Avant-propos

Cet ouvrage présente les mécanismes de sécurité déployés dans les réseaux Ethernet, Wi-Fi (*Wireless-Fidelity*), IP (*Internet Protocol*) et MPLS (*Multi-Protocol Label Switching*). Ces mécanismes sont classés selon les quatre fonctions suivantes :

– la protection des données ;

– le contrôle d'accès ;

– le cloisonnement du réseau ;

– la surveillance des données.

La protection des données est fournie par les services de confidentialité et de contrôle de l'intégrité des données :

– la confidentialité consiste à s'assurer que les données ne puissent être interprétées que par des personnes autorisées. Ce service est obtenu à partir du mécanisme de chiffrement des données concernées ;

– le contrôle d'intégrité consiste à détecter des modifications des données transférées. Ce service est obtenu à partir d'une fonction de hachage ou d'un algorithme de chiffrement qui génère un sceau.

Le contrôle d'accès est fourni par le service d'authentification d'un tiers. Ce service consiste à vérifier l'identité de la personne qui désire accéder à un réseau. Ce service est généralement obtenu à partir d'une fonction de hachage, comme pour le contrôle d'intégrité.

Le cloisonnement du réseau est fourni par le service VPN (*Virtual Private Network*). Ce service permet de constituer des groupes fermés d'utilisateurs et à autoriser la communication uniquement entre les utilisateurs appartenant au même groupe. Il est à noter que le contrôle d'accès permet également de cloisonner implicitement le réseau.

La surveillance des données consiste appliquer des règles sur les données afin d'autoriser leur transfert ou de détecter des attaques. Le service est fourni à partir de l'analyse des champs des différents protocoles constituant la structure des données.

Le réseau

Le rôle du réseau est l'acheminement de données entre deux hôtes. Le réseau est constitué de deux entités (figure 1) :

– le LAN (*Local Area Network*) est le réseau sur lequel se connectent les hôtes. C'est généralement un réseau privé déployé par les entreprises ;

– le WAN (*Wide Area Network*) est le réseau qui assure l'interconnexion des réseaux LAN. C'est généralement un réseau public déployé par les opérateurs d'accès et de transit Internet.

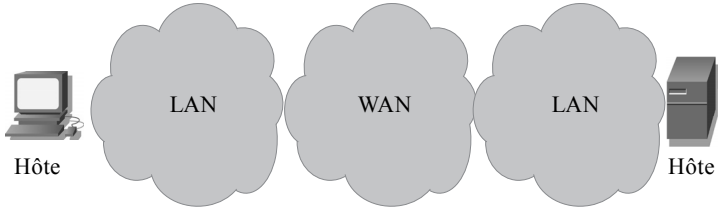

Figure 1. *L'architecture du réseau*

Le réseau LAN est construit à partir de deux types de blocs, le bloc d'accès et le bloc cœur (figure 2) :

– le bloc d'accès connecte les hôtes du réseau. Les blocs d'accès peuvent être dédiés à des types d'hôtes différents :

- les ordinateurs, les postes téléphoniques,
- les serveurs d'application,
- le système d'exploitation du réseau et de la sécurité,
- le réseau WAN ;

– le bloc cœur permet d'interconnecter les blocs d'accès.

Le réseau WAN du fournisseur d'accès Internet est structuré en trois entités (figure 3) :

– le réseau d'accès. Il correspond au raccordement du réseau LAN au premier site technique de l'opérateur ;

– le réseau d'agrégation. Il procède à la collecte du trafic issu des réseaux d'accès. Il a généralement une couverture régionale ;

– le cœur de réseau. Il connecte les différents réseaux d'agrégation. Il a généralement une couverture nationale. Il procure également l'interface entre les opérateurs.

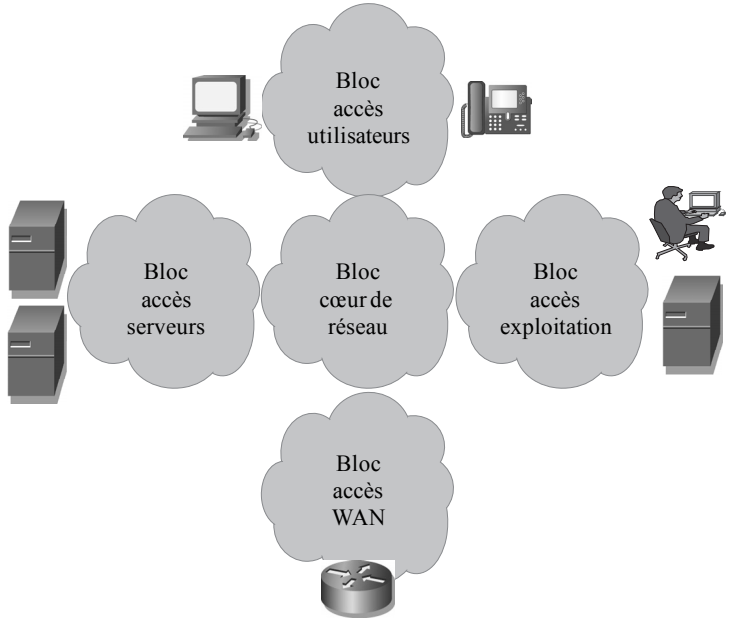

Figure 2. *L'architecture du réseau LAN*

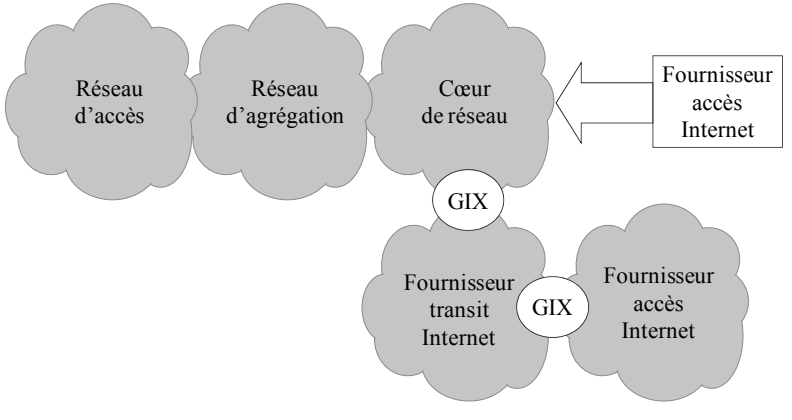

Figure 3. *L'architecture du réseau WAN*

L'interconnexion des réseaux WAN des différents fournisseurs d'accès Internet s'effectue au niveau du cœur de réseau de deux manières différentes :

– soit la connexion est directe, lorsque les fournisseurs d'accès Internet opèrent sur le même territoire ;

– soit la connexion est réalisée par un fournisseur de transit Internet dans le cas contraire. Le réseau du transit Internet a une architecture semblable à celle du cœur de réseau du fournisseur d'accès Internet.

Un point d'échange GIX (*Global Internet eXchange*) permet aux différents fournisseurs d'accès et de transit Internet d'échanger du trafic grâce à des accords mutuels dits de *peering*, généralement basés sur l'équilibrage des volumes de données transmises et reçues (figure 3).

Introduction à la cryptographie

Le chapitre 1 présente les concepts fondamentaux relatifs à la cryptographie. La cryptographie traite les aspects liés à la sécurité des communications, dans le but d'offrir les services de confidentialité, de contrôle d'intégrité et d'authentification d'un tiers.

Le service de confidentialité est mis en œuvre par des mécanismes de chiffrement. On distingue deux grandes familles d'algorithmes cryptographiques : les algorithmes symétriques à clé secrète et les algorithmes asymétriques à clé publique et privée.

Les algorithmes symétriques sont bien adaptés au chiffrement des données mais posent le problème de l'établissement de la clé secrète. Deux méthodes couramment utilisées sont la génération à partir de l'algorithme Diffie-Hellman ou le transport de la clé secrète par des algorithmes asymétriques. Le chiffrement est fourni par exemple par l'algorithme AES (*Advanced Encryption Standard*) ou 3DES (*Triple Data Encryption Standard*).

Les algorithmes asymétriques trouvent leur champ d'application dans le transport de la clé secrète et la signature numérique. Pour le premier cas, la clé secrète est chiffrée par la clé publique et déchiffrée par la clé privée. Pour le second cas, c'est l'inverse qui se produit. Le chiffrement est fourni par des algorithmes basés sur l'exponentiation modulaire comme l'algorithme RSA (nommé par les initiales de ses trois inventeurs Rivest, Shamir, Adleman) ou sur les courbes elliptiques ECC (*Elliptic Curve Cryptography*).

La fonction de hachage est un autre type de fonction cryptographique. Elle convertit une chaîne de longueur quelconque (les données à protéger) en une chaîne

de taille inférieure et généralement fixe (empreinte ou *digest*). La fonction de hachage peut être fournie par les deux algorithmes suivants :

– MD5 (*Message Digest 5*) qui calcule une empreinte de 128 bits ;

– SHA (*Secure Hash Algorithm*) qui calcule une empreinte de 160 bits à 512 bits.

Le scellement est basé sur la clé secrète et fournit le service de contrôle d'intégrité des données. Le sceau peut être calculé de deux manières différentes :

– l'algorithme de chiffrement symétrique est appliqué aux données, le sceau est alors le dernier bloc du cryptogramme ;

– la fonction de hachage est appliquée à un ensemble comprenant les données et une clé secrète, dont l'association est définie par exemple par la fonction de calcul HMAC (*Hashed Message Authentication Code*).

La signature est basée le chiffrement de l'empreinte par une clé privée et le déchiffrement par une clé publique. Elle fournit le service d'intégrité et de non-répudiation par la source des données reçues par le destinataire.

La distribution des clés publiques est associée à la présentation d'un certificat. C'est une structure de données signée par une autorité de certification qui garantit que l'émetteur de ladite clé publique en est bien le détenteur.

Le mécanisme 802.1x

Le chapitre 2 présente le mécanisme de contrôle d'accès 802.1x déployé dans le réseau LAN mettant en œuvre les technologies suivantes :

– la technologie Ethernet dans le cas d'un accès à un *switch* ;

– la technologie Wi-Fi dans le cas d'une connexion à un point d'accès AP (*Access Point*).

Le mécanisme 802.1x définit trois composants (figure 4) :

– le solliciteur est le dispositif (par exemple l'ordinateur) qui désire accéder au réseau Ethernet ou Wi-Fi ;

– l'authentificateur est le dispositif (le *switch* Ethernet ou le point d'accès Wi-Fi) qui contrôle l'accès du solliciteur au réseau LAN ;

– le serveur d'authentification est le dispositif qui authentifie le solliciteur et autorise l'accès au réseau LAN.

Le mécanisme 802.1x s'appuie sur une suite de protocoles (figure 4) :

– le protocole EAPOL (*EAP* (*Extensible Authentication Protocol*) *Over LAN*) échangé entre le solliciteur et l'authentificateur ;

– le protocole EAP échangé entre, d'une part, le solliciteur et, d'autre part, l'authentificateur ou le serveur d'authentification. Le protocole EAP est porté par le protocole EAPOL sur l'interface entre le solliciteur et l'authentificateur ;

– le protocole RADIUS (*Remote Authentication Dial-In User Service*) échangé entre l'authentificateur et le serveur d'authentification. Le protocole RADIUS porte le protocole EAP sur l'interface entre l'authentificateur et le serveur d'authentification ;

– le protocole EAP-Method échangé entre le solliciteur et le serveur d'application. Le protocole EAP-Method est porté par le protocole EAP.

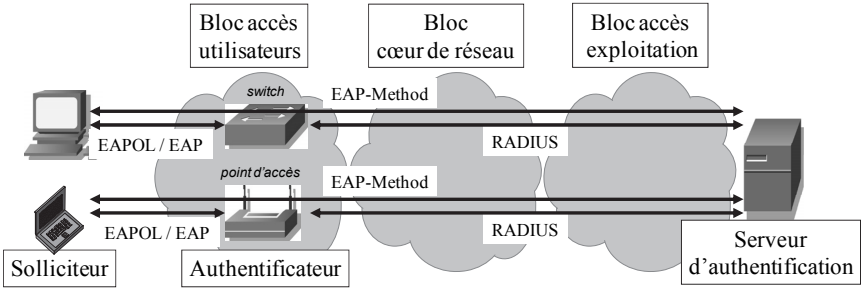

Figure 4. *Le mécanisme 802.1x*

Le protocole EAP-Method propose plusieurs types d'authentification :

– la méthode EAP-MD5. Le client s'authentifie à partir d'un mot de passe. Cette méthode est similaire au protocole CHAP (*Challenge-Handshake Authentication Protocol*) s'appuyant sur le protocole PPP (*Point to Point Protocol*) utilisé pour les liaisons point à point ;

– la méthode EAP-TLS (*Transport Layer Security*). L'authentification est mutuelle entre le solliciteur et le serveur d'authentification par le biais de certificats ;

– la méthode EAP-TTLS (*Tunneled-TLS*). L'authentification est mutuelle entre le solliciteur et le serveur d'authentification par le biais d'un certificat côté serveur d'authentification, le solliciteur pouvant utiliser un mot de passe.

En complément de l'authentification, le protocole EAPOL intervient dans la génération des clés pour le chiffrement et de contrôle d'intégrité utilisées par les mécanismes WPA1 (*Wi-Fi Protected Access*) et WPA2 décrits au chapitre 3.

Les mécanismes WPA

Le chapitre 3 présente les mécanismes de sécurité WPA1 et WPA2 appliqués au réseau Wi-Fi. La technologie Wi-Fi est à l'origine une technologie d'accès au réseau privé LAN, utilisant une transmission radioélectrique. Elle a comme particularité l'utilisation de bandes de fréquences libres. Elle est également déployée au niveau du réseau public WAN pour constituer des *hotspots*.

Les mécanismes de sécurité WPA1 et WPA2 sont utilisés uniquement dans le réseau privé. La sécurité déployée dans le cas de *hotspots* met en œuvre généralement la sécurité du transport décrite au chapitre 5.

La sécurité de l'interface radio a démarré avec le mécanisme WEP (*Wired Equivalent Privacy*). Du fait de ses faiblesses, il a été supplanté par le mécanisme WPA1, puis par le mécanisme WPA2. Ces trois mécanismes implémentent spécifiquement les services de contrôle d'accès d'un tiers et de protection des données.

Pour le mécanisme WEP, le contrôle d'accès d'un tiers est basé sur l'algorithme RC4 (*Rivest Cipher* 4). Le contrôle d'accès a lieu lors de la phase d'authentification, qui est une procédure associée au protocole de liaison de données MAC (*Medium Access Control*).

Les mécanismes WPA1 et WPA2 utilisent pour le contrôle d'accès le mécanisme 802.1x décrit au chapitre 2. La phase d'authentification est précédée par la procédure de mise en accord de la politique de sécurité entre le point d'accès et la station.

Pour les mécanismes WEP et WPA1, le chiffrement est réalisé par l'algorithme RC4. Pour le mécanisme WEP, la clé maîtresse est utilisée pour le chiffrement de chaque trame Wi-Fi.

Pour le mécanisme WPA1, le chiffrement est obtenu à partir d'une clé dérivée de la clé maîtresse, cette clé dérivée étant utilisée temporairement. En association avec le chiffrement, un protocole contenant le vecteur d'initialisation est ajouté au protocole de liaison de données MAC (figure 5) :

– le protocole WEP dans le cas du mécanisme WEP ;

– le protocole TKIP (*Temporal Key Integrity Protocol*) dans le cas du mécanisme WPA1.

Pour le mécanisme WPA2, le chiffrement se base sur l'algorithme AES (*Advanced Encryption Standard*) et l'en-tête du protocole de liaison de données MAC est complété par l'en-tête CCMP (*Counter-mode/Cipher block chaining* MAC (*Message Authentification Code*) *Protocol*) (figure 5).

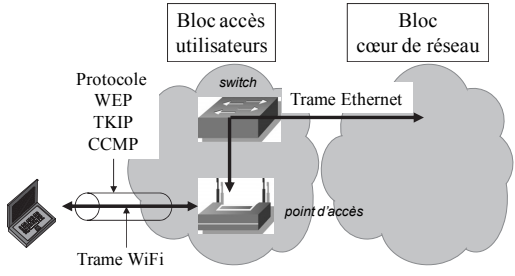

Figure 5. *Les protocoles WEP, TKIP et CCMP*

Le contrôle d'intégrité est offert par un contrôle de redondance cyclique CRC (*Cyclic Redundancy Check*) pour le mécanisme WEP. Le mécanisme WPA1 utilise l'algorithme MICHAEL. Dans le cas du mécanisme WPA2, le contrôle d'intégrité est obtenu à partir de l'algorithme AES.

Le mécanisme IPSec

Le chapitre 4 présente le mécanisme de sécurité IPSec (*Internet Protocol Security*) appliqué au paquet IP. Ce mécanisme comprend deux parties (figure 6) :

– l'établissement de l'association de sécurité entre deux passerelles de sécurité, situées dans le réseau LAN, au niveau du bloc d'accès au réseau WAN ;

– la protection des données entre ces deux passerelles.

L'association de sécurité s'effectue en deux phases :

– la première phase consiste à authentifier les passerelles de sécurité qui désirent établir l'association de sécurité ;

– la seconde phase permet d'établir les paramètres à utiliser pour la mise en œuvre de la protection des données (protocole, algorithme, clé).

Deux versions de protocoles ont été définies pour l'établissement de l'association de sécurité. La première version comporte trois parties :

– le protocole ISAKMP (*Internet Security Association and Key Management Protocol*) définit le cadre de l'établissement, de la modification et de la suppression de l'association de sécurité ;

– le document DOI (*Domain of Interpretation*) définit les paramètres négociés relatifs à l'utilisation du protocole ISAKMP ;

– le mécanisme IKEv1 (*Internet Key Exchange*) définit les procédures d'échange relatives à l'utilisation du protocole ISAKMP.

Le chapitre 4 décrit uniquement la seconde version IKEv2 qui apporte une simplification par rapport à la version précédente. Cette version regroupe les fonctionnalités définies dans IKEv1 et ISAKMP, dont elle supprime les processus inutiles. Elle élimine le caractère générique de la version précédente en intégrant la fonction DOI qui définit les paramètres propres à l'association de sécurité.

La protection des données introduit deux extensions de l'en-tête IPv4 ou IPv6 (figure 6) :

– l'en-tête AH (*Authentication Header*) est conçu pour assurer le contrôle de l'intégrité, sans chiffrement des données (sans confidentialité) ;

– l'en-tête ESP (*Encapsulating Security Payload*) a pour rôle d'assurer le contrôle de l'intégrité et la confidentialité des paquets IP.

La protection des données entre les deux passerelles de sécurité utilise le mode tunnel. Ce mode se caractérise par le fait que l'en-tête AH ou ESP encapsule le paquet IP d'origine, et que l'ensemble est à son tour encapsulé par un nouvel en-tête IP.

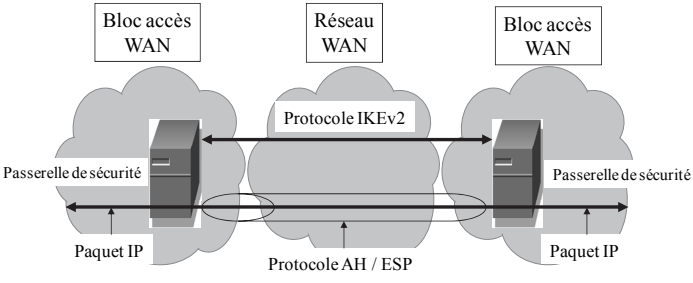

Figure 6. *Le mécanisme IPSec*

Les protocoles SSL / TLS / DTLS

Le chapitre 5 présente les protocoles de sécurité SSL (*Secure Sockets Layer*) / TLS (*Transport Layer Security*) relatifs au transport des données et appliqués aux segments TCP (*Transmission Control Protocol*). Le protocole DTLS (*Datagram TLS*) est une adaptation pour les protocoles de transport UDP (*User Datagram Protocol*), DCCP (*Datagram Congestion Control Protocol*), SCTP (*Stream Control Transmission Protocol*) et SRTP (*Secure Real-time Transport Protocol*).

Le protocole TLS est standardisé par l'IETF (*Internet Engineering Task Force*). Il fait suite au protocole SSL, développé par la société Netscape, dont l'objet était à l'origine d'établir la sécurité des échanges entre un navigateur et un serveur *web*.

Plusieurs versions du protocole TLS ont été définies par la suite : TLS 1.0, TLS 1.1, TLS 1.2. La version TLS 1.0 correspond à la version SSL 3.1 qui est la dernière version du protocole SSL. Les différences entre SSL 3.0, présent dans les navigateurs, et TLS 1.0 sont infimes, mais suffisantes cependant pour rendre ces protocoles incompatibles.

TLS 1.0 a permis de corriger une faille cryptographique de SSL 3.0 et de proposer des algorithmes cryptographiques concernant l'échange de clé et l'authentification. TLS 1.1 est une révision permettant de se protéger contre des attaques mises en évidence sur l'emploi du chiffrement en mode CBC (*Cipher Block Chaining*). TLS 1.2 intègre des éléments épars au sein de la norme et décrit les extensions TLS comme étant un élément à part entière du standard.

La sécurité du transport des données est mise en œuvre entre un client qui initialise la session et une passerelle de sécurité faisant office de serveur, localisée dans le réseau LAN, au niveau du bloc d'accès au réseau WAN.

Les protocoles SSL / TLS correspondent à un en-tête *Record* qui encapsule les messages SSL / TLS ou les données de la couche d'application et aux messages SSL / TLS échangés entre le client et la passerelle de sécurité :

– le message c*hange_cipher_spec* indique une modification des paramètres de sécurité ;

– le message *alert* signale une erreur dans la communication entre l'hôte et la passerelle de sécurité ;

– les messages *handshake* négocient les paramètres de sécurité entre l'hôte et la passerelle de sécurité.

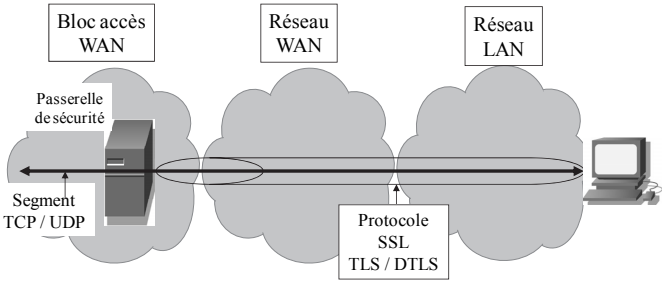

Figure 7. *Les protocoles SSL, TLS et DTLS*

La gestion du réseau

Le chapitre 6 présente les mécanismes de sécurité relatifs aux protocoles liés à la gestion du réseau.

Le protocole SNMP (*Simple Network Management Protocol*) permet de réaliser les fonctions de gestion des équipements (un *switch*, un routeur) qui se répartissent en trois domaines (figure 8) :

– la supervision ou la gestion des alarmes ;

– la gestion de la configuration ;

– la gestion des performances.

Le protocole SNMPv1 est la première version du protocole. La sécurité est basée sur une chaîne de caractères appelée communauté (*community*) qui fournit le droit de lire (*ro read only*) ou de lire et d'écrire (*rw read write*). Cette version présente l'inconvénient de transporter ce mot de passe en clair dans le message SNMP.

Le protocole SNMPv2 est la seconde version du protocole. Il complète la structure de la base de données MIB (*Management Information Base*) décrivant l'équipement sous forme d'objets. Le protocole est également enrichi par de nouveaux messages. En revanche, aucune modification n'est apportée à la sécurité des échanges.

Le protocole SNMPv3 est la troisième version du protocole. Sa principale contribution réside dans l'introduction de mécanismes de sécurité plus robustes :

– le contrôle d'intégrité est basé sur l'algorithme MD5 ou SHA-1 ;

– la confidentialité est assurée par l'algorithme de chiffrement DES.

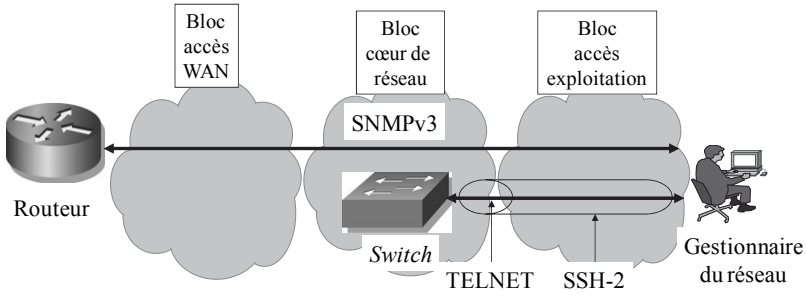

Figure 8. *L'administration du réseau*

TELNET est un protocole permettant la mise en relation d'un client, situé du côté de la plate-forme d'administrateur, avec un interpréteur de commandes côté serveur, localisé dans l'équipement à administrer. L'ouverture de la session TELNET s'effectue sur la base d'un mot de passe circulant en clair entre le client et le serveur.

Le protocole SSH (*Secure Shell*) fournit les services d'authentification, de contrôle d'intégrité et de confidentialité pour les messages TELNET échangés (figure 8). SSH-2 est la version normalisée du protocole. Il comporte trois parties :

– SSH *Transport Layer Protocol* (SSH-TRANS) est le protocole fournissant les bases du contrôle d'intégrité et de la confidentialité ;

– SSH *Authentication Protocol* (SSH-USERAUTH) est le protocole permettant d'authentifier le client ;

– SSH *Connection Protocol* (SSH-CONNECT) est le protocole permettant de maintenir plusieurs sessions sur une connexion SSH.

La technologie MPLS

Le chapitre 7 présente les mécanismes permettant de constituer dans le réseau WAN un cloisonnement au niveau des paquets IP.

Les réseaux d'accès et d'agrégation du réseau WAN sont en fait des réseaux Ethernet, dont le cloisonnement est décrit au chapitre 8 (figure 9).

Le cœur de réseau du réseau WAN est un réseau MPLS intégrant la fonction VPN IP (figure 9).

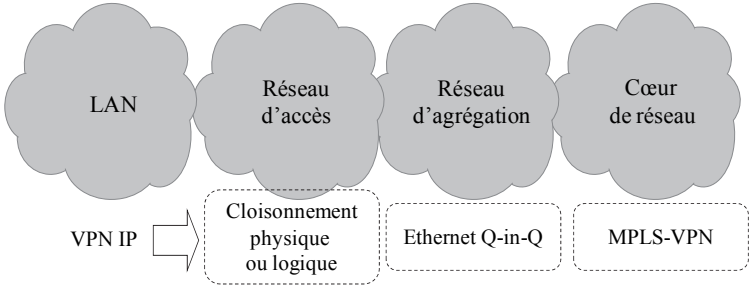

Figure 9. *Le VPN IP*

La fonction MPLS consiste à labelliser un paquet IP et à utiliser ce label pour commuter en remplacement du routage IP. Ce label LSP (*Label Switching Path*) est

porté par un en-tête MPLS qui s'insère entre la couche 3 (IP) et la couche 2 (généralement Ethernet).

La table de commutation des labels LFIB (*Label Forwarding Information Base*) est mise en place par l'intermédiaire de deux protocoles :

– le protocole de distribution de labels LDP (*Label Distribution Protocol*), qui associe un label à une adresse IP de réseau. Ce protocole alimente la table des labels LIB (*Label Information Base*) ;

– le protocole de routage OSPF (*Open Shortest Path First*) ou IS-IS (*Intermediate System to Intermediate System*), qui détermine un port de sortie pour une adresse de réseau IP. Ce protocole renseigne la table de routage RIB (*Routing Information Base*).

La fonction VPN est réalisée par les équipements PE (*Provider Edge*) de bordure du cœur de réseau. Elle consiste à introduire les mécanismes suivants :

– le cloisonnement de la table de routage, afin de ne propager les routes que dans les instances de routage propres à un groupe fermé d'utilisateurs ;

– le marquage des paquets IP par un label particulier. Ce label VPN est porté par un en-tête MPLS supplémentaire.

Le réseau MPLS-VPN introduit les adresses publiques de réseau VPN-IPv4, construites à partir d'adresses de réseau IPv4 publiques ou privées, permettant ainsi de constituer un réseau privé sur une infrastructure publique.

La distribution des labels VPN et des adresses VPN-IPv4 est assurée par le protocole de routage MP-BGP-4 (*Multi-Protocol Border Gateway Protocol*) échangé entre les équipements de bordure PE.

Le réseau MPLS-VPN permet également la construction d'architectures VPN complexes à partir de règles d'importation et d'exportation de routes IPv4.

Le VPN Ethernet

Le chapitre 8 présente les mécanismes permettant de constituer dans les réseaux LAN et WAN un cloisonnement au niveau des trames Ethernet.

Le cloisonnement des trames Ethernet dans un réseau LAN est réalisé par la fonction VLAN (*Virtual LAN*) ou Q-VLAN. Il se base sur le marquage des trames Ethernet, chaque marque correspondant à un groupe fermé d'utilisateurs.

Le cloisonnement des trames Ethernet dans un réseau WAN peut être réalisé à partir des trois technologies suivantes :

– PBT (*Provider Bridge Transport*) ;

– VPLS (*Virtual Private LAN Service*) ;

– L2TPv3 (*Layer 2 Tunnelling Protocol*).

La technologie PBT peut être considérée comme une extension de la fonction Q-VLAN réalisée dans le réseau LAN. Elle est généralement déployée dans le réseau d'agrégation par la mise en place du double marquage (*Q-in-Q*) des trames Ethernet.

La technologie PBT a défini également le cloisonnement des trames Ethernet dans le cœur de réseau par la mise en œuvre d'un double en-tête Ethernet (*MAC-in-MAC*). Cette fonction n'est pas déployée et n'est donc pas décrite dans le chapitre 8.

La technologie VPLS est une extension de la technologie MPLS. Elle est déployée dans le cœur de réseau, et présente l'avantage de partager les équipements P (*Provider*) avec le réseau MPLS-VPN.

La technologie VPLS peut être étendue au réseau d'agrégation avec la fonction H-VPLS (*Hierarchical*-VPLS).

La technologie L2TPv3 est une fonctionnalité mise en œuvre pour le transfert de trames Ethernet, uniquement en point à point, à travers un réseau de routeurs IP.

En résumé, la mise en œuvre du VPN Ethernet dans le réseau WAN est obtenue de différentes façons (figure 10) :

– au niveau du réseau d'accès, le cloisonnement est physique ou logique, en fonction du type de technologie utilisée. La connexion de deux utilisateurs au niveau du réseau d'accès est généralement interdite. Le trafic provenant des utilisateurs doit être transmis obligatoirement vers le réseau d'agrégation ;

– au niveau du réseau d'agrégation, le cloisonnement est réalisé en utilisant la fonction H-VPLS ou le double marquage Ethernet (Q-in-Q) ;

– au niveau du cœur de réseau, le cloisonnement est réalisé par la fonction VPLS ou MAC-in-MAC ou L2TPv3.

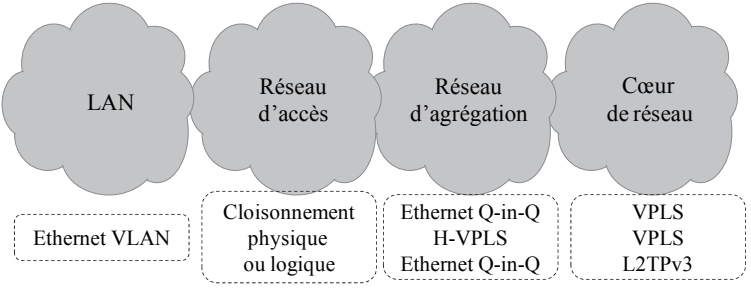

Figure 10. *Le VPN Ethernet*

Les pare-feux

Le chapitre 9 présente les fonctionnalités des pare-feux (*firewalls*). Ils assurent la surveillance des données transitant entre les réseaux LAN et WAN en contrôlant les champs des différents protocoles selon des règles établies.

Il existe plusieurs types de pare-feux qui se caractérisent par les fonctions suivantes :

– le filtre de paquets sans états effectue le filtrage de paquets (*packet filter*). Le contrôle s'applique sur les champs des en-têtes IP, TCP (*Transmission Control Protocol*), UDP (*User Datagram Protocol*) ou ICMP (*Internet Control Message Protocol*) ;

– le filtre de paquets avec état effectue le contrôle de la machine d'état TCP (*stateful inspection*). Le contrôle s'effectue sur les enchaînements des segments TCP ;

– le filtre applicatif effectue le filtrage des messages. Cette fonction est remplie par des passerelles applicatives ALG (*Application-Layer Gateway*) qui inspectent le contenu du message.

Les pare-feux sont déployés dans le réseau LAN, au niveau du bloc d'accès au réseau WAN. Ils sont intégrés dans la zone démilitarisée DMZ (*DeMilitarized Zone*).

Deux filtres de paquets encadrent la DMZ :

– un des filtres de paquets (*front-end firewall*) inspecte les paquets échangés entre le réseau WAN et la zone démilitarisée ;

– l'autre filtre de paquets (*back-end firewall*) inspecte les paquets échangés entre le réseau LAN et la zone démilitarisée.

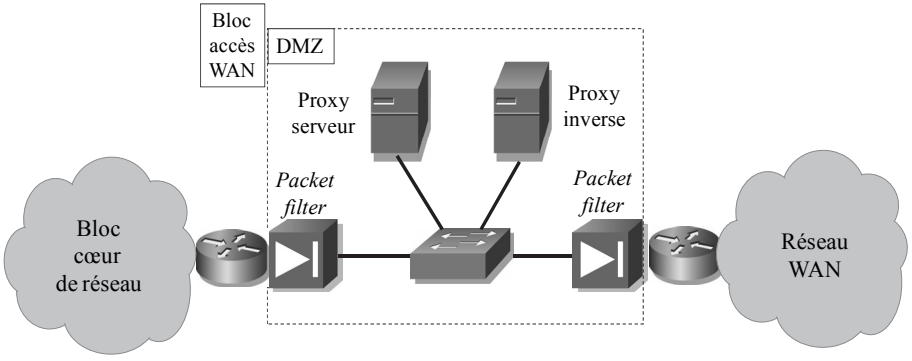

Figure 11. *La zone démilitarisée*

La zone démilitarisée héberge deux types de pare-feu applicatif : le serveur *proxy* et le serveur *proxy inverse*. Le serveur *proxy* (respectivement *proxy inverse*) effectue un contrôle du flux provenan du client (respectivement à destination du serveur) connecté au réseau LAN.

La traduction d'adresse NAT (*Network Address Translation*) ou d'adresse et de port NAPT (*Network Address and Port Translation*) est un type particulier de pare-feu. Cette fonction autorise uniquement le trafic initialisé par les hôtes du réseau LAN et bloque toute tentative de connexion provenant du réseau WAN.

Plusieurs configurations de NAPT définissent un filtrage plus ou moins sélectif : le cône ouvert, le cône restreint aux adresses, le cône restreint aux ports, le cône symétrique.

Le dispositif NAT / NAPT présente des difficultés pour certains flux devant le traverser, et pour lesquels des mécanismes particuliers sont définis :

– les applications ayant une identification spécifique comme le protocole ICMP (*Internet Control Message Protocol*) ;

– les protocoles protégeant la charge du paquet IP, comme par exemple le protocole ESP (*Encapsulated Security Payload*) du mécanisme de sécurité IPSec (*IP Security*) ;

– les applications transportant des adresses IP, comme par exemple les protocoles SIP (*Session Information Protocol*) et SDP (*Session Description Protocol*) ;

– les flux établis dynamiquement comme les protocoles FTP (*File Transfer Protocol*) ou RTP (*Real-time Transport Protocol*) ;

– les paquets IP fragmentés.

La détection d'intrusion

Le chapitre 10 présente les fonctionnalités des systèmes de détection d'intrusion IDS (*Intrusion Detection System*) et de prévention d'intrusion IPS (*Intrusion Prevention System*). Ces deux types de système sont regroupés sous le vocable IDPS (*Intrusion Detection Prevention System*).

Ces dispositifs assurent la surveillance des données transitant entre les réseaux LAN et WAN, ou à l'intérieur du réseau LAN, à partir d'une analyse des données permettant de détecter les attaques.

Les méthodes de détection d'intrusion sont mises en place à partir des techniques suivantes :

– la détection basée sur des signatures d'attaques connues dans les données circulant dans le réseau LAN ;

– la détection d'anomalies à partir d'une analyse d'activités suspectes dans le comportement d'un hôte ;

– l'analyse des protocoles afin de vérifier leur conformité aux normes.

Différents types de dispositif IDPS sont déployés dans le réseau selon la localisation ou la fonction remplie :

– N-IDPS (*Network-based* IDPS) : ce dispositif permet une surveillance des données sur les différents segments du réseau LAN (*Local Area Network*). Ce dispositif s'applique généralement sur les interfaces Ethernet ;

– WIDPS (*Wireless* IDPS) : ce dispositif permet une surveillance des données transitant par l'interface radioélectrique Wi-Fi. Il constitue un cas particulier du dispositif N-IDPS ;

– H-IDPS (*Home-based* IDPS) : ce dispositif présente des fonctionnalités semblables aux dispositifs précédents. Il permet une surveillance des données uniquement au niveau des hôtes du réseau ;

– NBA (*Network Behavior Analysis*) : ce dispositif permet d'effectuer spécifiquement une analyse du trafic afin de détecter une activité inhabituelle.