charters/aaa-charter.html

RADIUS (Remote Authentication Dial-in User Service => IETF)

4.b Architecture de réseau L2TP (2/2)

- L2TP utilise internet et ses connexions de réseau pour permettre à ses points terminaux d'être situés dans des lieux géographiquement différents
- Figure précédente :
  1. Le PC de l'utilisateur établit une connexion PPP avec le POP (Point of Presence) du fournisseur. Le LAC (L2TP Access Concentrator) accepte la connexion.
  2. Le LAC authentifie l'utilisateur au moyen d'un serveur AAA puis transmet la session PPP chiffrée vers le LNS
  3. Le LAC vérifie ensuite le nom utilisateur, le nom de domaine ou le DNIS (***d**ialed **n**umber **i**dentification **s**ervice)* utilisés pour vérifier que l'utilisateur est un client VPN
  4. Si l'utilisateur n'est pas client VPN => connexion comme utilisateur ordinaire. Si l'utilisateur est client VPN, sa connexion nomme un LNS comme point terminal du VPN. Les informations sont alors envoyées au serveur AAA connecté au LNS à des fins d'authentification
  5. Les points terminaux du VPN (LAC et LNS) s'authentifient mutuellement avant toute transmission de données de l'utilisateur sur le tunnel
  6. Après que le tunnel VPN (utilisant L2TP) a été créé, une session entre l'utilisateur et le réseau d'entreprise est initiée

4.b Etape de la création d'un tunnel L2TP

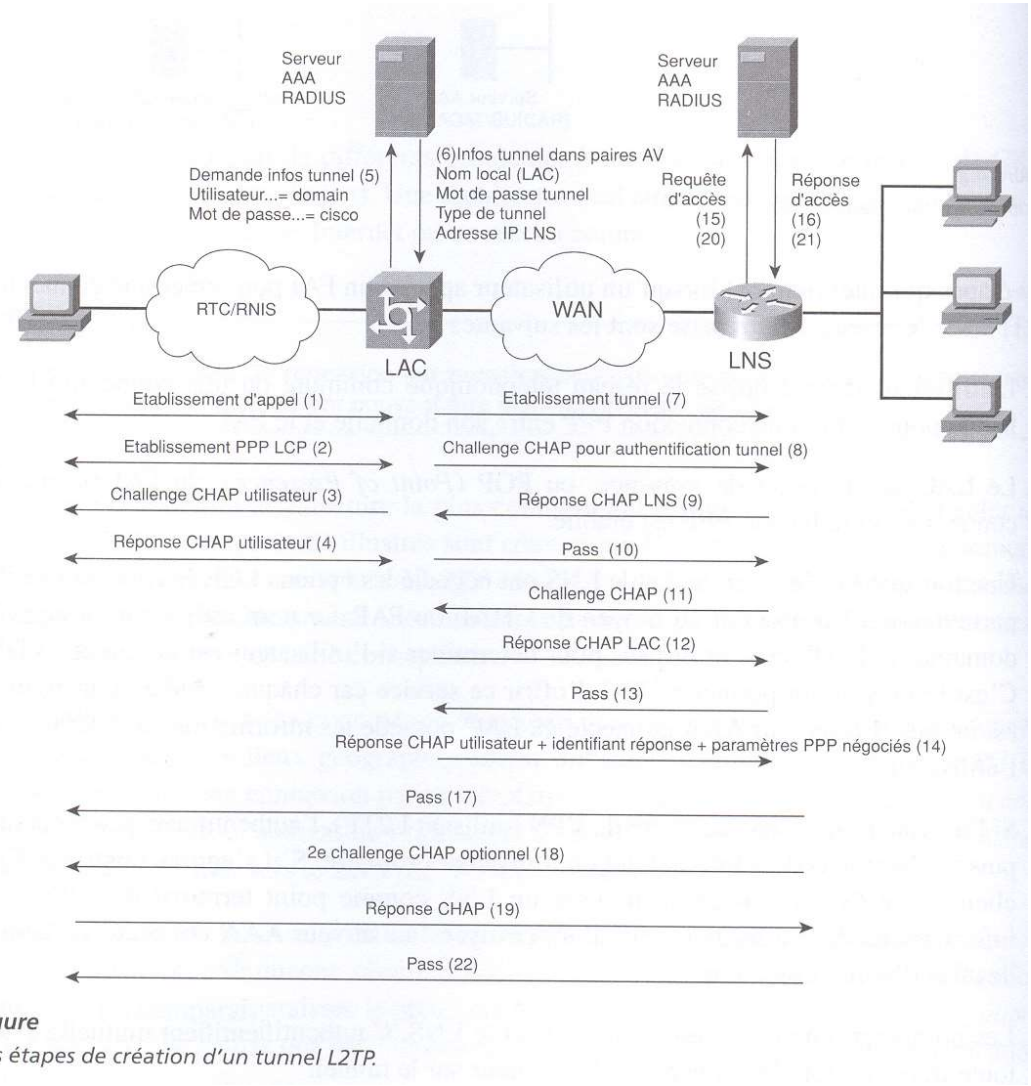


Figure
Les étapes de création d'un tunnel L2TP.

4.c SSH (Secure Shell)

- Connexion directe à un système (comme telnet)
- Fonctions de sécurité avancées + communication chiffrée à travers un réseau non sécurisé (internet)
- 1995: SSH1 (pour remplacer les commandes « r » d'Unix : rlogin, rsh, rcp)
- Standard défini en 2006 : SSH2 avec des fonctionnalités et sécurité supérieures à SSH1
- Utilisation la plus fréquente : création d'un shell de commandes sécurisé (session à distance)
- Disponible sur toutes les plate-formes (MacIntosh, Windows, Unix, Linux…)

4.c Utilisations de SSH

- Ouverture d'un shell de commande
- Transfert (copie) sécurisé de fichiers
- Transmission du trafic d'un port

- Session distante
- Tunnel générique
  - copie de fichiers
  - transmission sécurisée d'e-mails
  - exécution à distance de programmes

4.c Méthodes de chiffrement de SSH

Méthode de chiffrement	SSH1	SSH2
DES	Oui	Non
3DES	Oui	Oui
IDEA	Oui	Non
BLOWFISH	Oui	Oui
TWOFISH	Non	Oui
ARCFOUR	Non	Oui
CAST-128-CBC	Non	Oui
RSA	Oui	Non
DSA	Non	Oui

4.c Tunelling et transmission du trafic d'un port

- SSH fournit une fonction de sécurité intéressante :
  - Acheminement d'un certain trafic identifié par un numéro de port par l'intermédiaire d'un tunnel SSH : protocoles FTP ou X Window par exemple => possibilité d'exécuter certaines opérations particulières sur l'hôte distant via le tunnel SSH
  - Ex 1 : Transfert de fichiers à travers internet vers un serveur web
  - Ex 2 : disposer d'un accès de type bureau à l'hôte distant (via X Window)

4.c Limitations de SSH

- SSH1 comportait une série de bogues et de problèmes
  - SSH2 (à préférer) les corrige
- SSH ne permet pas de protéger les équipements du réseau (PC, serveurs…)
- SSH n'est pas un protocole de VPN

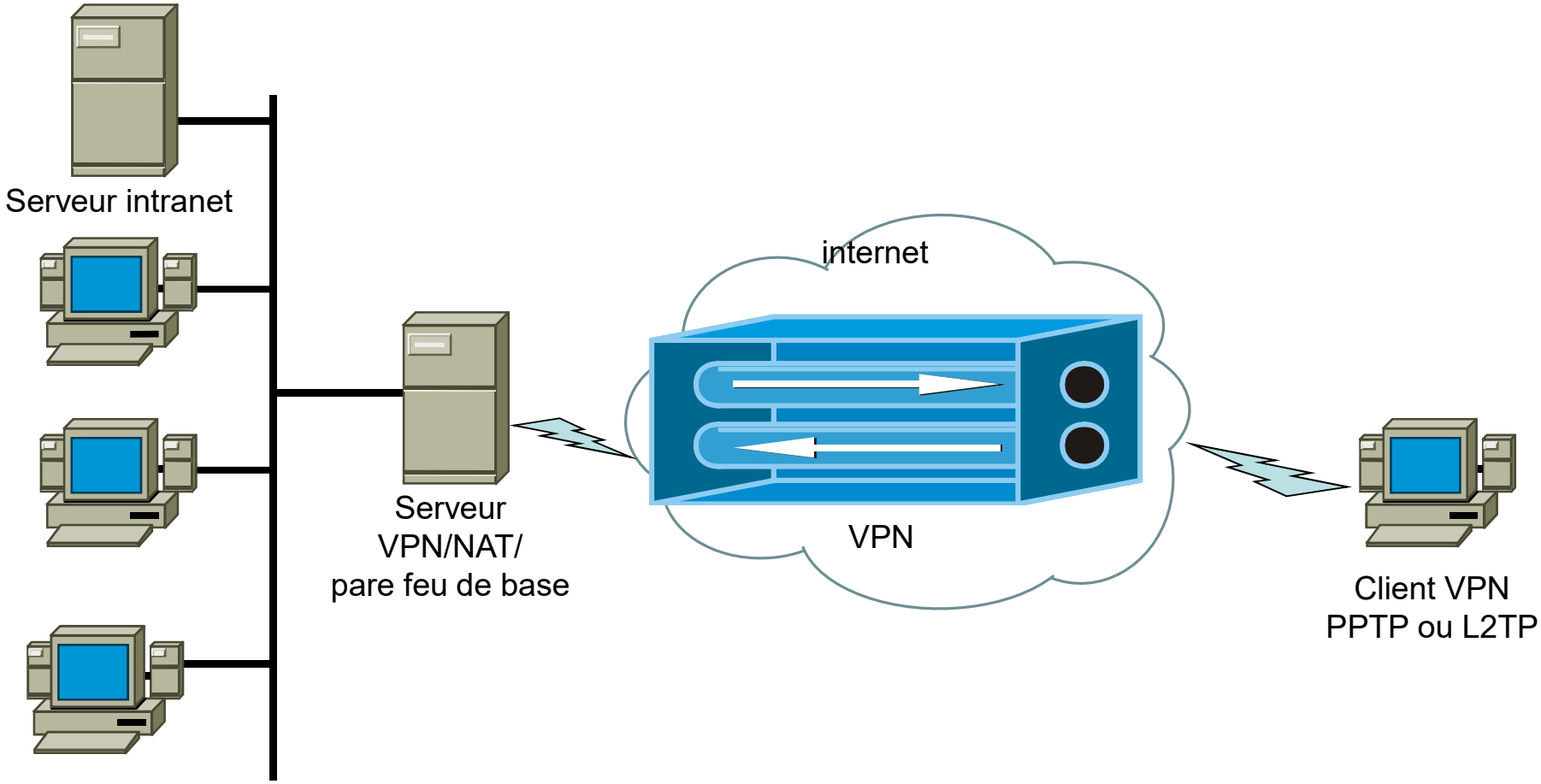
4.d Quelques considérations sur les VPN

- VPN et accès distant
  - Permettre à des utilisateurs situés physiquement hors du réseau de l'entreprise de pouvoir se connecter au réseau d'entreprise
- Les VPN forment une classe particulière de réseaux partagés
  - Ressources d'un réseau réel partagé entre plusieurs sous réseaux
- Information de gestion à prendre en compte
  - Topologie : détermination des points d'accès vers les sites qui doivent être interconnectés par le VPN
  - Adressage : localisation des points d'accès et des sites qui doivent être interconnectés par le VPN
  - Routage : possibilité d'atteindre les sites du VPN
  - Informations de sécurité : établissement et activation des filtres laissant ou non passer les paquets
  - Informations de qualité de service : paramètres pour le contrôle des ressources nécessaires à la qualité de service

4.d Introduction sur les VPN

- VPN de niveau 2 (trame) : ex : VPN constitué de réseaux Ethernet
- VPN de niveau 3 (paquet) : ex : VPN constitué de réseaux IP => les plus répandus au niveau « entreprise » car intégrant toutes les fonctionnalités IP
- VPN de niveau 7 (application) : ex : VPN mis en place pour une application comme HTTP, POP, IMAP, SMTP, FTP…
- VPN = extension du ***réseau privé*** de l'entreprise, ***virtuellement*** par le biais du réseau public
- ! La notion de sécurité est absente de la définition de base du VPN ! => doit être étudiée en particulier (ex : utilisation de L2TP/IPSec)

4.d Serveur VPN en périphérie de réseau (1/2)

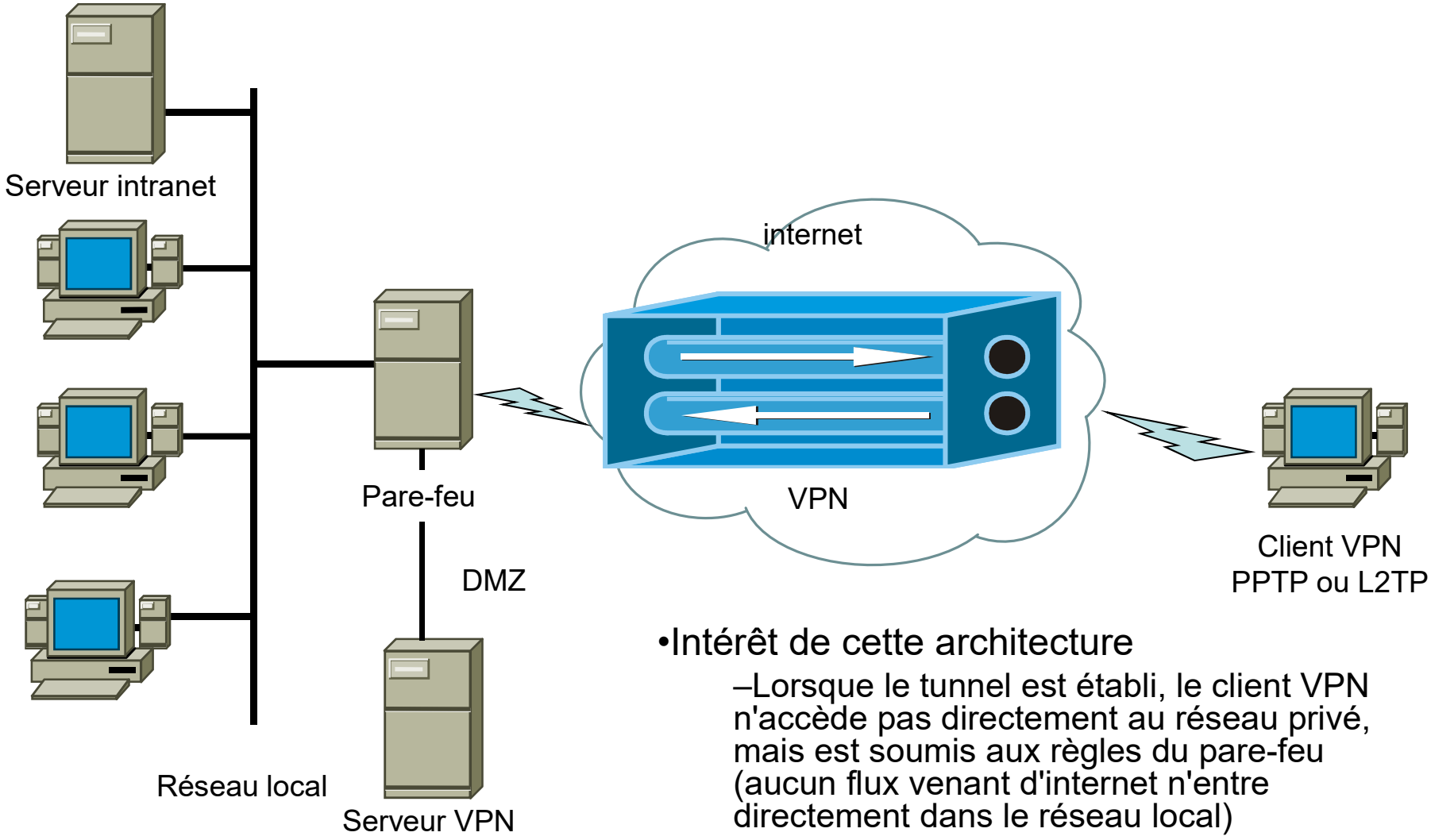


4.d Serveur VPN en périphérie de réseau (2/2)

Pré-requis nécessaires à l'installation d'un serveur VPN

- Le serveur VPN doit être connecté à internet (généralement par l'intermédiaire du fournisseur d'accès internet)
- Le serveur VPN devra posséder une adresse IP publique fixe ou un nom DNS correspondant
- Le serveur VPN doit respecter les règles de base en terme de sécurité
  - Désactiver tous les services inutiles sur le serveur
  - Activer un pare-feu sur le serveur
  - Utiliser des stratégies de mots de passe complexes, ou une authentification "forte" (carte à puces, reconnaissance biométrique)
- Vérifier que le fournisseur d'accès internet n'applique pas de filtre sur son routeur qui vous connecte à internet, et que l'offre d'accès internet souscrite permet de faire entrer les flux

4.d Serveur VPN dans une DMZ



- Intérêt de cette architecture
  - Lorsque le tunnel est établi, le client VPN n'accède pas directement au réseau privé, mais est soumis aux règles du pare-feu (aucun flux venant d'internet n'entre directement dans le réseau local)

4.d Autres points sur les VPN

- Il est possible d'interconnecter deux réseaux privés par VPN
  - VPN d'accès distant : relation entre deux sites d'une entreprise
  - VPN intersite : relation entre un client et son fournisseur
- Certains terminaux (smart phones) sont compatibles VPN
- Il est possible d'utiliser un téléphone sécurisé (ex : application VoIP SoftPhone)

4.d Avantages des VPN

- Avant l'avènement des VPN, les employés en déplacement se connectaient au réseau de leur entreprise au moyen d'appels longue distance. Avec les VPN, ils peuvent utiliser une connexion locale à internet et leur logiciel client VPN pour aboutir au même résultat.
- Amélioration de la productivité des utilisateurs car ils se connectent de façon sécurisée aux ressources de l'entreprise indépendamment de la zone géographique où ils se trouvent
- Baisse des coûts de fonctionnement par le remplacement de lignes WAN dédiées par des connexions internet directes à large bande grâce auxquelles les bureaux distants peuvent communiquer via un VPN intersite
- Une grande entreprise peut simplifier la topologie de son infrastructure en ajoutant des VPN à des emplacements stratégiques

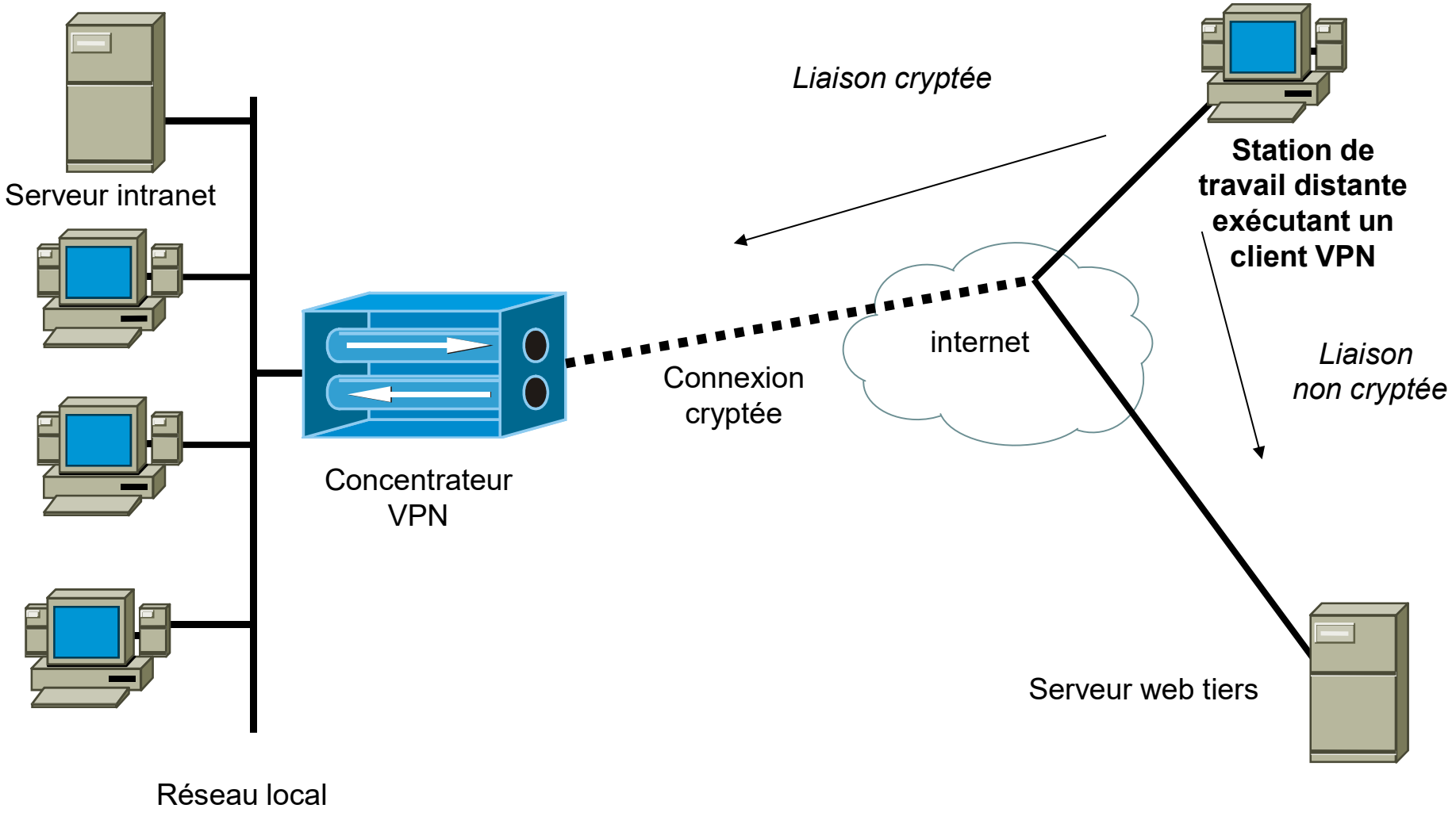
4.d Split-tunneling

- Dans beaucoup d'environnements, les utilisateurs distants ont l'obligation d'accéder aux ressources par l'intermédiaire d'un VPN
  - Un VPN n'autorise habituellement pas un utilisateur à accéder à la fois au réseau de l'entreprise et aux ressources de son LAN
    => Pb par exemple si l'utilisateur veut lancer en même temps une impression sur son imprimante locale
  - La fonction de *split-tunneling* fournit une solution
  - Le split-tunneling intervient aussi lorsqu'un utilisateur ou un site est autorisé à utiliser le VPN tout en étant connecté à un réseau public

    => non nécessité que le trafic destiné au réseau public passe par le tunnel

    => ATTENTION à la configuration du client : cette situation peut permettre à un attaquant de compromettre l'ordinateur et éventuellement de s'en servir comme d'une passerelle vers le réseau privé

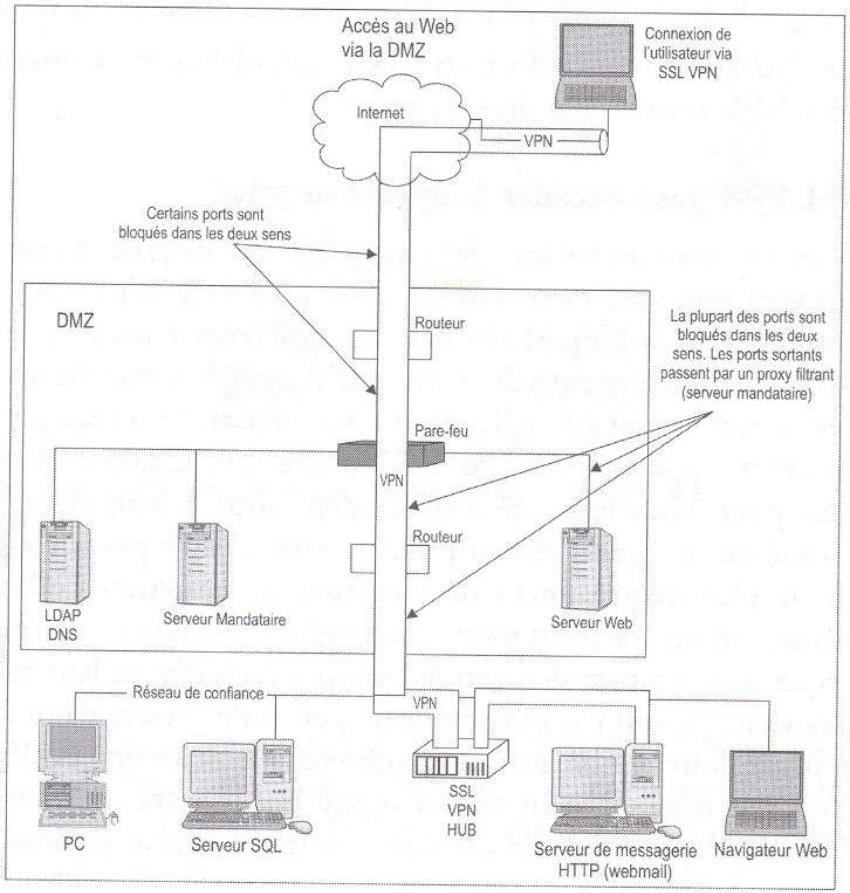
4.d Présentation du split-tunneling



4.d Etablissement d'une connexion VPN cryptée

Modèles d'installation de SSL VPN : Accès via un serveur SSL VPN à certains périphériques du réseau interne

- Client connecté via internet (non sûr) à un serveur SSL VPN situé dans le réseau interne

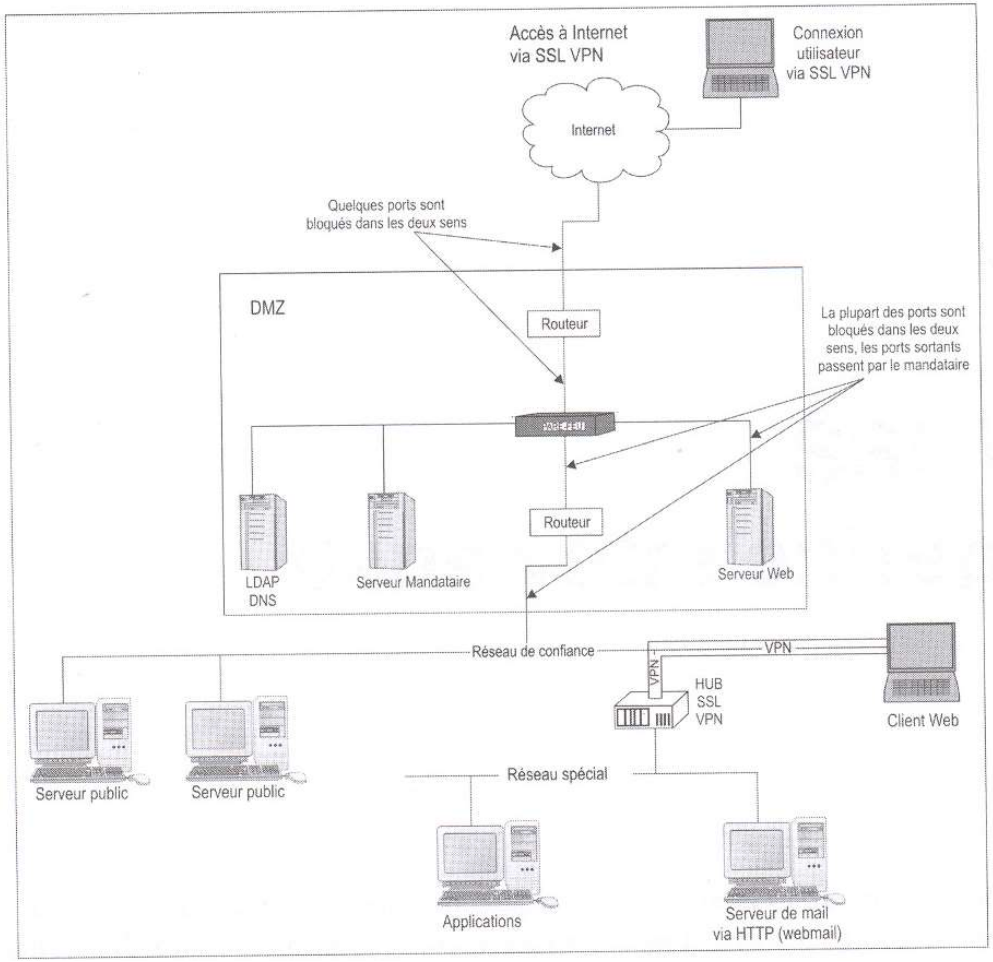


Modèles d'installation de SSL VPN : Accès via un serveur SSL VPN à certains périphériques du réseau interne

- Trames réseau routées dans la DMZ
  - Elles arrivent sur le premier routeur (routeur frontière (border router))
  - Le routeur va affecter une IP de la DMZ à cette connexion
  - La DMZ vérifie ensuite cette connexion
    - Inscription dans les logs (historique de connexion)
    - Détection des attaques de déni de service
    - …
- Si tout va bien, la connexion est transmise au routeur situé entre la DMZ et le réseau interne
  - L'adresse de destination est alors modifiée à nouveau pour mettre l'adresse IP du serveur SSL VPN interne du réseau interne
- La trame arrive au serveur SSL VPN interne
  - Le serveur SSL va assurer des vérifications supplémentaires, après déchiffrement du tunnel
    - Authentification du client
    - Négociation des protocoles de chiffrement
  - La communication pourra être transmise au serveur demandé (exemple : messagerie)

Modèles d'installation de SSL VPN : Accès via un serveur SSL VPN à un réseau spécial dédié aux accès distants sécurisés

- SSL VPN pour accéder à un réseau privé



Modèles d'installation de SSL VPN : Accès via un serveur SSL VPN à un réseau spécial dédié aux accès distants sécurisés

- Exemple des grandes entreprises
  - Plusieurs réseaux privés interconnectés
  - Interconnexion par plusieurs fournisseurs d'accès (ISP: Internet Service Provider)
  - Utilisation de POP (Point of Presence), points d'accès à internet => points sensibles en terme de sécurité
  - Pas toujours confiance en l'ensemble des employés de la société
- Utilisation de SSL VPN pour fournir un accès sûr à un réseau interne spécial depuis le réseau interne à confiance limitée

SSL VPN au niveau application

- Pourquoi ?
- De nombreux périphériques interdisent la création de canaux de communication de niveau 3, mais autorisent les communications de niveau 7 à travers un navigateur web
- La politique de sécurité la plus élémentaire interdit de connecter au réseau d'une société des ordinateurs de cybercafé ou empruntés à un inconnu
- Inconvénient : très peu de standards forts au niveau applicatif
- Communication au niveau des couches 6 et 7 => Impact important en terme de sécurité

Avantages SSL VPN vs. serveur mandataire (proxy)

- Accéder aux applications non web
- Accès aux fichiers, imprimantes et autres ressources informatiques
  - Montage de dossier distant
  - Interface web d'accès aux fichiers
- Accès aux imprimantes ou à d'autres ressources
- Accès telnet, accès à des terminaux
  - Telnet, SSH, Putty…
- Serveurs de terminaux
- Accès à un intranet
  - Via une adresse privée non routable
  - Via un domaine DNS non publié (ex : gtr.iut)
- Accès distant cohérent et ergonomique en terme d'interface
- Accès, si besoin, au réseau interne de l'entreprise (SSL VPN intègre des fonctionnalités de sécurité informatique)

Accès au réseau interne de l'entreprise

- Etablissement de connexion réseau à travers le tunnel SSL
  - Niveau 3
  - Le serveur SSL envoie au client un programme (ActiveX ou applet Java) qui crée une interface réseau virtuelle
  - Le client reçoit une adresse IP du réseau interne
  - Trame d'information chiffrée dans son intégralité
- Deux types de tunnel
  - Tunnel complet : tout le flux réseau passe par le tunnel réseau => flux vers le réseau interne et flux vers internet
  - Tunnel partiel : seules les connections à destination du réseau interne passent par le tunnel

Sécurisation d'un accès SSL VPN
1. Identification et autorisations

- Identification
  - Mots de passe
  - Mots de passe à usage unique
    - À partir d'une liste de mots de passe
    - Périphérique matériel ou logiciel générant des mots de passe uniques (fonction de l'heure, d'une clé …)
    - Technique de challenge-response
  - Informations biométriques
  - Certificats numériques du client
    - Nécessite un périphérique spécifique et de confiance
  - Cartes à puce ou clé USB
    - Contiennent un certificat numérique qui ne peut être extrait. Seule une signature numérique en sort, prouvant l'identité de l'utilisateur

Sécurisation d'un accès VPN
2. Sécurité du client

- Données sensibles dans un endroit non sûr
  - Récupération sur l'ordinateur portable de données provenant du site de l'entreprise
  - Cache (navigateurs + fichiers)
  - Cache non standards (utilisées par certaines applications commerciales …)
  - Fichiers temporaires (ouverture de pièces jointes de messagerie)
  - Mémorisation des adresses e-mail (lorsqu'on remplit un formulaire par internet) ou des adresses web (navigateur)
  - Cookies
  - Historique de navigation
  - Swap (fichier d'échange, ou mémoire d'appoint) : peut être amené à stocker des données sensibles (la récupération est difficile, mais pas impossible)

Sécurisation d'un accès SSL VPN
2. Sécurité du client

- Corrections possibles
  - Utiliser la commande NOCACHE dans le navigateur
    - Evite seulement le non stockage des éléments web reçus
    - Peut entraîner des dysfonctionnements (à l'ouverture d'un fichier PDF ou Word par exemple)
  - Supprimer toutes les données mises en cache en fin de session, difficile :
    - Navigateur « plante »
    - Fermeture du navigateur sans déconnexion
    - Plantage ordinateur…
  - Utiliser un stockage chiffré supprimé à la fin de la session
    - Stockage de toutes les informations de session dans un disque virtuel
    - Suppression du disque virtuel en fin de session => si plantage système, le disque peut être effacé à la réinitialisation, et de toute façon, le contenu chiffré est illisible
    - Difficulté : cette solution ne marche pas avec tous les programmes

Sécurisation d'un accès SSL VPN
2. Sécurité du client

- Effacement des fichiers
  - Un simple « efface » sur un système d'exploitation n'efface pas le fichier physiquement
  - Norme militaire : un effacement physique signifie que l'on a réécrit sur le fichier au moins trois fois de suite des suites aléatoires de 0 et de 1
- Fermeture automatique de session au bout d'un certain temps d'inactivité
  - Préférer les solutions qui consistent à prévenir l'utilisateur (ex : « êtes-vous toujours présent ? » nécessitant de cliquer sur OUI pour empêcher la connexion de s'arrêter) une ou deux minutes avant la fin de la session

Sécurisation d'un accès SSL VPN
2. Sécurité du client

- Virus entrant dans le réseau interne via SSL VPN
- Solutions
  - Vérifier la présence d'un anti-virus sur le poste client (activation, date de mise à jour)
    - Avant de lui donner accès
  - Interdire les envois de fichiers
  - Se baser sur l'anti-virus interne de la société
    - Fichiers envoyés ou attachés à un courriel sont scannés par le serveur à leur arrivée

Sécurisation d'un accès SSL VPN
2. Sécurité du client

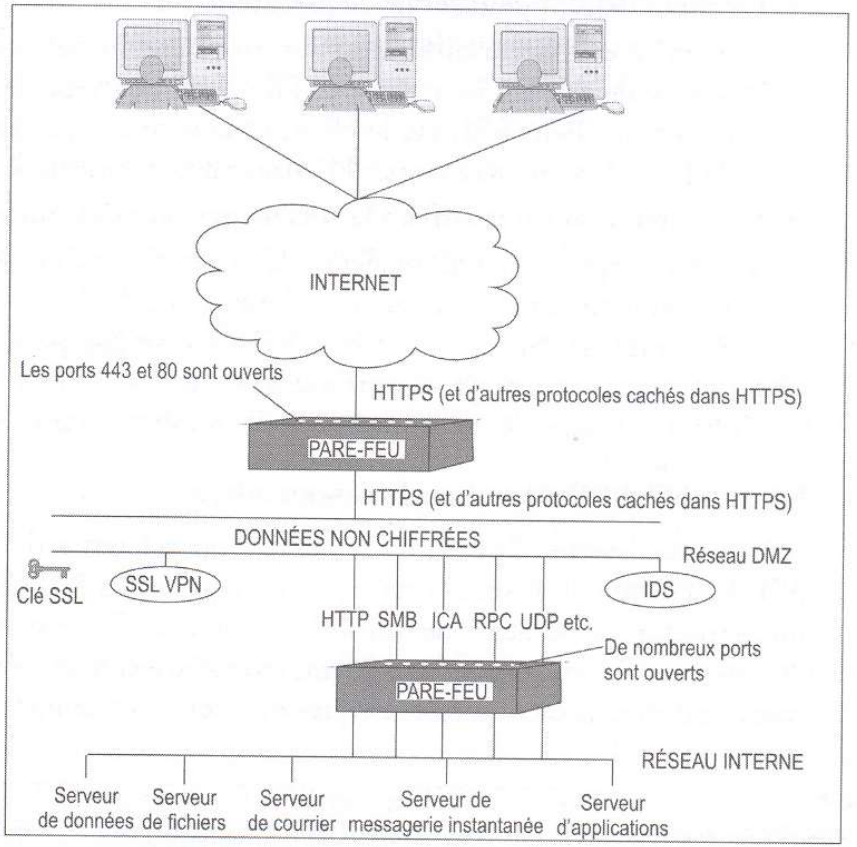
- Un ver accède au réseau interne via SSL VPN
- Solution : interdire la connexion à une machine non protégée contre les vers
  - Utilisation de pare-feu personnels (ne laissent pas passer le trafic réseau non voulu, donc les vers)
  - Utilisation de pare-feu applicatifs (avec des règles de filtrage)

Droits d'accès en fonction de la sécurité du périphérique distant

Sécurité du périphérique distant	Sécurité du périphérique distant	Sécurité du périphérique distant	Droits d'accès sur le SSL VPN	Droits d'accès sur le SSL VPN	Droits d'accès sur le SSL VPN	Droits d'accès sur le SSL VPN
Machine de confiance ?	**Antivirus installé et mis à jour?**	**Possibilité de supprimer les fichiers temporaires ?**	**Autorisation de lecture du courrier électronique**	**Autorisation d'envoi de courriers électroniques**	**Autorisation d'ouverture des pièces jointes**	**Autorisation d'envoi de pièces jointes**
Non	Oui	Oui	Oui	Oui	Oui	Oui
Non	Oui	Non	Oui	Oui	Non	Oui
Non	Non	Oui	Oui	Oui	Oui	Non
Non	Non	Non	Oui	Oui	Non	Non
Oui, confiance niveau II	Oui	Oui/Non	Oui	Oui	Oui	Oui
Oui, confiance niveau II	Non	Oui/Non	Oui	Oui	Oui	Non
Oui, confiance niveau I	Oui/Non	Oui/Non	Oui	Oui	Oui	Oui

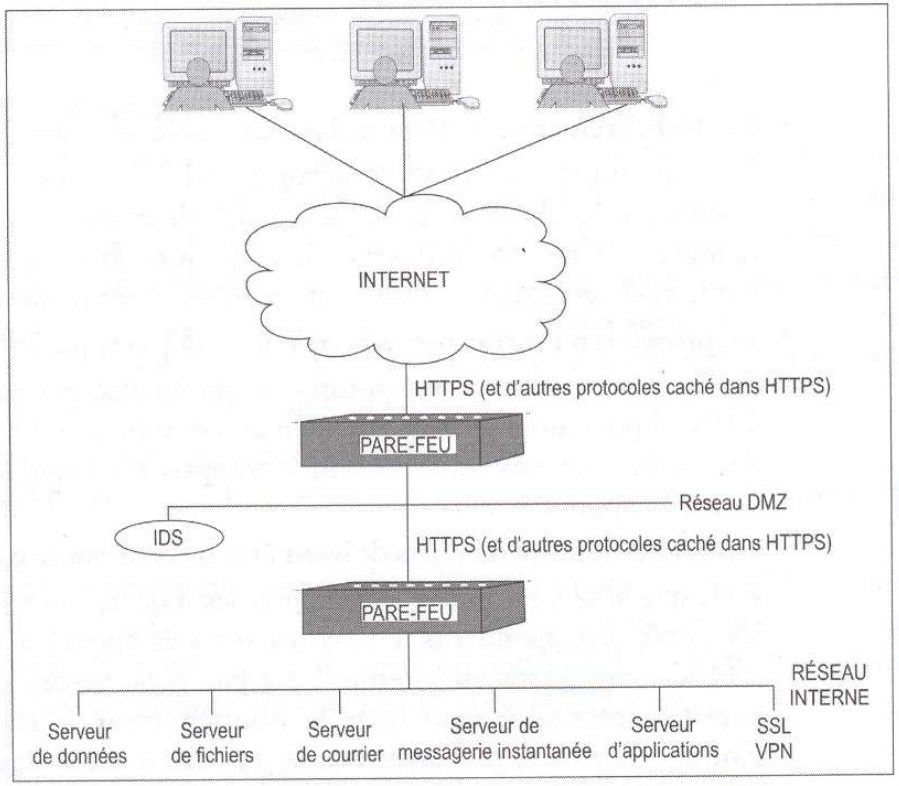
Sécurisation du serveur SSL VPN

- Pare-feu
  - Communications ouvertes pour TCP/IP, et parfois même UDP et ICMP
- Serveur SSL VPN situé dans la DMZ
  - Pare-feu doit transmettre le port TCP 443 vers l'extérieur (souvent aussi le port 80)
  - Les clés de chiffrement SSL sont stockées dans un environnement non sûr (la DMZ)
  - Le chiffrement est effectué dans une zone non sûre (en particulier, la communication entre le serveur SSL VPN et le réseau interne est non chiffrée)
  - La protection fournie par le pare-feu est déjouée par le SSL VPN (il est possible de faire passer à travers le tunnel des protocoles réseau qui auraient été interdits par le pare-feu)
  - Un grand nombre de ports doivent être ouverts sur le pare-feu interne…
  - Un client distant peut servir de passerelle vers un autre réseau



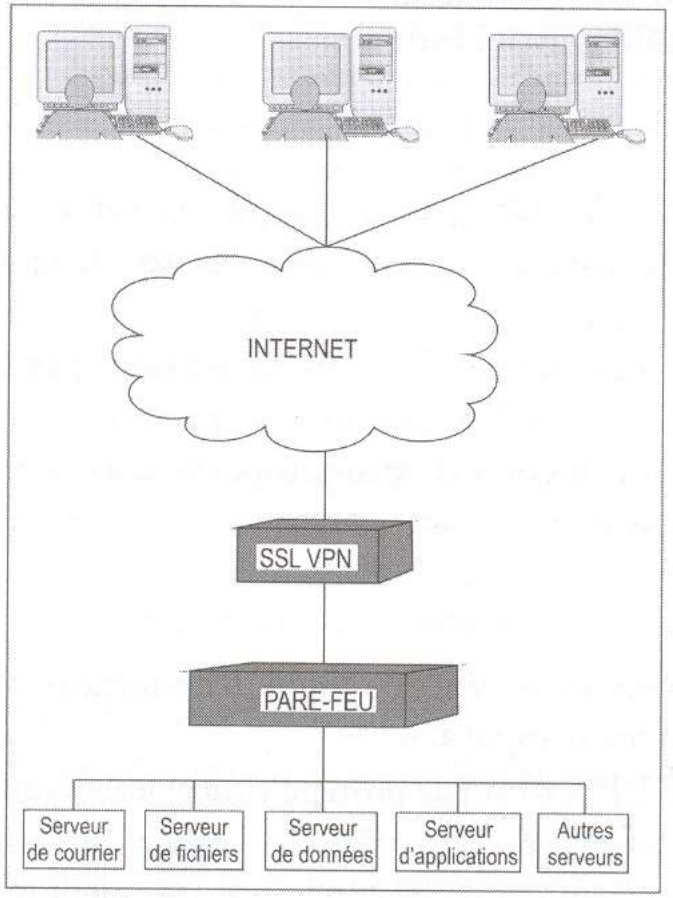
Sécurisation du serveur SSL VPN

- Serveur SSL VPN situé dans le réseau interne
  - Toute l'infrastructure du pare-feu est remise en cause
  - Des utilisateurs non identifiés peuvent envoyer des informations dans le réseau interne (ex : des trames envoyées par des utilisateurs souhaitant s'identifier)
  - Le logiciel de détection d'intrusion (IDS) installé dans la DMZ sera inefficace (car les informations passant par le tunnel sont cryptées)



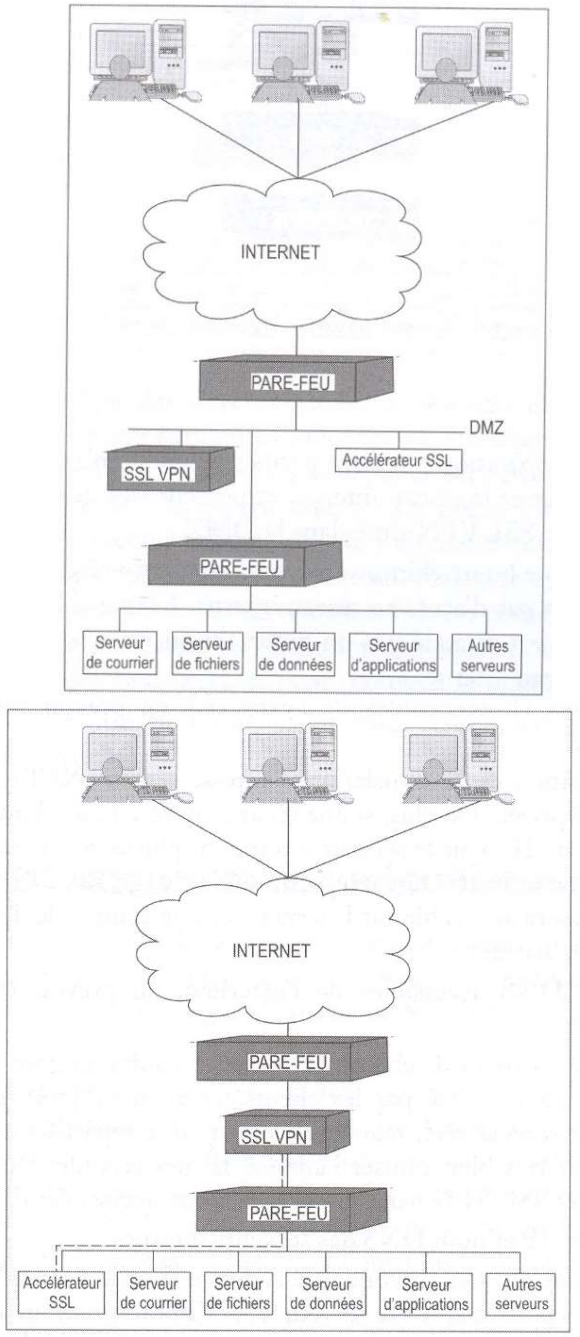
Sécurisation du serveur SSL VPN

- SSL VPN en dehors du pare-feu extérieur
- Avantages
  - Les protocoles non autorisés ne rentrent pas ni dans le réseau interne, ni dans la DMZ
  - Les utilisateurs non identifiés ne rentrent pas ni dans le réseau interne, ni dans la DMZ
  - Les systèmes de détection d'intrusion peuvent détecter les attaques, aussi bien dans la DMZ que dans le réseau interne
- Inconvénients
  - Serveur SSL VPN non protégé des attaques réseau
  - Clés SSL de déchiffrement dans un environnement hostile
  - Nécessité d'ouvrir de nombreux ports sur les pare-feu externe et interne



Sécurisation du serveur SSL VPN

- Calcul SSL externalisé
  - Décharger le serveur SSL VPN principal en confiant le calcul du chiffrement et du déchiffrement à une machine externe dédiée
- Attention : si l'on veut poser le serveur de calcul dans un réseau plus sûr que le serveur SSL VPN lui-même, il faut ouvrir des ports sur les pare-feu intermédiaires, par ex :
  - Décharger le calcul SSL d'un serveur situé sur internet dans la DMZ
  - Décharger le calcul SSL d'un serveur situé dans la DMZ dans le réseau interne
  - Décharger le calcul SSL d'un serveur situé sur une DMZ externe dans une DMZ interne
- Avantages
  - Chiffrement et déchiffrement dans un endroit sûr
- Inconvénients
  - Ouverture du port réseau

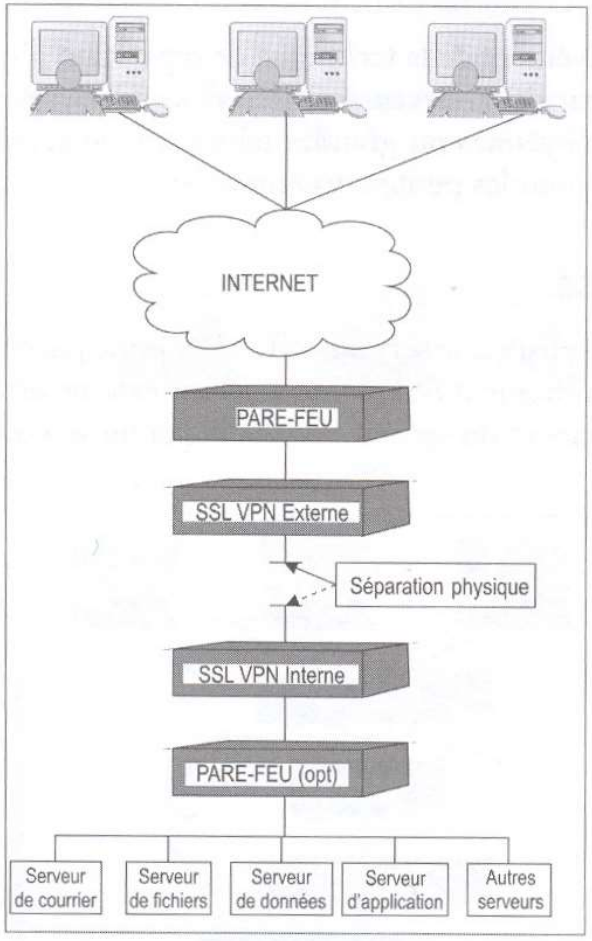


Solutions pour la sécurisation du serveur SSL VPN

- Pas de solution toute faite
- Combiner divers outils de sécurité
- Le SSL VPN doit s'assurer qu'il interagit bien avec le pare-feu de l'entreprise et s'intègre bien dans son infrastructure
- =>L'Etablissement de connexion réseau à travers un tunnel SSL VPN ne devrait être autorisé que depuis des machines qui sont autorisées dans le réseau local (les machines maintenues dans l'entreprise)
- Prendre conscience du fait que même dans ce cas, le pare-feu de la machine devient de fait un pare-feu de l'entreprise => il n'est pas forcément dimensionné pour
- Préférer de manière générale d'autres accès distants que l'accès réseau (c'est-à-dire éviter de donner la possibilité à une machine d'aller n'importe où dans le réseau en se connectant par VPN), par exemple :
  - Router à travers le tunnel uniquement les ports requis
  - Ne permettre qu'un accès restreint (qui ? quelle application ? quel serveur ? depuis quel périphérique (un ordinateur connu avec pare-feu et anti-virus à jour))

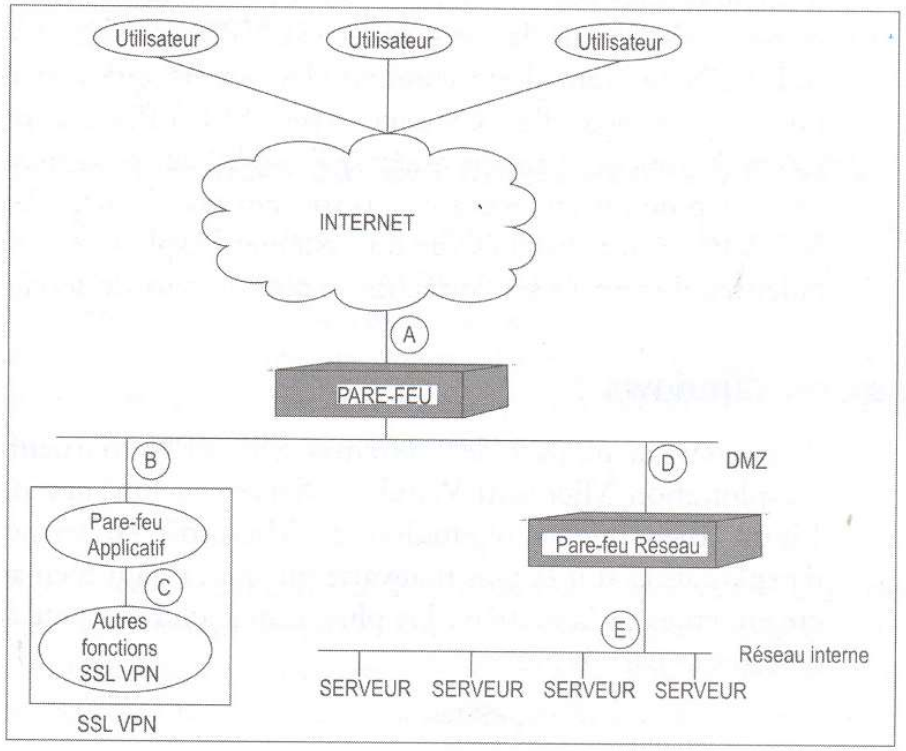
Solutions pour la sécurisation du serveur SSL VPN

- Problème du stockage du certificat SSL
  - Utiliser un accélérateur SSL => permet d'accélérer les temps de traitement et de stocker les certificats dans l'environnement sécurisé de l'accélérateur SSL
  - Utiliser une « séparation physique », appelée Air Gap Technology, qui permet de déporter le certificat dans l'environnement sécurisé du réseau interne. Cette technique consiste à utiliser deux serveurs partageant une mémoire commune (banque de mémoire leur permettant de communiquer)
    - un serveur est relié à internet
    - un serveur est relié au réseau interne et fait tourner l'ensemble des fonctions SSL VPN
  - Utiliser les deux en même temps pour protéger encore plus efficacement les certificats



Problème des failles applicatives

- Des failles peuvent être détectées dans l'application serveur
- Le système d'exploitation utilisé par le serveur SSL VPN peut être vulnérable à des problèmes de sécurité spécifiques
- Protection à envisager
  - Mettre en place un filtrage applicatif pour protéger des vers (à droite les données circulent selon le chemin ABCDE)
  - Filtrage des requêtes envoyées par un client distant à un serveur interne via le SSL VPN



Autres considérations sur les serveurs SSL VPN

- Utiliser un chiffrement adéquat
- Mettre à jour les logiciels serveurs SSL VPN (bogues)
- Linux ou Windows
  - Aucun système n'est parfait
  - Se tenir informé des failles de sécurité rencontrées et mettre à jour les systèmes
- Considérer la séparation physique
  - Mais chère (deux serveurs)
- Ne pas oublier également de sécuriser le serveur SSL VPN dans le réseau interne
  - Protéger contre toute attaque venant de l'intérieur du réseau
  - Exiger un mot de passe pour l'accès à toutes les fonctionnalités d'administration du serveur
  - Configuration du pare-feu entre le réseau interne et le serveur SSL VPN (évite la propagation des vers et spywares)

Utilisation d'un serveur SSL VPN : Déterminer les besoins de l'entreprise

- Communication inter-sites (donner l'illusion d'un réseau complet)
  - Préférer IPSec
    - utiliser les technologies de réseaux privés virtuels entre les sites, et les relier entre eux
    - Équipement ou logiciel dédié installé dans le pare-feu en bordure de réseau
- Communication d'un utilisateur vers un site d'exploitation
  - Accès distant des utilisateurs aux ressources du réseau interne tels les fichiers, applications, bases de données, services de terminaux => technologie SSL VPN appropriée pour ce type d'accès distant

Utilisation d'un serveur SSL VPN : Déterminer les besoins des utilisateurs

- Accès distant au courrier électronique
  - Solutions de service SSL VPN dédiées au courrier électronique
- Accès complet au réseau
  - Préférer une solution à base de IPSec + authentification du client par certificat numérique, avec reconnaissance d'une machine spécifique => à limiter à quelques rares utilisateurs
- Accès aux clients et fournisseurs de l'entreprise
  - Serveur SSL VPN pouvant prendre en charge des configurations avec gestion complexe des droits d'accès (applications accessibles différentes en fonction des types de profils et du compte connecté)
- Accès distant à une station de travail pour un ou deux utilisateurs
  - Préférer l'utilisation d'un logiciel simple de prise de contrôle distant sécurisé tel PcAnywhere ou des logiciels de la suite VNC (UltraVNC, TightVNC, etc…) peu chers et répondant exactement à la fonctionnalité attendue

Modèles de serveurs SSL VPN

- 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

4.e Serveur RADIUS

4.e Serveur RADIUS

- Remote Authentication Dial-In User Service : service d'authentification des utilisateurs pour des connexions à la demande
- Permet de sous-traiter les demandes d'ouvertures de session et le suivi des connexions
- Service largement utilisé par les fournisseurs d'accès internet
- RADIUS n'est pas un standard officiel, mais est maintenu par un groupe de travail de l'IETF

4.e Introduction

- Protocole permettant de centraliser l'authentification et l'autorisation des utilisateurs distants
  - Services et applicatifs prenant en charge une authentification RADIUS : routeurs, pare-feu, bornes réseaux sans fil, etc…
  - Développé par Linvingstone Entreprise Inc
  - IETF (RFC 2865-2866 et 2869)
  - Protocole client/serveur fonctionnant sur UDP

4.e Utilisation d'un serveur RADIUS (ex 1 sous Windows server)

- Utilisation de la base d'annuaire Active Directory afin d'authentifier les accès à internet des utilisateurs des réseaux privés
  - Le pare-feu qui permet la connexion à internet dispose de règles imposant une authentification des utilisateurs afin de leur octroyer ou non l'accès
  - La technologie de pare-feu utilisée prend en charge le protocole RADIUS

⇒ Nous pouvons configurer le pare-feu en tant que client RADIUS d'un serveur RADIUS fonctionnant sous W. Server et membre du domaine Active Directory dont font partie les utilisateurs

⇒ Ceci offre une authentification d'accès à internet pour les utilisateurs, sans avoir à définir une nouvelle base de comptes pour le pare-feu (et complexifier inutilement la gestion et l'utilisation des mots de passe)

4.e Utilisation d'un serveur RADIUS (ex 2)

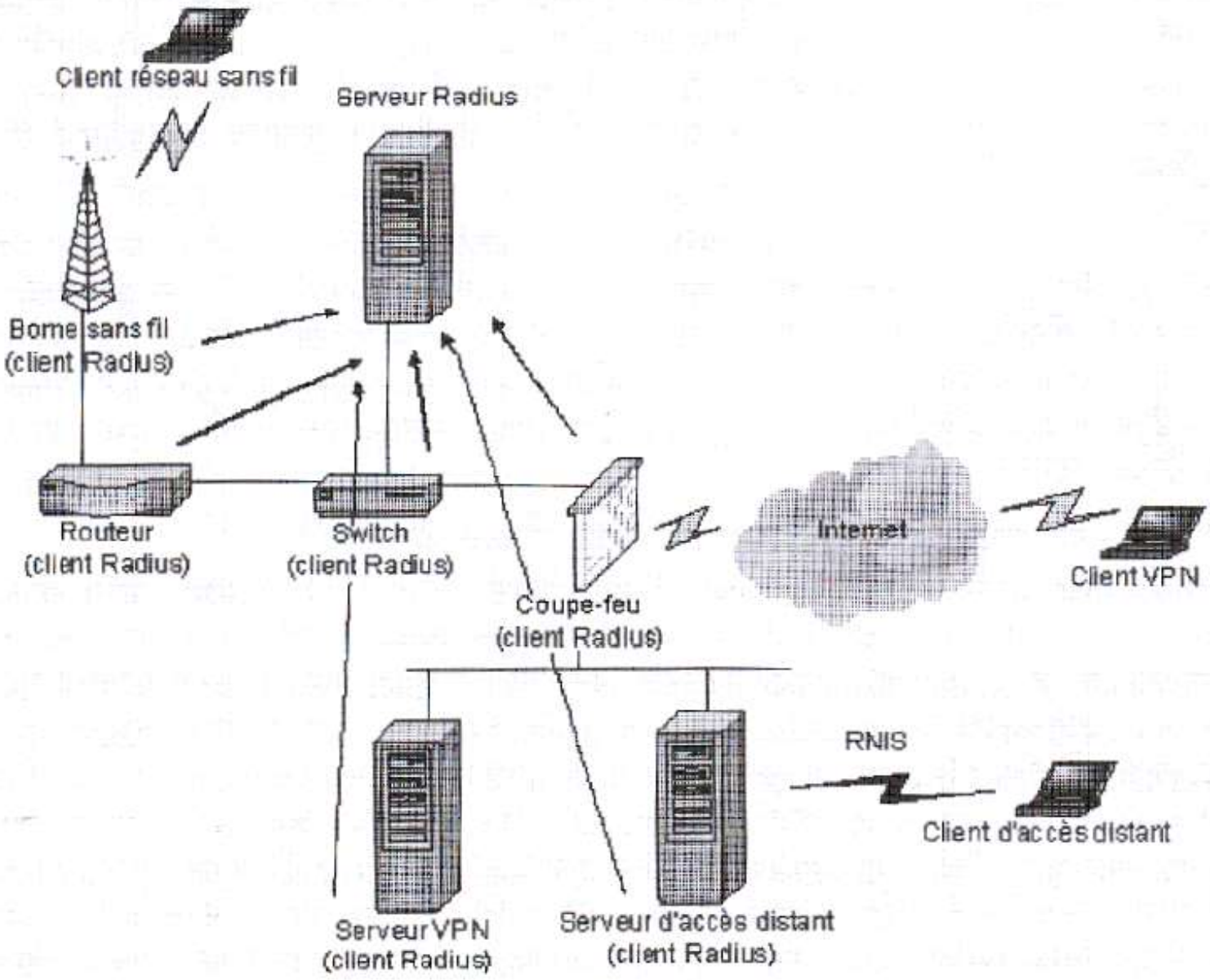
- L'entreprise possède plusieurs serveurs d'accès distant et serveurs VPN
  - Création d'une ou un ensemble de stratégies sur le serveur RADIUS
  - Configuration des serveurs d'accès distants et VPN comme clients RADIUS

Utilisation d'un serveur RADIUS (ex 3)

- On souhaite renforcer la sécurité d'accès aux bornes du réseau sans fil. Le protocole RADIUS peut être utilisé

4.e Autres intérêts d'utiliser un serveur RADIUS

- Centralisation de l'authentification (déjà vue)
- Authentification de clients VPN dans un domaine auquel le serveur VPN n'appartient pas
- Ex : positionnement dans la DMZ d'un serveur VPN dans un groupe de travail, et faire en sorte que l'authentification des clients VPN se fassent dans leur domaine, en redirigeant les requêtes d'authentification vers un serveur RADIUS membre du domaine


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)

4.e Configuration du serveur RADIUS

- Création de stratégies d'accès distant
- Authentification des clients
- Définition des clients Radius pour lesquels le serveur Radius va opérer

- Utilisation de la MMC "Service d'authentification internet"

4.e Configuration du client RADIUS

- Utilisation de la console "Routage et accès distant"
- "Propriétés du serveur"
- "Fournisseur d'authentification"
- "Authentification RADIUS"
- "Configurer"

Références Bibliographiques

- 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, accès web et extranets sécurisés – J. Steinberg & T. Speed, Eyrolles, 2006.
- 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