ÉCOLE DE TECHNOLOGIE SUPÉRIEURE
UNIVERSITÉ DU QUÉBEC

MÉMOIRE PRÉSENTÉ À
L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

COMME EXIGENCE PARTIELLE
À L'OBTENTION DE LA MAÎTRISE EN GÉNIE
AVEC CONCENTRATION EN RÉSEAUX DE TÉLÉCOMMUNICATIONS
M. Ing.

PAR
LAURENT CHARBONNIER

ÉVALUATION DE LA SÉCURITÉ DES RÉSEAUX PRIVÉS VIRTUELS SUR MPLS

MONTRÉAL, LE 10 DÉCEMBRE 2007

CE MÉMOIRE A ÉTÉ ÉVALUÉ

PAR UN JURY COMPOSÉ DE :

M. Michel Lavoie, directeur de mémoire
Département de génie logiciel à l'École de technologie supérieure

Mme Maria Bennani, codirecteur de mémoire
Département de génie logiciel à l'École de technologie supérieure

M. Michel Kadoch, président du jury
Département de génie électrique à l'École de technologie supérieure

M. Jean Marc Robert, membre du jury
Département de génie logiciel à l'École de technologie supérieure

IL A FAIT L'OBJET D'UNE SOUTENANCE DEVANT JURY ET PUBLIC

LE 5 NOVEMBRE 2007

À L'ÉCOLE DE TECHNOLOGIE SUPÉRIEURE

REMERCIEMENTS

Je souhaite remercier en premier lieu mon directeur de recherche, Michel Lavoie, pour m'avoir accompagné tout au long de ce projet de recherche et avoir suscité chez moi un intérêt toujours grandissant pour le domaine de la sécurité informatique. Son aide clairvoyante et ses réponses rapides, enthousiastes et détaillées m'ont permis d'avancer lorsque des difficultés étaient présentes.

Pour leur collaboration sans laquelle ce projet n'aurait pu être possible, mes remerciements s'adressent également à Bell Canada. Leur réseau MPLS m'a permis de vérifier mes suppositions théoriques et de réaliser des expérimentations techniques constructives. Merci également à Maria Bennani pour m'avoir proposé ce projet, pour son temps et sa disponibilité.

Je tiens à exprimer ma gratitude à Jean Marc Robert pour son expertise scientifique avancée et son concours sur la vérification de légitimité de problèmes potentiels dans l'architecture MPLS/VPN. Ma reconnaissance va en outre à Michel Kadoch qui a engendré mon intérêt actuel pour la voix sur IP et m'a permis de transmettre ce qu'il m'a appris dans le domaine des télécommunications à des étudiants de l'ETS depuis plusieurs sessions.

Je ne pourrais conclure ces remerciements sans avoir une pensée pour ma famille et mes amis qui m'ont toujours soutenu et donné la force de mener à bien cette maitrise. Un grand merci à toi, Andrée, pour ton appui permanent, tes conseils et tes encouragements. Enfin, je vous remercie, Olivier, Rémi et Guillaume pour avoir été plus que de simples collègues de travail, Zizou pour ton geste libérateur.

ÉVALUATION DE LA SÉCURITÉ DES RÉSEAUX PRIVÉS VIRTUELS SUR MPLS

LAURENT CHARBONNIER

RÉSUMÉ

Les besoins actuels en termes de transmission sécurisée de l'information sont colossaux. Si les lignes louées représentaient dans le passé la méthode la plus communément employée pour relier deux sites distants, les réseaux privés virtuels prennent de plus en plus le pas sur ces lignes louées, essentiellement grâce à leur coût beaucoup plus faible. Néanmoins, les VPN de niveau 2 sont complexes à mettre en œuvre et difficiles à mettre à l'échelle. Récemment sont apparus les VPN sur MPLS, offrant de meilleures performances et ne nécessitant pas de chiffrement des données.

Le concept des VPN sur MPLS repose sur l'utilisation de tables de routage et de contextes séparés dans les routeurs de bordure pour chaque VPN. Les paquets sont acheminés dans le réseau MPLS en ajoutant une étiquette supplémentaire permettant de définir leur appartenance à un VPN. Le réseau MPLS est transparent pour les clients des VPN, toutefois ceux-ci doivent faire confiance au fournisseur de service.

Étant de plus en plus déployés, il est nécessaire de vérifier que les VPN sur MPLS sont effectivement sécuritaires et ne permettent pas à des attaquants de s'introduire dans le réseau MPLS ou dans les VPN. Ces derniers doivent être étanches, ne permettant pas de divulguer ou modifier l'information.

La recherche préliminaire des différents modes d'attaques sur un réseau nous permet de confronter la technologie MPLS/VPN à des menaces variées, puis de tester des architectures particulières utilisant cette technologie. Des expérimentations ont été menées sur un réseau MPLS de Bell Canada pour montrer que certaines conditions peuvent compromettre la sécurité des VPN sur MPLS. Le protocole BGP, utilisé sous sa variante MP-BGP pour effectuer la signalisation des VPN dans le réseau MPLS fait l'objet d'une étude approfondie. Nos résultats montrent que l'architecture MPLS/VPN est sécuritaire à la condition qu'aucune erreur de configuration ne soit présente. Finalement, des conseils et recommandations sont présentés afin d'esquiver toute tentative d'attaque.

ÉVALUATION DE LA SÉCURITÉ DES RÉSEAUX PRIVÉS VIRTUELS SUR MPLS

LAURENT CHARBONNIER

ABSTRACT

The actual needs in terms of secure data communication are tremendous. In the past, the use of leased lines was the most widespread method to link two distant sites. Today, virtual private networks are stealing the show with their much lower costs. However, layer 2 VPN are difficult to implement and they suffer poor scalability. Nevertheless, VPN using MPLS have recently appeared on the market, offering higher performance without needing data encryption.

The concept of MPLS VPN relies on separate contexts and routing tables on border routers for each VPN. Packets are forwarded in the core network using an extra label defining a VPN membership. Each customer is unaware of the MPLS cloud because of the address space separation. However, high levels of trust toward the service provider are essential.

Considering its ever-growing popularity, it is crucial to make sure that the MPLS VPN technology is indeed secure and would never allow intrusions in the core network or in the VPNs. Likewise, the previously mentioned should provide users with isolation and security, protecting information against eavesdropping or modification.

Preliminary researches on numerous network attack techniques allows us to evaluate the response of MPLS VPN to various threats and then to test particular architectures using that technology. Experimental testing has been performed on a Bell Canada network in order to demonstrate that specific conditions can put the security of MPLS VPNs at risk. MP-BGP, a variant of BGP protocol, used to propagate VPN routing information is extensively analyzed. Our results show that the MPLS VPN architecture is secure, given that no configuration mistake has been made. Finally, advices and recommendations will be suggested in order to dodge any attack attempt.

TABLE DES MATIÈRES

Page

LISTE DES TABLEAUX

Page

LISTE DES FIGURES

Page

LISTE DES ABRÉVIATIONS, SIGLES ET ACRONYMES

AES	Advanced Encryption Standard
AH	Authentication Header
AS	Autonomous System
ASBR	Autonomous System Border Router
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CDP	Cisco Discovery Protocol
CE	Customer Edge (router)
CERT	Computer Emergency Response Team
CGI	Common Gateway Interface
CIDR	Classless Inter-Domain Routing
CR-LDP	Constraint Routing – Label Distribution Protocol
CSRF	Cross-Site Request Forgery
CTCPEC	Canadian Trusted Computer Product Evaluation Criteria
DES	Data Encryption Standard
DLCI	Data Link Connection Identifier
DNS	Domain Name Server
DoS	Deny of Service
DS	Differentiated Services
DSCP	Differentiated Services Code Point
eBGP	exterior Border Gateway Protocol

EIGRP	Enhanced Interior Gateway Routing Protocol
ESP	Encapsulating Security Payload
FEC	Forwarding Equivalence Class
FLIX	Florida Internet Exchange
FR	Frame Relay
FTP	File Transfer Protocol
GRE	Generic Routing Encapsulation
HTTP	Hypertext Transfer Protocol
IANA	Internet Assigned Number Authority
ICANN	Internet Corporation of Assigned Numbers and Names
IBC	Identity Based Cryptography
iBGP	interior Border Gateway Protocol
IETF	Internet Engineering Task Force
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IGP	Interior Gateway Protocol
IKE	Internet Key Exchange
IP	Internet Protocol
IPsec	Internet Protocol security
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
IPX	Internetwork Packet Exchange

IRR	Internet Routing Registry
IRV	Inter-Domain Routing Validator
ITSEC	Information Technology Security Evaluation Criteria
L2TP	Layer 2 Tunneling Protocol
L2TPv3	Layer 2 Tunneling Protocol version 3
LAN	Local Area Network
LDP	Label Distribution Protocol
LER	Label Edge Router
LSP	Label Switch Path
LSR	Label Switch Router
MAC	Medium Access Control
MD5	Message Digest 5
MP-BGP	Multi Protocol Border Gateway Protocol
MPLS	Multi Protocol Label Switching
NAT	Network Address Translation
NOC	Network Operations Center
OSI	Open Systems Interconnection
OSPF	Open Shortest Path First
P	Provider (router)
PE	Provider Edge (router)
PGBGP	Pretty Good Border Gateway Protocol
PHP	Penultimate Hop Popping

PKI	Public Key Infrastructure
P2P	Peer to Peer
PPTP	Point to Point Tunneling Protocol
psBGP	pretty secure Border Gateway Protocol
PWE	Pseudo Wire Emulation
RC4	Rivest Cipher 4
RD	Route Distinguisher
RFC	Request For Comments
RIP	Routing Information Protocol
RIR	Regional Internet Registry
RR	Route Reflector
RSA	Rivest, Shamir, Adleman
RSVP	Resource Reservation Protocol
RT	Route Target
S-BGP	Secure Border Gateway Protocol
SHA	Secure Hash Algorithm
soBGP	secure origin Border Gateway Protocol
SOO	Site Of Origin
SPV	Secure Path Vector
SSH	Secure Shell
SSID	Service Set IDentifier
SSL	Secure Socket Layer

TCP	Transmission Control Protocol
TCSEC	Trusted Computer System Evaluation Criteria
TE	Traffic Engineering
TLS	Transport Layer Security
ToS	Type of Service
TTL	Time to Live
VCI	Virtual Circuit Identifier
VLAN	Virtual Local Area Network
VPI	Virtual Path Identifier
VPLS	Virtual Private LAN Service
VPN	Virtual Private Network
VPWS	Virtual Private Wire Service
VRF	VPN Routing and Forwarding
WEP	Wireless Equivalent Privacy
WPA	Wi-Fi Protected Access
XSS	Cross-Site Scripting

INTRODUCTION

L'avènement d'un accès rapide à Internet pour tous et partout a simplifié l'accès aux services et aux connaissances, ce qui constitue un réel progrès dans notre façon de vivre. Hélas, les procédures d'attaques, qu'elles visent une entité particulière ou Internet tout entier, s'en sont également trouvées facilitées. De nos jours, un virus ou un déni de service de portée planétaire peuvent être lancés dans l'anonymat le plus complet en sirotant un chai latté sur la terrasse du *Starbucks* du coin grâce au réseau sans-fil mis gratuitement à la disposition des clients.

Ce contexte de la croissance exponentielle d'Internet implique la nécessité de créer des réseaux toujours plus démesurés, toujours plus rapides, toujours plus sécuritaires. Comme la complexité des réseaux se fait grandissante, la gestion et le dimensionnement des réseaux deviennent primordiaux.

Le plus gros défi des concepteurs n'est peut-être plus de concevoir des technologies fonctionnelles – les outils de développement étant de plus en plus évolués – mais de créer des technologies sans faille de sécurité.

MPLS (*Multi Protocol Label Switching*) est une technologie de réseau permettant de nouvelles applications comme l'ingénierie de trafic et les réseaux privés virtuels. Ces derniers, les VPN sur MPLS, permettent de relier plusieurs sites géographiquement distants d'une manière totalement transparente pour les clients, tout en garantissant la confidentialité et l'intégrité des données sans que celles-ci ne soient chiffrées durant leur transport.

La perspective d'une technologie ne nécessitant aucun chiffrement est très intéressante, ce dernier créant toujours une perte de performance incompatible avec les applications temps réel et nécessitant une architecture de gestion des clés pointue. Cependant, la

caractéristique première d'un réseau privé demeure d'assurer le maintien du secret des informations transportées. Ce mémoire tentera de démontrer que MPLS a su relever ce défi.

Tout d'abord, nous présentons divers aspects de MPLS, son fonctionnement, ses applications, la gestion de la sécurité et la mise en œuvre des VPN sur MPLS. La garantie de l'étanchéité des réseaux privés virtuels constitue la problématique et est discutée à la fin de ce premier chapitre.

Après avoir dressé une liste quasi-exhaustive des différents types d'attaques possibles sur un réseau MPLS, le second chapitre fait l'analyse complète de la sécurité de MPLS/VPN. En premier lieu, nous décrivons les attaques directes ou indirectes qui pourraient permettre de briser l'étanchéité des VPN et analysons en corrélation le point de vue d'autres chercheurs à ce sujet. Une comparaison avec ATM (*Asynchronous Transfer Mode*) et Frame Relay, technologies réputées sécuritaires utilisant un principe similaire au niveau 2 est ensuite effectuée, avant d'étudier plus spécifiquement certaines architectures MPLS/VPN avancées.

Le troisième chapitre détaille quelques connectivités élaborées de réseaux MPLS puis présente la réalisation de tests pratiques permettant de vérifier la sécurité d'une de ces connectivités sur un réseau MPLS de Bell Canada. À la lumière de ces tests, une étude de la sécurité du protocole BGP est effectuée dans le quatrième chapitre.

Enfin, le cinquième chapitre suggère une marche à suivre visant la garantie d'un fonctionnement sécuritaire de MPLS/VPN. Pour y parvenir, nous parcourons chaque étape de création d'un VPN en considérant les failles possibles des protocoles utilisés.

CHAPITRE 1

ÉTAT DE L'ART

Ce chapitre présente la technologie MPLS, son fonctionnement et ses applications et se concentre particulièrement sur la sécurité des VPN sur MPLS. La vérification de l'étanchéité des VPN est l'objet de la problématique.

1.1 La technologie MPLS

MPLS est une technologie de réseau qui applique certains aspects des technologies à commutation de circuits telles qu'ATM ou Frame Relay à un réseau à commutation de paquets. MPLS vient s'intercaler entre la couche 2 et la couche 3 du modèle OSI (*Open Systems Interconnection*), il y est d'ailleurs souvent fait référence comme appartenant à la couche 2.5.

MPLS ajoute un entête situé entre l'entête de la couche réseau et l'entête de la couche liaison de données. Cet entête porte le nom d'entête *shim*. Comme l'indique son abréviation, MPLS supporte n'importe quel protocole de couche réseau (Rosen, 2001). En général, le protocole de la couche réseau est IPv4, bien qu'IPv6 (*Internet Protocol version 6*), IPX (*Internetwork Packet Exchange*), AppleTalk, etc. soient aussi supportés.

Le principe de MPLS a été suggéré en 1996 par *Ipsilon Networks* en tant que technologie d'*IP switching* fonctionnant sur ATM, et par Cisco sous le nom de *Tag switching*. Le nom a été changé pour *Label switching* lorsque l'IETF a créé le groupe de travail sur MPLS pour standardiser MPLS en 1997.

1.1.1 Fonctionnement de MPLS

MPLS réalise une commutation d'étiquette en lieu et place du routage IP traditionnel. Dans un environnement classique IP, chaque routeur réalise sa décision d'acheminement en fonction de l'adresse IP située dans l'entête réseau du paquet et du contenu de sa table de routage. Dans un environnement MPLS, chaque routeur possède une table de commutation des étiquettes. En fonction de la valeur de l'étiquette située dans l'entête MPLS et de l'interface d'entrée du paquet, le routeur cherchera dans cette table l'étiquette à utiliser en sortie ainsi que l'interface de sortie. Une fois entré dans le réseau MPLS, l'entête réseau d'un paquet ne sera plus jamais consultée jusqu'à sa sortie de ce réseau. Seules les étiquettes affectent l'acheminement des paquets.

L'avantage de cette technique de commutation d'étiquette est qu'elle n'impose pas de décomposer le paquet reçu jusqu'à l'entête réseau afin de pouvoir effectuer la décision d'acheminement, se rapprochant ainsi des technologies de niveau 2. De plus, la notion de chemin est transparente pour les routeurs du réseau, appelés LSR (*Label Switching Router*), qui n'ont donc aucune connaissance nécessaire des réseaux interconnectés au nuage MPLS (représenté par le cœur du réseau). Le tableau ci-dessous présente un exemple de table de commutation d'étiquette.

Tableau 1.1

Exemple de table de commutation d'étiquette sur un routeur MPLS

Interface IN	Label IN	Interface OUT	Label OUT
0	15	1	24
0	41	2	39
2	6	1	24

En plus des routeurs LSR, qui se chargent d'effectuer la commutation d'étiquette au cœur du réseau MPLS, il existe des routeurs de bordure, appelés LER (*Label Edge Router*), qui sont les points d'entrée et de sortie du réseau MPLS. Leur rôle est d'assigner l'étiquette au paquet entrant dans le réseau, et de l'ôter au paquet sortant du réseau.

L'itinéraire emprunté par un paquet dans le réseau MPLS suit un chemin appelé LSP (*Label Switch Path*). Ces chemins, reliant entre eux les routeurs LER, peuvent être configurés manuellement par le gestionnaire du réseau ou automatiquement par les LER. Ces derniers s'appuient pour cela sur des protocoles de distribution d'étiquettes tels que LDP (*Label Distribution Protocol*, *cf.* RFC3036 (Anderson et al., 2001)) ou RSVP-TE (*Resource Reservation Protocol*, *cf.* RFC3209 (Awduche et al., 2001)). Ce dernier est utilisé pour l'ingénierie de trafic, une des applications des réseaux MPLS.

Les étiquettes peuvent être distribuées de plusieurs façons : tout d'abord de façon descendante (*downstream*) ou montante (*upstream*), selon le sens de propagation de l'information, puis soit à la demande, soit automatiquement (*unsolicited*). Le tout étant soit ordonné, soit indépendant (sans ordre).

Le routage classique, utilisant un IGP (*Interior Gateway Protocol*) comme OSPF (*Open Shortest Path First*), est nécessaire afin de permettre aux routeurs du nuage MPLS de communiquer entre eux. Il n'est par contre pas utilisé pour indiquer les réseaux joignables en dehors du nuage MPLS ou pour router les paquets de données dans le nuage.

Les classes d'équivalences ou FEC (*Forwarding Equivalence Class*) permettent de classifier les paquets à leur entrée dans le réseau MPLS. Tous les paquets faisant partie de la même FEC suivront le même chemin dans le réseau et donc utiliseront les mêmes étiquettes. La classification est effectuée par rapport soit au réseau de destination, soit à

la classe de service, soit suivant des paramètres d'ingénierie de trafic. Elle se base sur le contenu de l'entête réseau, par exemple l'adresse IP de destination ou le champ ToS (*Type of Service*).

Les chemins LSP n'ont pas d'existence concrète, mais sont la somme des correspondances étiquette d'entrée/étiquette de sortie entre un routeur d'entrée dans le réseau MPLS, appelé LER *Ingress* et un routeur de sortie du réseau MPLS, appelé LER *Egress*.

Lors du fonctionnement normal du réseau MPLS, le routeur LER *Ingress* ajoute l'entête MPLS en appliquant l'étiquette correspondant au chemin à suivre puis l'envoie sur le LSP. Chaque routeur LSR traversé va lire l'étiquette située dans l'entête , chercher l'étiquette de sortie dans sa table de correspondance, changer la valeur de l'étiquette dans l'entête pour celle trouvée dans la table et enfin réaliser la commutation du paquet.
Le routeur LER *Egress* enleve l'entête MPLS et envoye le paquet sur l'interface correspondant au réseau de destination, en fonction à nouveau de l'adresse IP.

Il faut noter qu'il existe une fonctionnalité, le *penultimate hop popping* (PHP), permettant de réduire la charge sur les routeurs LER *Egress*. Elle consiste à enlever l'entête MPLS non pas au routeur LER mais au dernier routeur LSR traversé. Ainsi le LER *Egress* réalisera simplement le routage du paquet lorsqu'il le recevra, puisque celui-ci ne comportera pas d'entête MPLS.

L'entête ajouté par MPLS, présenté ci-dessous, contient plusieurs champs :

- l'étiquette MPLS, d'une longueur de 20 bits, utilisée pour la commutation,
- le champ *experimental* sur trois bits, qui peut être utilisé pour indiquer la qualité de service du paquet, en association avec le champ ToS/DiffServ de l'entête IP,
- le bit S, définissant s'il vaut « 1 » qu'il s'agit du dernier entête MPLS,
- le TTL (Time to Live) sur huit bits qui permet d'éviter les boucles infinies.

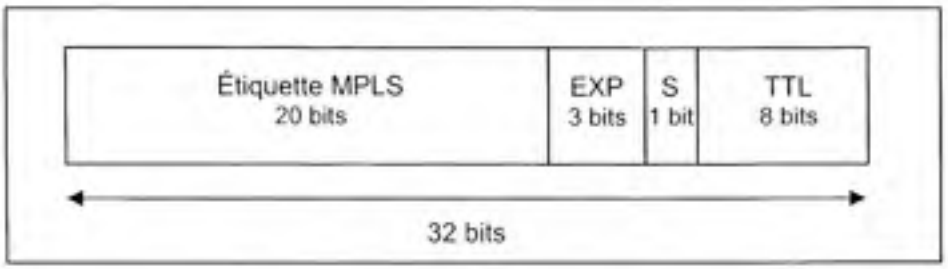

Figure 1.1 ***Contenu de l'entête MPLS.***

La longueur totale de l'entête est de 32 bits soit 4 octets. La surcharge causée par l'ajout de cet entête est donc restreinte par rapport aux entêtes existants (Ethernet = 16 octets, IP = 20 octets, TCP = 20 octets, etc.), ce qui permet de limiter la perte d'efficacité du réseau, exprimée en fonction du rapport entre les données utiles de la couche application et les données effectivement transmises sur le réseau, avec les entêtes.

Le champ *experimental* est parfois nommé « Classe de service ». À l'origine sans fonction attitrée, il peut servir pour faire le lien entre la qualité de service indiquée au niveau de l'entête IP par le champ ToS ou DS (*Differentiated Services*) de l'entête IP. Cela permet de classer les paquets arrivant dans les LSR dans différentes queues traitées selon leur qualité de service associée. Les trois bits du champ *experimental* peuvent être associés facilement aux bits de précédence du champ ToS. Par contre un problème se pose s'ils doivent être associés aux codes DSCP (*Differentiated Services Code Point*) utilisés par les services différenciés (ou *DiffServ*) qui utilisent six bits (il en est ainsi car l'entête MPLS a été conçu avant les codes DSCP). Le manque de place peut néanmoins être compensé en affectant des étiquettes MPLS différentes selon la qualité de service, le routeur LSR faisant alors la distinction de traitement entre les paquets en fonction de la valeur de l'étiquette MPLS. Plus d'information sur ce point peut être obtenue en lisant la RFC3270 (Le Faucheur et al., 2002).

En plus de permettre un acheminement plus rapide des paquets, un autre des avantages de la technologie MPLS est la possibilité d'empiler les étiquettes, technique connue sous le nom de *label stacking*. Cela rend possible – entre autres – des applications telles que l'ingénierie de trafic, les réseaux privés virtuels ou VPN sur MPLS, ou encore le transport sur des réseaux MPLS hiérarchisés (*cf.* partie 2.2.5.2).

De la même façon qu'IPv6 utilise un champ « *next header* » pour gérer les options en indiquant la nature de l'entête suivant, le bit S de l'entête MPLS permet d'indiquer si l'étiquette concernée est la dernière de l'empilement (si S=1) ou non (si S=0).

Enfin, le champ TTL a les mêmes fonctionnalités que son pendant de l'entête IP, avec pour objectif d'éviter que le paquet ne rentre dans une boucle infinie. Le LER *Ingress* va recopier la valeur du champ TTL de l'entête IP dans celui de l'entête MPLS. Chaque routeur LSR traversé par le paquet va décrémenter sa valeur. Arrivé au LER *Egress*, il sera recopié à la place du champ équivalent de l'entête IP. Il est à noter qu'un paramètre de configuration permet de rendre transparents tous les routeurs du réseau MPLS et donc le nuage MPLS en ne recopiant pas la valeur du champ TTL de l'entête MPLS dans l'entête IP.

Pour plus d'information sur l'architecture MPLS, le lecteur peut consulter la RFC3031 (Rosen, 2001). De son côté, la RFC3032 (Rosen et al., 2001) présente la technique d'encodage de l'étiquette MPLS par les routeurs LSR, les règles et procédures pour traiter les différents champs de l'étiquette ainsi que certaines considérations telles que la limitation de taille des paquets par la couche de niveau 2 utilisée.

1.1.2 Buts de MPLS

1.1.2.1 Buts initiaux

Le but initial de MPLS était d'améliorer les performances de routage des grands réseaux en apportant la vitesse de commutation de la couche 2 à la couche 3. Cela a été rendu possible en suivant le principe développé lors de technologies précédentes comme ATM ou FR : les circuits ou chemins virtuels. Au lieu de devoir consulter à chaque routeur traversé la table de routage afin de déterminer l'interface de sortie, MPLS permet de ne consulter qu'une table de commutation d'étiquettes, indiquant selon l'étiquette inclue dans l'entête *shim* l'interface de sortie ainsi que l'étiquette à placer dans ce même entête (de la même façon que les VPI (*Virtual Path Identifier*) et VCI (*Virtual Circuit Identifier*) inclus dans l'entête des cellules ATM ou les DLCI (*Data Link Connection Identifier*) de l'entête FR).

Cependant, avec l'amélioration des performances des routeurs modernes, la différence de performances entre un routage IP et une commutation par MPLS est devenue négligeable.

Un autre but de MPLS était de simplifier le transport d'IP sur ATM, complexe à cause des protocoles de signalisation d'ATM. Cette simplification a été apportée par les étiquettes remplaçant les VPI/VCI d'ATM, par un protocole de distribution des étiquettes spécifique à MPLS : LDP et par des protocoles de routage du monde IP, tels que BGP (*Border Gateway Protocol*) et OSPF.

1.1.2.2 Nouveaux buts et applications

L'intérêt de MPLS ne réside pas dans son utilisation isolée. Des applications comme l'ingénierie de trafic ainsi que les réseaux privés virtuels sur MPLS ont été développées pour permettre de nouvelles potentialités.

Tel qu'énoncé précédemment, MPLS n'apporte pas lui-même de gain notable en termes de performances. De plus, cette technologie ne permet pas à elle seule d'empêcher la congestion, surtout si le trafic dans le réseau n'est pas stable mais évolutif. Néanmoins, en étant utilisée en association à l'ingénierie de trafic, elle permet un accroissement très appréciable de performances.

1.1.2.3 L'ingénierie de trafic

L'ingénierie de trafic permet l'utilisation optimale des ressources du réseau, contrairement au routage IP qui privilégie le chemin le plus court, en termes de nombre de sauts (RIP, *Routing Information Protocol*) ou d'états de liens (OSPF par exemple). Elle offre la possibilité d'utiliser différents chemins pour relier un nœud source et un nœud destination afin de répartir la charge sur le réseau et ainsi améliorer l'efficacité de ce dernier. Pour y parvenir, un routage explicite est utilisé, c'est-à-dire que des contraintes telles que la bande passante nécessaire pour le trafic, sont prises en compte lors de la création des LSP. Le protocole CR-LDP (*Constraint Routing-LDP*) permet de créer de tels LSP. D'autres protocoles comme RSVP-TE (*RSVP-Traffic Engineering*) et OSPF-TE (*OSPF-Traffic Engineering*) sont aussi utilisés pour gérer efficacement le réseau MPLS et réserver des chemins non congestionnés de manière dynamique, s'adaptant en temps réel à la charge sur le réseau et pas uniquement sur des réglages préétablis.

Une des possibilités permises par l'ingénierie de trafic, en l'occurrence par le protocole RSVP-TE, est la réservation d'une bande passante garantie sur le réseau. Il est ainsi possible d'offrir une qualité de service de haut niveau à des applications temps réel comme la voix sur IP, la vidéoconférence, etc.

Afin de ne pas surcharger le réseau avec les données de contrôle, MPLS permet l'agrégation de flux de trafic. Cela signifie que pour plusieurs flux de trafic entrants par différents LSP, il est possible d'utiliser un seul LSP en sortie et ainsi réduire la quantité d'informations sur les chemins créés ainsi que le nombre de connexions à gérer par les routeurs LSR du réseau MPLS.

Des extensions à l'ingénierie de trafic existent, comme le « reroutage » rapide (*Fast Reroute*) qui est un mécanisme de protection locale de MPLS-TE. Pour chaque LSP primaire créé il existe un LSP secondaire dit « de secours » qui sera activé dès la détection d'une panne sur le LSP primaire. Le but de ce mécanisme de protection est de limiter le temps de panne du chemin concerné à une valeur inférieure à 100ms, permettant aux applications temps réel de ne pas souffrir de la panne.

Il existe d'autres solutions permettant d'empêcher la congestion, telle que l'ingénierie de réseau. Si l'ingénierie de trafic place le trafic là où le réseau n'est pas congestionné, l'ingénierie de réseau augmente quant à elle la capacité des liens fortement achalandés. Il est aisé de comprendre que l'ingénierie de trafic est de loin la plus avantageuse, surtout si le trafic dans le réseau est dynamique.

1.1.2.4 Les réseaux privés virtuels sur MPLS (MPLS/VPN)

Avec l'ingénierie de trafic, l'autre grande application de MPLS est la possibilité de créer des réseaux privés virtuels (appelés par la suite VPN : *Virtual Private Network*) utilisant MPLS comme mode de transport. L'avantage découlant de l'utilisation de MPLS est la possibilité de ne pas avoir à chiffrer les données lors de leur transport tout en garantissant leur confidentialité. C'est le but primordial d'un VPN.

Pour permettre cela, MPLS utilise la notion de routeurs virtuels garantissant, au sein d'un même routeur physique, la création de différents contextes de routage, chaque VPN

possédant son propre contexte. Ainsi, deux sites géographiquement séparés peuvent être liés et demeurer privés sans pour autant nécessiter l'utilisation de protocoles de chiffrement comme IPsec (*Internet Protocol security*) ou de technologies de VPN classiques, par exemple L2TP (*Layer 2 Tunneling Protocol*).

Les technologies de VPN « classiques », c'est-à-dire de niveau 2, sont réputées et fréquemment utilisées pour permettre le transport de données de façon sécuritaire sur un médium qui ne l'est pas. Un des usages possibles est d'offrir un accès à distance sécurisé d'un poste client au réseau de l'entreprise par exemple. Le niveau de sécurité de ces technologies VPN n'est pas remis en cause, cependant elles sont caractérisées par une certaine lourdeur et une complexité d'utilisation liées au chiffrement des données et à l'interconnexion des passerelles VPN point à point.

MPLS/VPN est une solution plus simple, légère, transparente à l'utilisateur final, la configuration étant effectuée par le fournisseur de service au niveau des routeurs de bordure du réseau MPLS et non sur les ordinateurs des clients. En conséquence, un utilisateur mobile devra employer un VPN classique, MPLS/VPN étant valide pour des réseaux connectés directement à un nuage MPLS. Cette nouvelle technologie trouve donc son application dans la connexion de sites de VPN ne se déplaçant pas géographiquement.

1.2 La sécurité dans MPLS

1.2.1 Généralités

Le succès d'une technologie utilisée à grande échelle ne dépend pas uniquement de son bon fonctionnement, il faut aussi en garantir la sécurité. S'il est possible à une personne malintentionnée de corrompre ou d'en interrompre sa marche normale, qui voudrait alors l'utiliser? Étant donné que des enjeux financiers sont la plupart du temps

impliqués, qu'il s'agisse de l'investissement pour adopter une nouvelle technologie ou des revenus qui découleront de son utilisation, tout risque est à éviter.

Comme mentionné précédemment, le but initial de MPLS était d'améliorer les performances des réseaux. La notion de réseaux privés virtuels utilisant MPLS est venue plus tard. Néanmoins, la conception de cette technologie a permis d'y intégrer la sécurité assez simplement.

Par hypothèse, la sécurité de MPLS repose sur l'intégrité des tables d'étiquettes. Aussi, le principe fondamental de MPLS/VPN s'établit sur la notion de routeurs virtuels. Au sein d'un seul routeur, MPLS/VPN permet de gérer plusieurs contextes, ce qui équivaut à avoir autant de routeurs physiquement séparés. Si à chaque contexte est associé un VPN, le réseau MPLS/VPN devient similaire – au niveau logique – à des lignes dédiées pour chaque VPN en ce qui a trait à la sécurité. Voir la Figure 1.2 pour le principe.

Enfin, il est primordial de faire l'hypothèse que le réseau MPLS est un réseau privé. Nul ne doit pouvoir s'introduire à l'intérieur du réseau, car les données y sont transférées sans être chiffrées. Permettre l'accès aux données par quiconque supprimerait la notion de réseau privé virtuel.

L'empilement des entêtes MPLS permet de maintenir cette sécurité entre les routeurs du réseau MPLS/VPN. L'étiquette « extérieure », c'est-à-dire la première rencontrée lors de la désencapsulation du paquet (représentée en blanc sur la Figure 1.3), conserve son rôle d'étiquette de LSP et permet la commutation entre le LER *Ingress* et le LER *Egress*. L'étiquette « intérieure » indique l'instance de routage et d'acheminement (VRF : *VPN Routing and Forwarding*), autrement dit le contexte de VPN concerné. Elle représente pour chaque VRF le tunnel mis en place entre les routeurs de bordure.

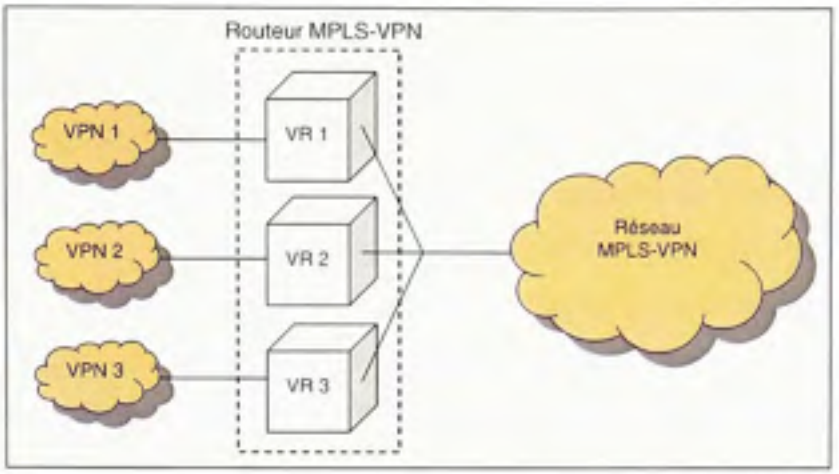

Figure 1.2 ***Schéma simplifié d'un routeur MPLS/VPN avec trois routeurs virtuels***

Les routeurs de bordure du réseau MPLS/VPN sont appelés PE pour *Provider Edge*. Il n'y a, sauf exception (*cf.* partie 2.2.5), qu'entre les routeurs PE que sont utilisées les étiquettes LSP et VPN. Les routeurs situés chez les clients et liés aux PE sont appelés CE pour *Customer Edge*.

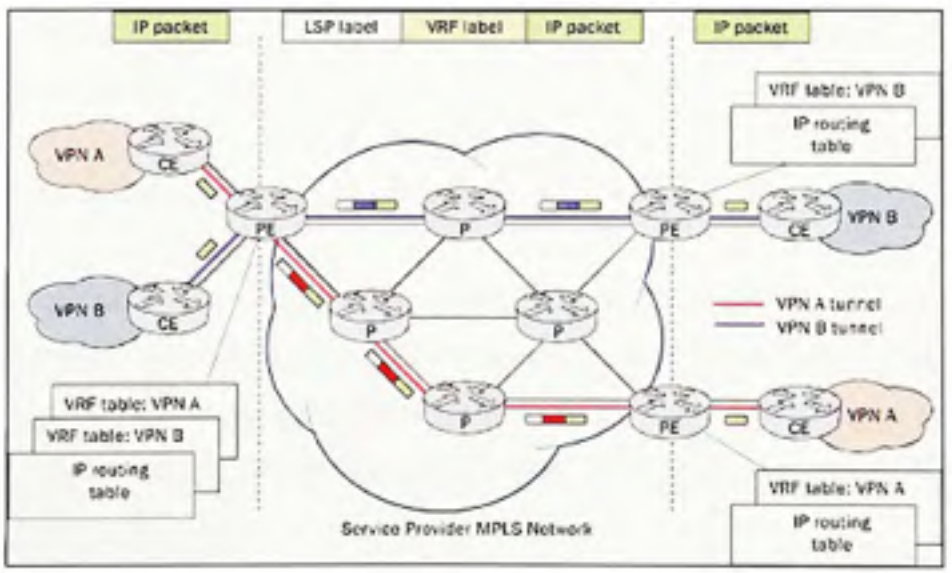

Figure 1.3 ***Principe de l'empilement d'étiquettes MPLS***
(Tiré de Ixia, 2004)

Les paquets provenant des réseaux privés des clients sont sans étiquette, les routeurs PE classent ces paquets en fonction de leur origine dans les différents contextes qu'ils gèrent, leur assignent ensuite selon leur contexte une étiquette de VPN spécifique, puis selon le chemin emprunté une étiquette de LSP. Durant leur trajet sur le réseau MPLS, seule l'étiquette de LSP sera lue et modifiée par les LSR, appelés routeurs P pour *Provider*. L'étiquette de VPN demeurera intacte jusqu'au PE *Egress*, où le paquet sera envoyé sur l'interface de sortie en fonction de son étiquette de VPN, qui lui aura préalablement été ôtée.

Les différents contextes d'un PE possèdent chacun leur table de VRF, autrement dit la liste des réseaux accessibles depuis leur VPN uniquement, afin de maintenir la notion de réseau privé. Il est possible de voir un exemple du principe de fonctionnement sur la Figure 1.3.

En ce qui concerne les données circulant dans chaque VPN, elles ne sont pas chiffrées. Cela leur permet de ne pas subir la baisse de performances qu'impose le chiffrement des données, comme dans un VPN classique par exemple. Pour des applications temps réel, c'est un point crucial.

1.2.2 Différents aspects à considérer

Lorsque l'on évalue la sécurité d'un système, il est essentiel de considérer trois différents aspects qui sont l'architecture du système, l'implémentation de l'architecture et le fonctionnement du système (Behringer et Morrow, 2005). Néanmoins, c'est surtout le premier de ces aspects, l'architecture du système, qui nous intéresse vraiment dans ce mémoire.

L'architecture du système est donnée par la spécification formelle, dans le cas de MPLS/VPN il s'agit de la RFC4364 : « BGP/MPLS IP Virtual Private Networks (VPNs) » (Rosen et Rekhter, 2006).

L'implémentation de l'architecture correspond à la façon dont les spécifications de cette dernière sont réellement intégrées. Certains choix d'implémentation peuvent remettre en cause la sécurité de tout le système, ou plus simplement donner lieu à des erreurs et oublis de programmation, créant de possibles portes dérobées (*backdoors*).

Le fonctionnement du système dépend quant à lui du gestionnaire du réseau, comment il gère et maintient son système, sachant que le problème le plus fréquemment rencontré est le non-changement des mots de passe par défaut des routeurs. Bien trop de gestionnaires de réseaux ne changent pas les mots de passe par défaut (tels que « *admin* », « *cisco* », etc.) ou utilisent des mots de passe trop simples ou évidents à deviner (Wayne et Edward, 2004). Ce simple oubli peut mettre en péril la sécurité de tout le réseau MPLS. Le maillon le plus faible reste donc bien l'être humain.

Les mots de passe ne sont pas les seules erreurs humaines éventuelles. La configuration des routeurs est ardue, c'est pourquoi pour réduire les risques d'erreurs l'utilisation d'outils de configuration automatique – bien que possédant eux aussi leurs limites – est fortement conseillée. L'utilisation de journaux d'évènements (*logs*) détaillés permet de surveiller le réseau et les opérations inhabituelles qui pourraient s'y produire.

Si nous considérons que seule l'architecture du système requiert une étude plus poussée, c'est parce que les problèmes découlant des deux autres aspects sont liés à des erreurs humaines, des opérateurs du réseau dans l'utilisation ou des concepteurs dans l'implémentation. De plus, concernant l'implémentation, elle dépend des choix de chaque constructeur, il faudrait par conséquent l'étudier au cas par cas.

1.2.3 Comparaison avec les VPN « classiques »

À l'inverse des VPN classiques, qui utilisent des protocoles d'encapsulation comme GRE (*Generic Routing Encapsulation*), IP/IP, etc., les VPN sur MPLS ne sont pas orientés connexion. Ce sont les VRF qui permettent de diriger l'information dans les VPN. Ceci est un atout important de MPLS/VPN. Il est possible de créer un grand nombre de VPN sans nécessiter de maintenir un grand nombre d'informations à chaque extrémité sur les VPN.

En utilisant les VPN classiques, les clients ont une visibilité complète sur leurs VPN et la possibilité de les contrôler. Par contre, avec MPLS/VPN les clients perdent cette visibilité – due à la transparence de cette technologie – toutefois la gestion s'en trouve simplifiée puisqu'il n'y a rien à faire par les clients. Cependant, il est nécessaire que le fournisseur de service porte une attention soutenue à la configuration des VPN dans les routeurs PE, afin d'éviter de briser l'intégrité d'un VPN en incluant, par exemple, un routeur PE qui n'a pas lieu dans un VPN. Un client se retrouvant devant un tel cas avec MPLS/VPN ne saura pas nécessairement que son VPN est corrompu.

Le chiffrement avec IPSec, SSL (*Secure Socket Layer*) ou TLS (*Transport Layer Security*) doit être utilisé dans les VPN classiques, car ceux-ci peuvent être amenés à voyager sur Internet et c'est ce chiffrement qui garantit la confidentialité des données.

Il est certes possible d'utiliser IPSec dans les VPN sur MPLS entre les routeurs PE. Toutefois, les VPN sur MPLS étant logiquement séparés, et en posant l'hypothèse que le réseau MPLS est privé, ceux-ci ne requièrent pas ce chiffrement pour garantir la sécurité des informations. Donc, dans ce cas, quel en est l'intérêt, sachant que le chiffrement nécessite du traitement, ce qui cause du délai? Est-ce que la sécurité n'est pas considérée comme parfaitement fiable? Ou bien est-ce une mesure visant à rassurer les clients?

D'après de nombreux chercheurs, la sécurité de MPLS/VPN repose sur la confiance que les clients font au fournisseur de service et donc du réseau MPLS. Car si ce dernier garantit que nul ne peut s'introduire dans le réseau – ce qui reste à vérifier – il pourrait avoir pour sa part accès aux données à l'intérieur du réseau MPLS.

1.2.4 Considérations techniques avancées

Cette partie décrit plus en détails la technologie MPLS/VPN en la séparant en plusieurs niveaux : le plan de contrôle, le plan de données et le plan de gestion.

1.2.4.1 Le plan de contrôle

Le plan de contrôle définit comment l'information de contrôle (ici, les routes VPN) est échangée sur le réseau. Les trois points importants sont les adresses VPN-IP, les *Route Distinguishers* (RD) et les *Route Targets* (RT).

Afin de permettre aux différents sites d'un réseau privé de parler entre eux, il y a une procédure d'échange de routes, entre routeurs CE et PE d'une part, et entre routeurs PE d'autre part. Les CE envoient leurs routes aux PE par du routage statique ou dynamique. De même, les PE envoient les routes provenant des autres sites d'un même VPN aux CE. Sur chaque PE, l'information de routage pour chaque VPN est maintenue dans des instances de routages de VPN, les VRF. À un VRF donné correspond une ou plusieurs interfaces du client connectées au CE et appartenant au même VPN. Les PE distribuent les routes reçues des CE et stockées dans les VRF aux autres PE qui connectent des sites du même VPN grâce au protocole MP-BGP (Bates et al., 2007).

L'espace d'adressage utilisé par chaque VPN pouvant se chevaucher, il est nécessaire de différencier les routes issues des différents VPN et ainsi éviter toute confusion quant à l'appartenance d'une adresse IP à un VPN donné. Pour y parvenir, les PE utilisent des *Route distinguishers* qui sont ajoutés à chaque route VPN reçue d'un routeur CE. Avec

cet ajout, il ne peut y avoir confusion avec l'information de contrôle de différents VPN. Il n'est alors plus question d'adresses IPv4 mais d'adresses VPN-IPv4 (ou v6, respectivement). Plus de détails seront fournis dans la section 1.2.5.

Ainsi, les annonces de routes échangées par le protocole MP-BGP (Bates et al., 2007) ne contiennent que des adresses VPN-IPv4 (et/ou VPN-IPv6, le cas échéant) associées aux étiquettes VPN liées aux routes échangées (Rekhter et Rosen, 2001). Les adresses VPN-IPv4 ne sont toutefois utilisées que dans le cœur du réseau. Entre PE et CE, ce sont les adresses IPv4 usuelles qui sont utilisées. Cela cause, entre autres conséquences, que les CE ignorent ce qui se passe dans le cœur du réseau, n'ayant ainsi aucune visibilité sur les autres VPN déployés.

Les routeurs PE s'échangent aussi au travers de MP-BGP des *Route Targets*, qui définissent quelles routes doivent être importées ou exportées pour chaque VRF. Une mauvaise configuration des RT peut gravement compromettre la sécurité de MPLS/VPN. Il s'agit toutefois là aussi d'une erreur humaine.

Pour plus de détails sur l'utilisation d'IPv6 dans le cadre des VPN sur MPLS, le lecteur peut consulter la RFC4659 (De Clercq et al., 2006).

1.2.4.2 Le plan de données

Le plan de données définit comment les données sont transmises sur le réseau. Entre le routeur CE et le PE, il s'agit de routage IP classique. Dans le cœur du réseau, les données transitent dans des tunnels, qu'ils s'agissent de chemins LSP, ou éventuellement de tunnels IPsec.

Pour cela, les PE-*ingress* réalisent un empilement d'étiquettes : en premier lieu, ils ajoutent une étiquette définissant le VPN auquel le paquet appartient, puis une seconde

étiquette MPLS qui permet de diriger le paquet à travers le réseau MPLS, en étant changée à chaque routeur P traversé, jusqu'aux PE-*egress*. Ces étiquettes sont enlevées par ces derniers et les paquets sont transmis aux routeurs CE de destination comme de simples paquets IP, en fonction de la valeur de l'étiquette VPN. Dans le cas du *penultimate hop popping*, c'est le dernier routeur P traversé avant le routeur PE-*egress* qui enlève l'étiquette MPLS.

1.2.4.3 Le plan de gestion

Le plan de gestion décrit comment sont gérés les éléments du réseau. La gestion d'un réseau IP peut être de type *in-band* (les données de gestion passent sur le réseau avec les autres données) ou *out-of-band* (hors-bande, la gestion s'effectue par un autre moyen, par exemple par le réseau téléphonique ou tout autre réseau indépendant).

Dans le cas de la gestion *in-band*, il est important de prendre plusieurs mesures de sécurité afin d'empêcher toute possibilité d'intrusion et/ou de modification des informations de gestion. Il faut notamment limiter l'accès sur chaque routeur aux seules interfaces et adresses d'origine nécessaires (et encore, il est possible de mystifier une adresse IP), utiliser des protocoles sécurisés comme SSH (*Secure Shell*) et une authentification forte (certificats, jetons, clés), bloquer les données de gestion venant de l'extérieur au moyen par exemple de listes d'accès, les *access lists* des routeurs. En outre, le nœud principal de gestion (*NOC : Network Operations Center*), s'il existe, doit être fortement protégé contre les intrusions afin d'éviter qu'un utilisateur aux mauvaises intentions n'en prenne le contrôle, et puisse par la suite gérer les routeurs depuis cet emplacement.

La gestion des CE peut se révéler plus complexe à mettre en œuvre. Elle nécessite soit deux liens logiques séparant le trafic normal et de gestion entre CE et PE (ce qui représente la meilleure solution), soit l'utilisation d'une interface de *loopback* du CE

placée dans le VRF de gestion du CE (auquel cas tout le VPN a accès à la station de gestion). Il faut donc là aussi utiliser des *access-lists* dans les interfaces *ingress* des routeurs PE.

Dans tous les cas, il ne faut pas oublier que les CE ne peuvent être considérés comme sûrs puisqu'ils se trouvent chez les clients.

La gestion *out-of-band* est à la base plus sûre car elle n'est pas réalisée sur le même réseau que celui où transitent les données. Toutefois, l'accès à ce réseau de gestion doit lui aussi être sécurisé, par exemple par les méthodes énoncées précédemment.

1.2.5 La séparation des VPN

Les exigences relatives à la sécurité des VPN dans le réseau MPLS du fournisseur de service peuvent être énoncées ainsi :

- Le trafic provenant d'un VPN ne doit pas être visible d'un autre VPN
- Le trafic issu du cœur ou d'autres VPN ne doit pas pouvoir s'introduire dans un VPN donné.

En outre, la possibilité d'utiliser des espaces d'adressage se chevauchant sans qu'il y ait confusion fait aussi partie des attentes.

1.2.5.1 Séparation des espaces d'adressage

La séparation des espaces d'adressage des différents VPN, nécessaire dans le cas où plusieurs VPN utilisent des plages d'adresses se chevauchant, est atteinte tel que décrit dans la RFC4364 (Rosen et Rekhter, 2006) par l'utilisation des adresses VPN-IPv4 (ou v6, le cas échéant – il faut noter que MPLS/VPN fonctionne indifféremment avec IPv4 ou IPv6).

Les adresses VPN-IPv4 sont la concaténation d'une adresse IPv4 classique et d'un *route distinguisher* sur 8 octets, tel que présenté ci-dessous :

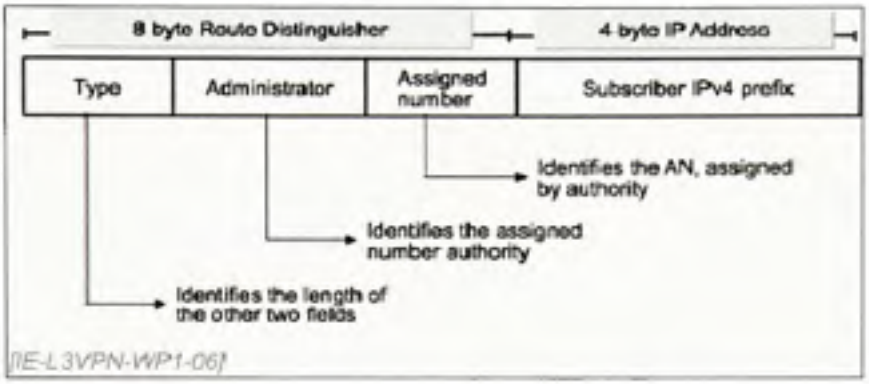

Figure 1.4 ***Format d'une adresse VPN-IPv4***
(Tiré de Berkowitz, 2003)

Les *route distinguishers* étant spécifiques à chaque VPN, il est possible d'utiliser la même plage d'adresse IP dans différents VPN sans que cela ne cause le moindre problème de chevauchement.

Les adresses VPN-IPv4 obtenues sont donc uniques, elles sont utilisées dans le cœur du réseau entre les PE pour réaliser les routes VPN. Le cœur utilise quant à lui des adresses IPv4 classiques pour réaliser le contrôle. Il n'y a donc pas non plus possibilité de chevauchement entre les adresses des VPN et les adresses des éléments du réseau cœur.

L'interface PE-CE du PE (à ne pas confondre avec le lien PE-CE) utilise aussi l'adressage VPN-IPv4, donc même au sein d'un routeur PE la séparation des VPN est opérante. Le seul inconvénient de ce dernier point est que cette interface du PE est joignable depuis le VPN concerné et donc des attaques contre le PE pourraient être tentées.

1.2.5.2 Séparation du trafic

La séparation du trafic au sein du réseau MPLS cœur est réalisée par l'encapsulation des données dans les LSP (*Label Switch Path*). Cette encapsulation consiste à ajouter aux données un entête définissant le VPN, en plus de l'entête MPLS classique.

Au niveau des routeurs PE, la séparation du trafic est accomplie en fonction des interfaces. Les interfaces faisant face au cœur réalisent le routage, ou plutôt, la commutation, en fonction de leur table de routage globale. Les paquets arrivant sur ces interfaces sont traités comme des paquets IP usuels. Les interfaces faisant face aux CE sont liées à des VRF par l'intermédiaire de la commande *ip vrf forwarding* ; la commutation est alors faite suivant l'instance de VRF.

Les LSP ne sont pas le seul moyen d'encapsulation disponible : les tunnels IPSec, L2TPv3, IP/IP et GRE sont aussi utilisables. Mais quelle que soit la méthode employée (simple marquage des paquets ou utilisation de tunnels), les VPN sont isolés les uns des autres.

Un point important dans la sécurité de MPLS/VPN au niveau de la séparation des VPN est que les routeurs P du cœur n'interviennent pas du tout au niveau des VPN. Ils ne font que la commutation des paquets en fonction de l'étiquette MPLS et n'ont aucune visibilité sur le contenu des VPN. Ils n'ont aucune interaction avec les VPN, donc un impact très restreint quant à la sécurité du réseau.

Comme beaucoup d'autres, ce dernier point n'est valable que si les routeurs P sont correctement configurés. La configuration des équipements est un point extrêmement important qu'il est possible de simplifier avec l'utilisation d'outils de configuration automatique.

1.3 Problématique

Par une stratégie rendant possible l'accès à Internet pour tous et partout, le monde de l'informatique s'est retrouvé complètement bouleversé. La sécurité, qui avait jusque-là une importance assez relative, est devenue primordiale. Les logiciels antivirus, anti-espiogiciels, les pare-feux, etc. sont devenus monnaie courante dans les entreprises comme chez les particuliers. La sécurité est désormais au cœur du développement des nouvelles applications et technologies.

Les réseaux informatiques permettent aux données de se rendre de leur source à leur destination. Le protocole IP est devenu, avec l'évolution d'Internet, le plus utilisé sur les réseaux, grâce à sa simplicité. Le protocole ATM offrait pour sa part une solution plus sûre, plus efficace, mais aussi plus complexe. Il est toujours utilisé, mais principalement pour transporter des paquets IP, laissant de côté une grande partie de ses avantages.

La notion de réseaux privés virtuels n'est pas nouvelle. Depuis longtemps, les entreprises ont besoin de liens privés reliant par exemple leurs différentes succursales. La solution la plus évidente est celle d'une ligne louée, qui peut néanmoins se révéler très dispendieuse. Les VPN ont été créés afin de permettre à ces entreprises d'utiliser le réseau Internet pour communiquer entre elles, en établissant des tunnels dont chaque extrémité se trouve dans une succursale. Afin de garantir la confidentialité des données, tous les paquets IP sont chiffrés et encapsulés par des protocoles comme L2TP, PPTP (*Point to Point Tunnelling Protocol*) ou IPsec.

L'arrivée de MPLS parmi les protocoles de communication a permis d'apporter la simplicité de la commutation dans les réseaux et aussi de proposer de nouvelles technologies comme l'ingénierie de trafic et les réseaux privés virtuels sur MPLS. Les VPN sur MPLS sont une évolution des VPN classiques énoncés précédemment, les simplifiant fortement pour les clients. L'utilisation des VPN sur MPLS offre à ces

derniers plusieurs avantages : la transparence (pas de client VPN à installer ou de configuration à réaliser) et la performance (pas de chiffrement donc moins de temps de calcul, plus de débit utile). Mais qu'en est-il de la sécurité?

Selon Behringer et Morrow (Behringer et Morrow, 2005), une politique de sécurité réseau qui se veut efficace se doit d'être prévue dès l'étape de la conception de celui-ci. La création d'un réseau et l'application de la sécurité sur ce réseau sont souvent le fait d'équipes de travail séparées. Aussi, l'ajout de la sécurité implique habituellement de restreindre une partie des capacités du réseau, afin d'empêcher les intrusions et de prévenir de possibles brèches.

Un des défis de l'expert en sécurité est de s'assurer qu'aucune brèche n'existe dans l'implémentation. Alors qu'un ingénieur réseau atteint son but lorsqu'il trouve une méthode fonctionnelle et performante pour implanter le réseau, l'expert en sécurité subit un échec s'il existe ne serait-ce qu'une seule faille dans la sécurité du réseau.

Avant de pouvoir déterminer ce qui est sécuritaire et ce qui ne l'est pas, il est important de définir le sens du terme « sécurité » et ce qui doit être mis en œuvre pour y parvenir. L'inconvénient est que selon le domaine, l'application, la valeur des biens ou de l'information à protéger, la réponse est très variable. Par exemple, la sécurité d'un aéroport international diffère de celle d'un aérodrome de tourisme. De même, la sécurité d'un site web bancaire n'est pas la même que celle d'un blogue réalisé par un particulier.

Pour beaucoup, la sécurité implique le chiffrement des données. Il ne faut pas croire que MPLS n'est pas une technologie sécuritaire parce que le chiffrement n'est pas utilisé par défaut. Si la sécurité consiste en l'isolement réciproque des réseaux privés virtuels, dans ce cas MPLS/VPN peut être vu comme sécuritaire.

Les objectifs de la sécurité informatique appliquée aux réseaux sont définis par :

- l'intégrité, qui garantit que les données ne sont pas altérées dans leur transport,
- la confidentialité, qui assure que les données ne sont pas révélées à des personnes non autorisées,
- la disponibilité, garantissant l'accès en tout temps aux données et l'absence de déni de service dans le réseau,
- l'authentification, qui permet de limiter l'accès aux personnes autorisées,
- la non-répudiation, qui empêche de nier une opération réalisée.

L'isolement des réseaux privés virtuels permet de remplir les objectifs d'intégrité et de confidentialité. La disponibilité et l'authentification doivent être gérées par le fournisseur de service, afin d'empêcher tout déni de service ou intrusion. Enfin, la non-répudiation est à la charge du client, ce n'est pas en général un service offert par le fournisseur de service.

L'élément clé de ce projet de recherche est de démontrer l'étanchéité des différents tunnels VPN, garantissant que la séparation des VPN est toujours effective. Cela afin de garantir la sécurité des données des clients.

La disponibilité du réseau MPLS cœur est toutefois aussi importante, afin d'éviter des attaques de type déni de service (DoS, *Deny of Service*). Cet aspect de la sécurité concerne néanmoins plutôt le fournisseur de service, car il en découle la disponibilité du réseau et non l'étanchéité des VPN en place.

Ce mémoire se concentrera sur les VPN de niveau 3 sur MPLS, solution la plus couramment employée dans la réalité. Les VPLS (*Virtual Private LAN Service*) et autres liens *Pseudo-wire* ne seront par contre pas traités. Par ailleurs, les problèmes liés à l'implémentation de l'architecture seront brièvement cités mais non détaillés. Les bugs liés aux systèmes d'exploitation des routeurs peuvent être corrigés et sortent du cadre de ce mémoire.

CHAPITRE 2

ANALYSE DE LA SÉCURITÉ DE MPLS/VPN

Tel qu'indiqué dans la problématique, l'aspect important de la sécurité pour ce projet est l'étanchéité des VPN, et par conséquent des VRF. Entre autres :

- aucun VPN ne doit pouvoir communiquer avec un autre VPN,
- aucun VPN ne doit pouvoir échanger de l'information avec le cœur du réseau.

Une autre façon de présenter cette étanchéité est de garantir que ce qui rentre dans le réseau MPLS par un VPN donné est forcé de sortir du réseau MPLS par ce même VPN.

Ce chapitre se propose d'analyser la sécurité et les menaces sur les réseaux MPLS/VPN en considérant les différents éléments constituant un réseau MPLS/VPN comme le réseau cœur et les réseaux d'accès (les liens CE-PE par exemple) mais aussi en considérant les différents types de menaces, quelles que soient leurs origines et destinations.

Dans un premier temps, nous présentons une étude assez exhaustive des menaces possibles dans un environnement réseau MPLS, ensuite nous verrons plus spécifiquement la sécurité des VPN sur MPLS en cherchant les vecteurs possibles d'attaques, en comparant avec les technologies éprouvées comme ATM/FR, et en détaillant des architectures utilisant le réseau MPLS/VPN qui nécessitent beaucoup plus d'attention pour être sécuritaires. Une des conditions permettant la réalisation d'une attaque inter-VPN dans une de ces architectures avancées a été le point de départ d'une étude du protocole BGP, présentée dans le chapitre 3. Elle expose entre autres ses faiblesses ainsi que les extensions qui lui sont proposées.

2.1 Menaces et attaques dans un environnement réseau

Cette partie a pour but de présenter une liste assez exhaustive des attaques éventuelles pouvant être perpétrées dans un réseau MPLS. Tous les types d'attaques réseau ne sont donc pas abordées ici, comme par exemple celles reliées aux environnements sans-fil et Web 2.0.

2.1.1 Catégories de menaces

Avant de dresser une liste des attaques s'appliquant à MPLS, il peut être intéressant de les regrouper pour les définir. Les attaques possibles sur un système ou un réseau peuvent à cet égard être catégorisées selon divers paramètres comme les dégâts causés, leur complexité, ou leur but (Easttom, 2006).

En classant les attaques selon leur objectif, nous pouvons distinguer :

- les tentatives d'intrusion, permettant de gagner un accès aux ressources d'un système,
- les dénis de service, bloquant l'accès au système pour les utilisateurs légitimes,
- les logiciels malveillants, comme les virus, les chevaux de Troie, les portes dérobées, les espiogiciels, etc. permettant le vol d'information ou l'utilisation illégitime de ressources.

Les intrusions peuvent permettre à l'intrus de disposer d'informations confidentielles, de modifier les paramètres du système pénétré à son avantage, en bref de compromettre la sécurité de ce système et éventuellement celle des systèmes attachés. Les intrusions utilisent généralement les failles des systèmes, bien que l'ingénierie sociale (*social engineering*), l'art de soutirer de l'information en abusant de la confiance des personnes, soit très utile pour obtenir les informations manquantes.

Le déni de service fait partie des attaques de type bloquantes qui ne permettent pas à l'attaquant de pénétrer le système visé (hormis dans certains cas où la surcharge d'un équipement peut permettre de laisser passer tout le trafic par défaut, par exemple avec certains anciens pare-feux), mais affaiblissent les ressources disponibles et par conséquent entravent le fonctionnement normal de l'équipement. Les utilisateurs légitimes du système vont alors se voir l'accès considérablement ralenti ou, idéalement pour l'attaquant, refusé. Ce type de menaces est en général bien plus simple à mettre en œuvre que les intrusions, c'est pourquoi les dénis de services sont très répandus.

Les logiciels malveillants (de l'anglais *malware*, contraction des deux mots *malicious* et *software*) forment la catégorie de menaces la plus utilisée. Mélange d'outils automatiques d'intrusion (les vers), de déclenchement (les bombes logiques) et d'action néfaste (les virus), ils peuvent souvent se répliquer d'eux-mêmes (vers, virus) pour se propager vers d'autres systèmes.

L'exemple de *malware* le plus connu est le virus, programme ayant pour but de se dupliquer et pouvant perturber le fonctionnement du système infecté. Il se répand par diverses méthodes, les plus populaires étant l'envoi de courriels via le carnet d'adresses d'une personne touchée (car les utilisateurs ne se méfient que peu ou pas des courriels provenant de personnes connues), l'échange de données (en particulier sur les réseaux d'échange P2P, *Peer to Peer*), les logiciels de messagerie instantanée (en utilisant les listes de contacts), ou en surfant sur certains sites web malveillants. Souvent, ils utilisent les failles de certains programmes, fureteurs Internet ou systèmes d'exploitation pour agir.

Parmi les autres logiciels malveillants se trouvent les chevaux de Troie qui appliquent le principe d'une porte dérobée pour s'installer sur le système, et qui vont ensuite télécharger eux-mêmes des virus ou ouvrir d'autres portes dérobées, permettant de futures intrusions.

Les espiogiciels représentent la dernière « mode » en termes de logiciels malveillants. Plus connus sous leur terme anglophone de *spywares*, ils surveillent les actions effectuées sur un système. Ils peuvent se limiter à un fichier témoin (*cookie*) du fureteur, celui-ci étant un fichier texte pourtant créé avec la noble cause de se souvenir de l'utilisateur pour lui permettre d'accélérer la reconnexion à un site web déjà visité où il aura enregistré des informations personnelles, un panier d'achat, etc. Le problème est que n'importe quel site peut venir lire ces fichiers et ainsi révéler de nombreuses informations confidentielles si le fureteur ne l'en empêche pas. Un autre type d'espiogiciel est l'enregistreur de frappe (*keylogger*), il enregistre tout ce qui est tapé par l'utilisateur du système infecté et peut aussi prendre régulièrement des captures d'écran, le tout étant soit envoyé par courriel ou relevé par celui l'ayant conçu et/ou installé.

La catégorie des logiciels malveillants évolue de plus en plus vite, le nombre de virus, vers, espiogiciels incluant leurs variantes ne cessant d'augmenter. Les logiciels malveillants permettent parfois des attaques qui se rapprochent des deux premières catégories de menaces, permettant intrusions via les portes dérobées et déni de service via les bombes logiques. Dans ce dernier cas, un virus étant hébergé sur de très nombreux systèmes de par le monde va lancer à un moment prévu à l'avance une attaque simultanée vers un site, une adresse ou un système dans le but de le faire tomber. L'attaque est parfois impossible à prévoir, et à cause de la répartition des machines « zombies » possédant la bombe logique, difficile à arrêter.

Enfin, en ce qui concerne l'environnement d'exécution, les logiciels malveillants visent surtout le système d'exploitation le plus utilisé, Windows XP/2000/Vista, présent sur les stations de travail ou sur les serveurs, mais pas sur les équipements réseaux. Ces derniers sont donc moins touchés par cette catégorie de menaces. Par contre, rien n'empêche un virus, un ver ou un cheval de Troie de s'installer sur une machine hôte mal protégée chez un client avant de s'attaquer aux équipements réseaux auxquels celui-ci est relié.

2.1.2 Types d'attaques

Après avoir étudié les différentes catégories de menaces possibles, cette partie présente les différents types d'attaques possibles dans un environnement réseau.

2.1.2.1 Écoute sur le réseau

L'écoute sur le réseau est une attaque passive permettant d'obtenir des informations (tels des mots de passe) pouvant être réutilisées dans le futur pour réaliser des accès non autorisés. L'écoute peut se faire grâce à un renifleur (*sniffer*), logiciel ou matériel placé dans le réseau. La présence d'un concentrateur (*hub*) dans le réseau rend cette attaque très simple, à cause du fonctionnement « duplicatif » du concentrateur qui offre l'information à toutes les stations qui lui sont connectées. L'attaque est par contre beaucoup plus délicate à mettre en œuvre si le médium est de la fibre optique, mais pas impossible (Everett, 2007).

L'attaquant doit posséder un accès au médium pour pouvoir écouter ce qui y transite. Si l'accès est physiquement impossible, l'installation de logiciels malveillants sur le poste d'une personne « à l'intérieur » peut être une solution de rechange. Il suffit alors d'un courriel contaminé envoyé à de multiples employés pour être quasiment certain que le programme malveillant (ver, cheval de Troie) soit installé en un point sensible et puisse alors renifler le trafic sur le réseau.

La meilleure parade à l'écoute sur le réseau est le chiffrement de tout le trafic qui passe sur celui-ci, ce qui est rarement faisable à grande échelle. L'utilisation de SSH et de tunnels VPN permet aussi de réduire le risque. De même, les concentrateurs devraient tous être bannis et remplacés par des commutateurs, qui ne partagent pas l'information. À noter qu'en 2000 un outil pouvant détecter les stations écoutant sur le réseau (de par leur mode promiscuité actif) nommé AntiSniff a fait son apparition. Mais hélas, ses

méthodes de détection des renifleurs ont été utilisées par la suite pour rendre ces derniers indétectables. Une attaque passive reste donc difficile à détecter.

2.1.2.2 Modification de données

Si l'écoute n'était qu'une attaque passive, la modification de données va plus loin et constitue une attaque active : l'attaquant va modifier certaines données qu'il parvient à lire sur le réseau et ainsi, en plus de briser la confidentialité, changer le sens du contenu des paquets. Même si la confidentialité n'est pas toujours primordiale, les données ne doivent pas être modifiées dans leur transmission : l'intégrité des données est essentielle quel que soit le domaine.

L'utilisation de chiffrement ou, si la confidentialité n'est pas requise, de signatures numériques à l'aide de systèmes de chiffrement asymétrique ou asymétrique peut permettre de garantir cette intégrité.

2.1.2.3 Mystification dans la pile protocolaire TCP/IP

La mystification est l'action de berner, d'abuser une personne en déformant la réalité. Appliquée aux réseaux, elle consiste à tromper un système (un pare-feu par exemple) en se faisant passer pour une autre entité que celle qui a réellement envoyé le message. Les différents paramètres pouvant être mystifiés se situent principalement dans les entêtes ajoutés par les couches liaison, réseau et transport : les adresses MAC et IP sources, les numéros de séquence TCP (*Transmission Control Protocol*), etc.

La mystification d'adresse MAC permet des attaques de niveau 2 au sein d'un réseau local, d'outrepasser les filtres d'adresses physiques autorisées dans un réseau sans-fil, de rediriger le trafic, etc. L'adresse physique ou adresse MAC est pourtant une donnée inscrite sur la carte d'accès réseau, unique dans le monde, hélas il est désormais possible

sur de nombreux modèles de modifier manuellement l'adresse de sa propre carte réseau. Un filtre basé sur des adresses physiques n'est donc pas sûr.

La mystification d'adresses IP ressemble à celle d'adresses MAC, tout en agissant à la couche réseau. Elle profite des systèmes utilisant l'adresse IP source comme base d'authentification, comme les filtres ou les listes d'accès des routeurs, les pare-feux, etc. Il suffit de deviner une adresse IP autorisée puis de la mystifier afin de traverser ces filtres sans être arrêter. Toutefois, dans le cas où les seules adresses autorisées sont celles appartenant au réseau local, le filtrage d'adresses sera efficace en bloquant les paquets provenant de l'extérieur portant une adresse source locale.

Au niveau de la couche transport, il est possible de mystifier les numéros de séquences TCP. Le protocole TCP permet d'établir une connexion entre deux systèmes, cette connexion est identifiée par des numéros de séquences qui permettent de réaliser du contrôle de congestion et de détecter les pertes de paquets. Les numéros de séquence évoluent au cours d'une communication en fonction de la quantité de données échangées. Un intrus écoutant une transmission TCP va alors pouvoir y injecter des paquets en prévoyant le numéro de séquence suivant correctement et éventuellement en prendre le contrôle. Cette technique est aussi appelée « vol de session ». Il est aussi possible de prédire les numéros de séquences même si ceux-ci sont initialisés aléatoirement, à cause du caractère peu aléatoire des générateurs de nombres aléatoires sur les systèmes informatiques (Venema, 1996).

Les attaques par mystification à différents niveaux de la pile protocolaire TCP/IP sont rendues possibles par la relation de confiance que deux systèmes établissent simplement en se basant sur les informations contenues dans les différents entêtes de la pile TCP/IP.

La mystification est aussi possible à la couche application, méthode très utilisée par exemple par les émetteurs de pourriels pour masquer leur identité en indiquant comme adresse source une adresse de courriel aléatoire les empêchant d'être trouvés.

La protection contre la mystification serait le chiffrement des entêtes et l'authentification, techniques aisément réalisables à la couche application, plus difficilement applicables aujourd'hui pour les autres couches (liaison, réseau, transport) cependant. Le chiffrement des entêtes pose en effet le problème suivant : si ceux-ci sont chiffrés, comment les équipements réseaux peuvent-ils acheminer les paquets correctement?

IPv6 propose pourtant ces techniques, chiffrement et authentification de la charge utile de bout en bout, de la charge utile et de l'entête en mode tunnel entre deux passerelles. Dans le premier mode, la sécurité repose sur le fait que mystifier une adresse source n'est pas suffisant pour que le paquet soit accepté à la destination. Si le contenu n'est pas authentifié correctement, le paquet sera rejeté même si l'adresse source « semble » valide. Donc IPv6 offre une solution valide contre la mystification à la couche réseau.

Toutefois, l'utilisation de ces techniques dans IPv6 présente des problèmes de compatibilité avec les équipements réseaux (McGehee, 2003). Plusieurs fonctionnalités réseaux comme la traduction d'adresses (NAT, *Network Address Translation*) et le filtrage des pare-feux, la qualité de service, le changement dynamique d'adresses pour les applications mobiles, etc. ne fonctionnent pas avec IPsec et par conséquent avec IPv6 lorsqu'il utilise IPsec.

2.1.2.4 Attaque « Man in the middle »

Une attaque de type *Man in the middle* se produit lorsque l'intrus se trouve sur le réseau entre deux utilisateurs légitimes, écoute le trafic circulant entre eux et peut l'intercepter

et le modifier sans que ceux-ci ne le remarquent. En quelque sorte, l'intrus se fait passer pour chacun des utilisateurs lorsqu'il converse avec l'autre.

Une des méthodes permettant ce type d'attaque est la mystification de serveur DNS (*Domain Name Server*), qui va indiquer une fausse adresse du serveur auquel le client souhaite se connecter, le renvoyant vers un système contrôlé par l'attaquant qui acheminera les paquets vers le réel serveur une fois ceux-ci lus afin que le client ne se rende compte de rien. Celui-ci va alors éventuellement donner des informations personnelles comme ses mots de passe, numéros de cartes de crédit, etc.

Il est aussi possible à l'attaquant de profiter des erreurs de frappe de l'utilisateur qui écrit mal l'adresse URL (*Uniform Ressource Locator*) du serveur en créant des serveurs ayant des URL très proches phonétiquement ou orthographiquement du serveur légitime. Un exemple : taper www.goggle.com au lieu de www.google.com redirige vers un site qui n'a aucun rapport avec *Google*. Ce n'est pas le cas ici, mais si ce site (profitant de la célébrité de *Google*!) redirigeait les paquets vers le vrai *Google*, tout en lisant les informations entrées par l'utilisateur, il pourrait enregistrer de nombreuses informations personnelles…

Le chiffrement des messages échangés peut empêcher à l'intrus de comprendre la signification de ces derniers. Mais ce dernier peut toujours les supprimer, n'empêchant donc pas le déni de service, ou être plus fin et réaliser des attaques de rejeu.

Une attaque de rejeu consiste à écouter un message qui passe et à le répéter ultérieurement. Il n'est pas nécessaire à l'attaquant d'en comprendre la signification c'est-à-dire de le déchiffrer. Le cas le plus courant est l'identification d'un client envoyant son nom d'utilisateur et son mot de passe, le tout étant chiffré. Si l'attaquant souhaite se connecter au même service, il lui suffit de répéter le même message, et il sera authentifié.

Pour empêcher le rejeu, il est nécessaire que les protocoles de chiffrement utilisent des challenges ou des clés de session qui différent à chaque fois, tenant éventuellement compte du temps.

2.1.2.5 Déni de service

Le but du déni de service est d'affaiblir ou de rendre inopérable un système ou un réseau. Il se base sur le fait que les ressources d'un système sont limitées physiquement. S'il est surchargé, il ne pourra plus répondre aux requêtes normales. L'attaquant ne peut acquérir aucun accès ou information mais empêche les utilisateurs légitimes d'accéder aux ressources visées par l'attaque. Il ne lui est toutefois pas possible de briser l'étanchéité des tables de labels ou de s'introduire dans un VPN de cette façon. Très répandu car simple à effectuer, le déni de service peut se réaliser de différentes façons.

L'inondation de messages TCP SYN est une attaque de déni de service qui utilise l'établissement de connexion dans TCP (aussi appelé *three-way handshake*). Le système source inonde la cible de messages SYN en indiquant une adresse source inexistante, de sorte qu'il n'en reçoive pas les réponses. Celle-ci se retrouve alors avec un grand nombre de connexions dans un état semi-ouvert, jusqu'à ce qu'elle ne puisse plus accepter de nouvelles connexions, mêmes légitimes.

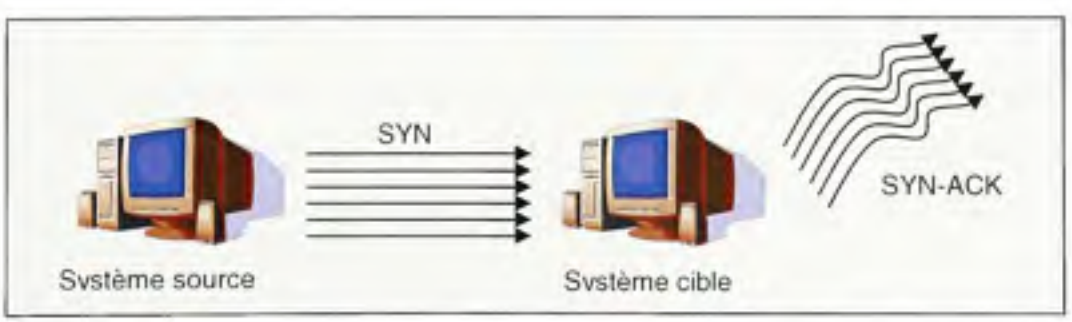

Figure 2.1 ***Inondation de messages TCP SYN***

La Figure 2.1 illustre cette inondation. Nous pouvons y voir que les messages SYN-ACK ne sont pas renvoyés vers la source mais dans une autre direction, d'ailleurs il n'est pas nécessaire que la fausse adresse source spécifiée existe. La raison du déni de service est que les systèmes ne peuvent gérer plus d'un certain nombre de connexions TCP simultanément. Pour empêcher que cette inondation ne soit destructrice, des temporisateurs courts doivent être utilisés afin de fermer rapidement les connexions semi-ouvertes.

Il existe d'autres techniques permettant d'empêcher une perte trop importante de mémoire due à ces inondations, comme les micro blocs, qui permettent d'allouer de la mémoire par micro fragments à chaque nouvelle connexion TCP SYN, ou les témoins SYN, qui permettent de n'allouer la mémoire qu'une fois que le client envoie le message ACK final grâce à l'utilisation de témoins (*cookies*) lors du renvoi du message SYN-ACK comprenant les informations du client ayant envoyé un message SYN. Il est aussi possible d'utiliser des témoins autrement (Chau, 2004) : à la réception d'un message SYN, le serveur envoie un message SYN-ACK erroné au client. Ce dernier, s'il est légitime, va envoyer un message de réinitialisation de connexion (RST). Si le serveur le reçoit, il sait que ce client est sûr et acceptera les requêtes SYN suivantes du même client. Pour se souvenir des clients, des témoins sont utilisés. Cette méthode est plus simple à implémenter que la précédente, mais fait perdre du temps pour établir la connexion (six messages doivent être échangés au lieu de trois).

L'inondation existe aussi pour des paquets UDP. Si un paquet UDP est dirigé vers un port non utilisé par exemple, le système cible va répondre par un message d'erreur ICMP. Si un grand nombre de messages UDP sont envoyés, il est possible que le système soit dépassé.

L'attaque de *smurf* (d'après le nom du code source utilisé pour lancer cette attaque) consiste à envoyer un paquet ICMP à l'adresse *broadcast* d'un réseau, en mystifiant l'adresse source du paquet pour y placer l'adresse de la machine cible de l'attaque. Toutes les stations du réseau recevant le message ICMP *ping request* vont en général répondre à la machine cible et si cette attaque est répétée de nombreuses fois, la machine cible va être surchargée par la réception de messages ICMP *ping reply* en provenance d'autres stations de son propre réseau. La seule difficulté de cette attaque est d'envoyer les paquets ICMP dans le réseau si un filtrage approprié est utilisé en bordure, il est toutefois possible d'y parvenir par l'intermédiaire d'un cheval de Troie.

Les pourriels (ou *spam*) sont d'un côté un agacement pour les utilisateurs qui les reçoivent mais peuvent aussi consister en un déni de service pour les serveurs de relais de courriels s'ils sont très nombreux. Une inondation d'un serveur de relais par des milliers de pourriels peut empêcher celui-ci de délivrer les courriels légitimes convenablement, ou le ralentir fortement. Le déni de service peut aussi s'appliquer aux utilisateurs qui perdent du temps à faire le tri entre les courriels légitimes et les pourriels. Ces derniers peuvent aussi en ayant recours à une adresse de courriel d'origine mystifiée (rien n'étant plus facile que de modifier une adresse de courriel source) permettre de lancer une attaque détournée vers une cible dont l'adresse courriel est celle apparaissant comme prétendue source à tous ceux ayant reçu les pourriels. Afin de limiter la gêne due aux pourriels, des filtres de courriels entrants peuvent être exploités, mais ne sont pas efficaces à 100%, en outre pour éviter que les adresses courriels sources soient mystifiées, tous les fournisseurs d'accès devraient vérifier que leurs utilisateurs emploient bien leur propre adresse comme adresse source.

La puissance d'une attaque de déni de service repose dans le nombre de machines participant à l'attaque. Plus l'attaque est distribuée, plus elle est puissante et éventuellement difficile à stopper. Les bombes logiques sont un très bon moyen d'accomplir une attaque distribuée. Liées à un virus, elles vont se placer dans de

nombreux systèmes en attendant le moment préprogrammé pour lancer l'attaque de déni de service, toutes simultanément.

2.1.2.6 Scan de ports

Habituellement ce genre d'attaque précède une intrusion : l'attaquant cherche sur le système cible, par exemple le routeur PE, les ports ouverts, comme le port 80 (web), 23 (telnet), 22 (SSH), 21 (ftp), etc., représentant autant de portes d'entrée permettant d'établir une communication avec la cible. Certaines des applications résidant derrière les ports ouverts possèdent des failles connues qui peuvent être exploitées pour parvenir à gagner l'accès au système visé. Le scan de port peut être réalisé à grande échelle avec des scripts automatisés, à la recherche de systèmes attaquables car non suffisamment protégés. Tous les ports non nécessaires doivent être fermés, dans le cas de l'interface CE d'un routeur PE seuls les ports utilisés par les protocoles de routage devraient être ouverts, avec des restrictions sur les listes d'accès vis-à-vis de l'émetteur des mises à jour de routage. Le port d'accès au mode console (telnet ou SSH) devrait être limité à la seule interface de configuration, distincte des interfaces CE/PE/P qui font transiter le trafic de données.

Il existe de nombreuses techniques de scan. La principale consiste à ouvrir une connexion TCP en envoyant un message SYN vers un port donné. Si le port est ouvert, la cible enverra un message SYN-ACK, s'il est fermé elle enverra un message RST. S'il est filtré (par un pare-feu par exemple), rien ne sera envoyé. L'attaquant peut donc savoir quels ports sont ouverts, filtrés ou fermés. D'autres techniques se servent des drapeaux de l'entête TCP pour envoyer des messages Null (aucun drapeau), FIN ou X-Mas (FIN, PSH, URG). L'attaquant saura dans ce cas que le port est fermé s'il reçoit un message RST, filtré s'il reçoit un message ICMP de type 3 *unreachable*, et finalement, ouvert si aucune réponse n'est reçue.

L'inconvénient d'un scan de ports pour l'attaquant est qu'il laisse des traces. Les systèmes de détection d'intrusion (IDS, *Intrusion Detection System*) reconnaissent les scans de port et peuvent en avertir les administrateurs réseaux. Le problème est que les programmes de scan comme *nmap* peuvent cependant être assez discrets pour ne pas se faire remarquer, en initiant des connexions TCP exploitant uniquement le premier message SYN (technique appelée *SYN scan*), puis en envoyant un message RST si un message SYN-ACK revient. Ces connexions non complétées ne sont pas inscrites dans les journaux d'évènements des IDS. L'utilisation de pare-feux à mémoire d'état (*stateful*), ne laissant que le trafic essentiel passer, est nécessaire.

2.1.2.7 Accès non autorisé

Si un attaquant parvient à déterminer à l'aide d'un scan de port qu'une application (par exemple, un serveur FTP) fonctionne, l'étape suivante va consister à en gagner l'accès. Habituellement, l'accès aux services à travers le réseau s'effectue à l'aide du couple nom d'utilisateur et mot de passe. L'inconvénient de ce système (sans parler du fait que trop souvent ces informations d'identification sont transmises de façon non chiffrée) est la faiblesse humaine. Comme tout utilisateur doit se souvenir d'un grand nombre de mots de passe pour différentes applications (comptes de courriels, connexion aux nombreux sites requérant une identification, etc.) il a tendance à recourir à des mots de passe faciles à mémoriser. Là où le bât blesse, c'est que plus un mot de passe est facile à mémoriser, plus il est facile de le casser. C'est donc un réel problème étant donné la croissance du nombre de mots de passe qu'il faut retenir. Il n'est pas possible d'augmenter la mémoire d'un être humain comme celle d'un ordinateur, notre cerveau possède ses limites. Une fois que l'attaquant possède le mot de passe d'un utilisateur, il a libre accès aux ressources offertes à l'utilisateur. Cela est encore pire pour la biométrie car si notre empreinte est dupliquée, il est impossible d'en changer…

La méthode d'identification classique nom et mot de passe est insuffisante, non pas à cause de son fonctionnement, fiable si chiffré, mais à cause des êtres humains. Il est donc nécessaire de ne pas se limiter à cette identification pour les services sensibles. L'authentification, qui permet en plus de s'assurer que la personne est bien celle qu'elle prétend être, devrait être utilisée. Par exemple, les jetons électroniques (le plus connu étant RSA) associés à un mot de passe représentent une technique d'authentification forte, dans laquelle l'utilisateur doit non seulement donner une information que lui seul connaît, et la valeur du jeton (quelque chose qu'il possède) qui change à chaque minute. Une autre possibilité d'authentification forte est la combinaison de la biométrie (qui se sert d'une caractéristique physique de l'utilisateur) avec un mot de passe ou avec un jeton électronique. Il est toutefois difficile aujourd'hui d'envisager de l'authentification forte pour toute application, particulièrement dans un cadre personnel non-commercial (serveurs de courriels, forums de discussion). L'authentification forte a un prix, et nécessite une gestion supplémentaire. Si l'information à protéger est d'une importance moindre, l'identification simple par mot de passe peut finalement être suffisante.

2.1.2.8 Attaques sur les mots de passe des routeurs

L'identification par mots de passe peut être sécuritaire si elle est chiffrée et que les mots de passe sont élaborés (c'est-à-dire qui emploient les différents caractères du clavier, lettres, chiffres et symboles). L'emploi de mots de passe plus courts n'utilisant que des lettres ou des chiffres peuvent être cassés de plus en plus aisément, et remettent en cause la valeur de l'identification.

Les attaques par dictionnaire consistent à essayer une liste de mots possibles, composée des mots usuels (noms communs, prénoms, etc.), utilisant éventuellement quelques règles complémentaires comme la variation de la casse des mots, la répétition des mots, l'ajout d'un chiffre à la fin d'un mot, etc. Pour augmenter les chances de trouver le mot de passe, il peut être nécessaire de faire quelques recherches sur la personne ayant créé

le mot de passe. Par exemple, utiliser un dictionnaire dans une langue plutôt qu'une autre selon la nationalité de la personne, les dates de naissance des différents membres de la famille, etc.

Les attaques par force brute sont différentes. Elles utilisent toutes les combinaisons possibles de caractères afin de trouver le mot de passe. Très efficaces si le mot de passe est constitué d'un nombre raisonnable de caractères (moins de huit), elles peuvent nécessiter un temps de calcul très important si le mot de passe est long. Par exemple, il existe $5{,}4.10^{12}$ mots de passe différents utilisant uniquement neuf lettres minuscules. Un ordinateur étant capable de tester jusqu'à quelques millions de mots de passe à la seconde, il faut en théorie jusqu'à 10^6 secondes (presque 12 jours) pour tester toutes les possibilités, ce qui est déjà beaucoup malgré le peu de caractères utilisés (les 26 lettres minuscules). Par contraste, il ne faut qu'une centaine de secondes pour tester toutes les possibilités de mots de passe de six lettres minuscules. D'où l'importance d'utiliser des mots de passe longs et utilisant tout type de caractères.

Afin d'empêcher un attaquant de deviner le mot de passe d'un utilisateur, il faut absolument restreindre le nombre d'essais autorisés. Au-delà d'un certain nombre d'essais erronés, le compte doit être bloqué. De nombreux sites Internet comme ceux des banques offrent cette possibilité, mais ce n'est pas toujours le cas : la plupart des autres sites web, les comptes utilisateurs dans Windows (par défaut), etc. ne sont pas limités en nombre d'essais erronés. Il est alors possible, surtout si le mot de passe est faible, de le casser dans un temps raisonnable. Des pratiques similaires, c'est-à-dire la restriction du nombre d'essais et l'utilisation de mots de passe complexes, devraient être réalisées pour empêcher les attaques par dictionnaire ou par force brute sur l'interface de console des routeurs, si celle-ci est accessible.

2.1.2.9 Attaques sur clés de chiffrement

Au lieu de deviner un mot de passe pour se connecter à un compte donné, il peut être intéressant à un attaquant de deviner une clé de chiffrement afin d'avoir accès à des informations confidentielles. Il existe deux types de chiffrement, soit symétrique et asymétrique.

La cryptographie symétrique consiste à utiliser une même clé pour le chiffrement et le déchiffrement. Son avantage est la rapidité de chiffrement due à la petite taille des clés, son inconvénient est la communication de la clé à la tierce partie, habituellement réalisée en utilisant la cryptographie asymétrique. Les algorithmes les plus courants sont DES (*Data Encryption Standard*), 3DES (*Triple DES*), AES (*Advanced Encryption Standard*). Si l'attaquant parvient à obtenir la clé de chiffrement, il peut alors prendre connaissance de tout message chiffré.

La cryptographie asymétrique est différente : elle utilise le principe de clé publique et clé privée, la première étant donnée à tous et sert à chiffrer les données alors que la seconde n'est connue que d'une seule personne et permet de les déchiffrer. Plus lente que la cryptographie symétrique, elle est par contre plus simple à utiliser, aucun échange secret de clé n'étant nécessaire. L'algorithme le plus connu est RSA (*River, Shamir, Adleman*, du nom des inventeurs). La nécessité d'utiliser de longues clés vient du fait que les clés sont générées mathématiquement et non aléatoirement. La robustesse des algorithmes de cryptographie asymétrique vient de la difficulté à factoriser de très grands nombres. De plus, la longueur de la clé est telle qu'il est impossible de procéder par force brute.

Les algorithmes de cryptographie symétrique et asymétrique sont à l'épreuve d'un attaquant puisqu'ils imposent une taille minimale de clé garantissant la sécurité (aujourd'hui respectivement de l'ordre de 128 et 2048 bits). Les seules attaques

possibles visent la cryptographie symétrique au niveau de l'échange de la clé unique, lequel doit être réalisé avec soin ; pour la cryptographie asymétrique des attaques de type *Man in the Middle*. Des infrastructures de gestion de clés (PKI, *Public Key Infrastructure*) doivent être employées pour être sûr de faire usage de la bonne clé et de ne pas se laisser berner par un intrus.

2.1.2.10 Attaques utilisant l'ingénierie sociale

Les attaques sur un réseau ne s'effectuent pas uniquement par l'exploitation de failles ou d'erreurs de conception. L'être humain est parfois bien malgré lui un participant actif à l'attaque, grâce aux droits qu'il possède et que l'attaquant n'a pas. L'ingénierie sociale permet d'obtenir de l'information telle le mot de passe d'un routeur PE ou de lancer directement des attaques depuis l'intérieur.

L'ingénierie sociale regroupe les différentes méthodes qu'un attaquant utilise pour soutirer de l'information à un utilisateur légitime, comme son nom d'utilisateur et son mot de passe. Il existe une multitude de façons de berner ce dernier : l'attaquant peut se faire passer pour l'administrateur réseau et demander directement le mot de passe de l'utilisateur en prétextant une urgence, pénétrer dans les locaux de l'entreprise en se faisant passer pour un consultant et se faire ainsi ouvrir la porte par un employé peu scrupuleux (ce qui permet de rechercher des informations à l'intérieur, fouiller dans les corbeilles, etc.), appeler le comptoir d'assistance aux utilisateurs et indiquer l'oubli de son mot de passe pour en obtenir un nouveau, regarder au dessus de l'épaule d'un employé ou espionner avec des jumelles, etc.

Le plus surprenant est que la plupart des attaques d'ingénierie sociale fonctionnent avec de nombreux employés. Des politiques strictes de sécurité dans l'entreprise doivent être appliquées, interdisant par exemple de révéler son mot de passe, même aux administrateurs réseaux, d'ouvrir la porte à des inconnus même lorsque ceux-ci semblent

soignés et peu suspects, etc. Car l'ingénierie sociale utilise justement le fait qu'un individu moyen se méfierait beaucoup plus d'une personne mal habillée qui ne semblerait pas avoir de rapport avec l'entreprise que d'une personne très bien habillée et sympathique qu'il va chercher à aider – c'est la nature humaine. Le plus connu des pirates en ingénierie sociale se prénomme Kevin Mitnick. Celui-ci a écrit plusieurs livres, dont *L'art de la supercherie*, relatant de nombreuses techniques d'ingénierie sociale (Mitnick et Simon, 2002).

2.1.2.11 Remise en cause du modèle TCP/IP

Chaque couche du modèle TCP/IP peut être sujette à attaque. Les paragraphes précédents présentaient des attaques concernant le médium physique, la couche liaison de données, la couche réseau, la couche transport et la couche application. Le principe des modèles en couches, qu'il s'agisse du modèle OSI ou du modèle TCP/IP, est de donner un rôle et des fonctions indépendants à chaque couche. Par exemple, la couche physique s'occupe de transmettre les bits sur le réseau (optique, cuivre, sans-fil, etc.), la couche réseau permet entre autres l'adressage logique, la détermination d'un chemin et l'acheminement des paquets, et ainsi de suite. Chaque couche N établit une communication avec les couches adjacentes N-1 et N+1 dans le but de pouvoir communiquer avec la couche N d'un système distant.

Si au niveau fonctionnel le tout est correct, il n'en va pas de même en ce qui concerne l'aspect sécuritaire du modèle en couches. Les protocoles des différentes couches ne se préoccupent pas de savoir si les données reçues des couches inférieures sont valides ou non, en fait, elles ont confiance en supposant que les couches inférieures sont sûres.

Lorsqu'une attaque se produit à une couche basse (physique, liaison, réseau), les couches supérieures vont en subir les effets car ces dernières n'intègrent pas par défaut de mécanisme permettant de vérifier l'intégrité des données. La couche application

devrait le plus souvent possible employer des protocoles de chiffrement et d'authentification lorsque les données sont sensibles.

Le travail de sécurité doit toutefois s'effectuer à tous les niveaux. Parallèlement au modèle de réseau OSI, il existe un modèle d'architecture de sécurité OSI (ISO 7498-2), qui décrit les requis permettant de garantir la sécurité d'un système d'information : authentification, contrôle d'accès, non répudiation, intégrité des données, confidentialité, disponibilité et signatures électroniques.

2.1.3 Bilan

En dressant un bilan, il existe un grand nombre d'attaques qui peuvent être portées sur un réseau MPLS. Afin de pouvoir attaquer l'intégrité des tables, il est nécessaire d'attaquer en premier lieu le routeur PE, entrée du réseau MPLS. Plusieurs méthodes permettent y parvenir, de l'écoute à l'ingénierie sociale, du scan de port à la recherche des mots de passe.

Les vulnérabilités permettant les attaques présentées peuvent être classées en trois types, selon leur origine (Canavan, 2001) :

- mauvaise conception des systèmes ou des logiciels,
- mauvaise implémentation des systèmes, configuration erronée,
- mauvaise gestion des équipements, piètre définition des rôles et des procédures.

Ces trois types de vulnérabilités correspondent aux différentes phases du cycle de vie d'un système ou d'un programme : sa conception, durant laquelle des brèches peuvent être créées et ouvrir des portes dérobées, par exemple ; son implémentation par un constructeur suivant maladroitement la norme ; sa configuration par l'administrateur réseau laissant les mots de passe par défaut ou donnant trop de droits à certains utilisateurs ; sa maintenance en oubliant de réaliser des audits de sécurité, en ne

changeant pas les mots de passe régulièrement ou en ne définissant pas les responsabilités de chacun.

La sécurité est un tout, qui doit être appliqué à chaque phase du cycle de vie. Des audits doivent permettre de contrôler que les procédures de sécurité sont cohérentes, des analyses de risques quantitatives et qualitatives peuvent aider à déterminer ce qui doit être protégé prioritairement de ce qui est moins important, déterminant un plan architectural des investissements à réaliser pour la sécurité (Panko, 2004).

La défense en profondeur est le premier principe de conception d'une architecture de sécurité. Il doit y avoir plusieurs niveaux de défense, permettant de limiter l'impact d'une faille sur une couche défensive, et laissant le temps de réagir lorsqu'une intrusion est détectée. Un autre principe est d'assurer une diversité des fournisseurs de solutions de sécurité. Chaque fournisseur ayant ses forces et ses faiblesses, combiner des produits de différents fournisseurs permet de joindre leurs forces et de réduire leurs faiblesses respectives. L'utilisation de pare-feux et de détecteurs d'intrusion est nécessaire pour réaliser une défense en profondeur.

Afin de simplifier la mise en place de la sécurité, des standards sont disponibles. Les *Critères Communs* (ISO/CEI 15408), basés sur trois anciens standards européen (ITSEC, *Information Technology Security Evaluation Criteria*), canadien (CTCPEC, *Canadian Trusted Computer Product Evaluation Criteria*) et américain (TCSEC, *Trusted Computer System Evaluation Criteria*) – aussi connu sous le nom du livre orange. Ils peuvent, en association avec des autorités en sécurité tel le CERT, aider à concevoir une architecture sécuritaire, déterminer le niveau de sécurité atteint et se tenir au courant des nouvelles vulnérabilités.

2.2 Analyse de la sécurité des VPN sur MPLS

La possibilité de créer des réseaux privés virtuels sur MPLS performants a été rendue possible par la simplicité de leur conception : la notion de routeurs virtuels, la connectivité de chaque VPN à l'aide d'imports/exports de routes, l'absence de chiffrement des données.

Afin de vérifier que l'architecture des VPN sur MPLS ainsi que son implémentation sont correctes, plusieurs analyses ont été réalisées par des experts en sécurité. La RFC4381 (Behringer, 2006) réalise une analyse de la sécurité des VPN utilisant BGP/MPLS, principalement au niveau architectural, considérant toutefois aussi leur implémentation et leur fonctionnement. Elle suppose que le réseau MPLS est sûr parce que bien configuré et qu'il est normal de faire confiance au fournisseur de service administrant ce réseau. Ce n'est pas une gageure, car il en va de même pour les réseaux ATM/FR que tout le monde prétend sécuritaires.

Le principe de base de sécurité est que le trafic d'un VPN ne doit jamais pouvoir entrer dans un autre VPN. Le cœur doit quant à lui être invisible du monde extérieur comme c'est le cas pour les architectures de niveau 2 équivalentes comme ATM/FR.

Cette partie analyse les différents vecteurs d'attaques sur le réseau MPLS. Elle considère les types d'attaques énoncés dans la partie 2.1.2 s'appliquant aux VPN sur MPLS. Les failles applicatives telles que les bugs du système d'exploitation des routeurs sortent du cadre de cette étude, parce que d'une part il n'est pas possible d'accéder au code du système d'exploitation des routeurs pour l'analyser, et d'autre part, des bugs dans une implémentation peuvent être colmatés par une rustine contrairement à des erreurs de conception qui nécessitent une mise à jour majeure.

2.2.1 Une attaque directe impossible

Une attaque directe consisterait à injecter des paquets à partir d'un VPN dans le réseau, qui pourraient s'introduire dans un autre VPN par une faille de l'architecture ou de l'implémentation de MPLS.

BGP permet aux VPN dans MPLS d'utiliser des espaces d'adressage se chevauchant, ceci grâce aux *route distinguishers* définis dans le chapitre 1. Le routage dans un réseau MPLS utilisant BGP est séparé pour chaque VPN par la notion de routeurs virtuels. Le trafic est quant à lui maintenu séparé sur le plan de données grâce à l'étiquette VPN ajoutée par le routeur PE *ingress*. De ce fait, ayant une séparation de l'adressage, du routage et du trafic, il est possible d'admettre que les MPLS/VPN utilisant BGP offrent la même sécurité que les VPN de couche 2 et rendent impossible la pénétration directe dans un autre VPN.

Les attaques ayant pour source le réseau MPLS sont dangereuses et délicates, car au sein du réseau MPLS il est possible d'écouter sur le réseau, de renifler le trafic, de l'intercepter, de le modifier et d'en injecter sans que les utilisateurs du réseau n'en soient seulement conscients étant donné que ni les données ne sont chiffrées ni les échanges protégés. Enno Rey, consultant chercheur spécialisé en sécurité a montré à la conférence Blackhat Europe 2006 qu'une attaque par mystification des étiquettes était possible et simple, et qu'une attaque par modification de session MP-BGP était envisageable, bien que plus difficile (Rey, 2006). Nonobstant, toutes ces attaques exigent un accès au cœur du réseau MPLS.

Les menaces internes peuvent être dues à une mauvaise configuration volontaire ou involontaire. Par exemple, une erreur involontaire de configuration dans la définition des *route targets* peut avoir pour effet d'exporter les routes d'un VPN vers un autre VPN et donc de briser l'intégrité des données. Ce genre d'erreur peut de plus être difficile à

détecter pour l'un des deux VPN (l'autre perdant sa connectivité normale, donc le remarquant rapidement). Cependant les outils de configuration automatique permettent d'éviter ce genre d'erreur.

Dans le cas des erreurs volontaires, où un opérateur va délibérément créer une faille dans le réseau, il n'y a pas vraiment d'autre solution que de s'assurer de la responsabilité et de l'intégrité des employés. Car les conséquences peuvent être catastrophiques, puisque pas nécessairement détectables.

Donc, si le réseau est convenablement configuré, une attaque d'origine interne ne peut venir que du fournisseur de service. Or comme il est présupposé – peut-être à tort! – que le fournisseur de service est un tiers de confiance, les attaques de ce type sont présumées inexistantes. Si un client ne fait pas confiance au fournisseur de service, alors il doit utiliser IPsec pour protéger son trafic. Bien que cela n'empêcherait pas de briser l'étanchéité des VPN, le trafic ne serait toutefois pas « compatible » car chiffré et donc illisible.

2.2.2 Attaques indirectes

Puisque la conception des VPN sur MPLS empêche une pénétration directe dans un VPN, un intrus devrait trouver un autre moyen pour parvenir à ses fins. Une méthode consisterait à attaquer le cœur du réseau MPLS dans un premier temps, puis pénétrer les VPN de ce point. Les points suivants vont être considérés dans cette partie :

- Attaque sur le cœur du réseau
- Mystification d'étiquettes MPLS ou d'adresses IP,
- Déni de service,
- Attaques sur le lien CE-PE,
- Attaques sur les protocoles de signalisation

2.2.2.1 Attaque sur le cœur du réseau

Avant de pouvoir attaquer le cœur du réseau, un attaquant doit savoir ce qui s'y trouve exactement. Pour cela, il va tenter des attaques de reconnaissance, difficiles à détecter car n'ayant pas d'impact négatif sur le réseau. Dans un réseau classique, l'utilisation de journaux d'évènements représente une des seules solutions pour détecter ce type d'attaque. Afin d'éviter le succès de telles attaques, il faut masquer le réseau au maximum. Or l'avantage du réseau MPLS cœur est d'être invisible de l'extérieur. Les seuls équipements visibles sont les routeurs PE, il faut donc sécuriser les interfaces externes de ces routeurs grâce aux listes d'accès, pour ne pas accepter de paquets à destination du cœur. La reconnaissance d'un réseau MPLS est donc loin d'être une chose aisée.

Les deux seules exceptions à cette invisibilité sont d'une part le paramètre *MPLS traceroute* qui est activé par défaut depuis les versions supérieures à 12.0(9)ST et 12.1(3)T de l'IOS Cisco, et l'utilisation de services Internet sur les routeurs du cœur (*cf.* Connectivité Internet, section 3.2). Par défaut les PE copient le champ TTL (Time To Live) du paquet IP dans l'entête MPLS. Chaque routeur P du cœur va décrémenter ce champ au passage d'un paquet, le PE de sortie recopiera la valeur résiduelle du TTL dans l'entête IP. Un *MPLS traceroute* va permettre de révéler de l'information sur la topologie du réseau MPLS. Il est important de le désactiver à l'intérieur du réseau MPLS pour éviter de dévoiler le contenu du réseau cœur.

Même en connaissant ou en devinant l'adresse d'un routeur P, les attaques vers le cœur du réseau ne sont pas réalisables, y compris en l'absence de liste d'accès. À cause de la séparation des espaces d'adressage effectuée par les routeurs PE, les adresses IP sont traduites en adresses VPN-IP qui n'ont une signification que pour le VPN auquel elles appartiennent. Les routeurs PE traiteraient alors des paquets à destination du cœur comme appartenant à l'espace d'adressage du client, donc à destination d'un des sites du

VPN et non du réseau MPLS. Une fois entrées dans le réseau MPLS, les données sont mises en tunnel jusqu'au routeur PE de sortie. Le seul point d'entrée est l'interface externe des PE, liée au CE.

Il y a deux possibilités d'attaques au niveau du PE. D'une part, attaquer le routeur PE directement, et d'autre part attaquer les mécanismes de signalisation de MPLS. Afin d'empêcher des attaques sur les routeurs PE, des listes d'accès doivent être adoptées, rendant inefficace tout scan de port. Ces listes d'accès doivent entre autres restreindre les droits d'accès aux ports de configuration des PE. De plus, seul SSH devrait être employé pour la configuration, étant plus sécuritaire que l'accès par *telnet*. Les mots de passe ne doivent jamais être ceux par défaut, ni faciles à deviner ou encore les mêmes partout.

Le type de routage le plus favorable entre CE et PE est le routage statique. Aucune route ne peut être introduite par un intrus puisqu'il n'y a pas de mise à jour du routage dans un tel cas. Aucun paquet ne doit donc avoir le PE comme destination si le routage statique est utilisé.

Le routage dynamique est plus simple à configurer, particulièrement en cas de changement d'adressage. En raison de sa facilité de mise à l'échelle, eBGP (*exterior Border Gateway Protocol*) est recommandé en tant que protocole de routage dynamique, et dans tous les cas l'authentification est primordiale. BGP propose des mécanismes tels que la commande *maximum-prefix* qui limite le nombre de routes que le routeur doit accepter afin d'éviter un déni de service par surconsommation des ressources du processeur ou de la mémoire. Dans le cas où BGP n'est pas supporté, des IGP (*Interior Gateway Protocol*) tels qu'EIGRP (Enhanced Interior Gateway Routing Protocol), OSPF ou RIPv2 peuvent être utilisés. La RFC4577 suggère dans ce cas l'utilisation d'OSPF comme protocole de routage CE-PE (Rosen, Psenak et Pillay-Esnault, 2006).

Quel que soit le protocole de routage dynamique utilisé, le seul trafic pouvant se diriger au PE doit être lié à ce protocole de routage. Ce dernier doit être protégé, grâce à des listes d'accès avancées ainsi que l'authentification des pairs par MD5 (*Message Digest 5*). La section 2.2.2.5 donne des détails supplémentaires sur cette possibilité. L'authentification des participants est aussi nécessaire pour éviter que les routeurs CE ne puissent mystifier l'appartenance à un VPN donné ou réaliser du déni de service en inondant le PE de mises à jour de routage. Le chapitre 4 analysera plus en détail le protocole de routage utilisé pour l'échange de routes VPN dans le réseau MPLS, MP-BGP.

Enfin, les attaques peuvent aussi se diriger vers le centre de gestion du réseau, le NOC (*Network Operations Center*), et l'équipement qui lui est lié, comme les stations de gestions, les serveurs FTP et TFTP, etc. Le centre de gestion peut être relié à Internet pour permettre une administration à distance. Le risque est ici très grand puisque si un intrus réussit à atteindre le centre de gestion, il devient en quelque sorte le « maître » du réseau, pouvant à sa guise changer la configuration des PE, et permettre ainsi d'accéder à des VPN depuis l'extérieur. L'utilisation de listes d'accès et de communications chiffrées est essentielle pour que différents VPN ne puissent être interconnectés au travers du NOC.

2.2.2.2 Mystification d'étiquettes MPLS ou d'adresses IP

Une autre attaque possible est la mystification de paquets comportant des étiquettes MPLS ou VPN. S'il était possible d'introduire des paquets labélisés (étiquetés) dans le réseau MPLS, les routeurs les achemineraient selon leur étiquette MPLS, cela pourrait éventuellement briser l'étanchéité des VPN. Il faudrait néanmoins deviner les étiquettes MPLS et VPN à utiliser. Heureusement, comme l'interface entre le CE et le PE est purement IP, il n'y a pas circulation de paquets labélisés à cet endroit. Il est donc important que les routeurs PE n'acceptent jamais de paquets labélisés en provenance des

CE, excepté dans certaines configurations particulières, telle celle de plusieurs réseaux MPLS reliés entre eux (architecture *Inter-AS, cf. 2.2.5.1*), ainsi que celle des réseaux MPLS hiérarchisés (*Carrier's carrier, cf. 2.2.5.2*).

Le cas de la mystification d'adresses IP ne représente pas en soi une attaque valide, car quelle que soit l'adresse de destination du paquet entrant dans un routeur PE, ce dernier effectue à l'entrée du réseau MPLS une séparation des espaces d'adressage avec les *route distinguishers*. Un utilisateur ne peut donc pas attaquer un autre VPN, mais seulement un autre utilisateur de son propre VPN, ce qui ne constitue pas une menace remettant en cause l'étanchéité de l'architecture MPLS/VPN.

2.2.2.3 Déni de service

Les attaques de type déni de service, possibles sur les routeurs PE, ne remettent pas en cause l'intégrité des données, par contre ils vont avoir pour conséquence d'empêcher le fonctionnement correct et normal des VPN, en termes de garantie de niveau de service et de performances. Le dimensionnement correct du réseau associé à des politiques de *policing/shaping* doit permettre d'éviter le déni de service en empêchant les clients de chaque VPN d'émettre à un rythme supérieur à celui souscrit. En outre, les routeurs récents commencent à intégrer des fonctionnalités de ressources séparées par VPN, autrement dit si un client d'un VPN émet une attaque de déni de service, il ne compromettra que son propre VPN et n'affectera pas les performances des autres VPN.

2.2.2.4 Attaques sur le lien CE-PE

Des chercheurs (Ren, Feng et Ma, 2004) de l'Académie chinoise des sciences de Pékin ont montré que le point faible de l'architecture MPLS/VPN est le lien CE-PE. Bien qu'ils concèdent qu'il est impossible d'injecter des paquets labélisés dans le réseau MPLS, les attaques sur le lien CE-PE sont possibles. Elles ne permettent toutefois pas de rejoindre un autre VPN, à cause des VRF propres à chaque VPN présents dans les PE

(ce qui est valable uniquement si un seul VPN utilise le lien CE-PE). Par contre, rien n'empêche un intrus se connectant entre un CE et un PE d'attaquer les clients du VPN concerné, le trafic étant à cet endroit purement IP.

Le fait que MPLS ne soit utilisé en général que sur le réseau du fournisseur de service au niveau de sa dorsale crée un lien CE-PE vulnérable. Ils suggèrent donc une solution améliorée de VPN sur MPLS utilisant IPSec, avec entre autres une autorité de certification et de distribution de clé de sécurité, en l'occurrence IKE (Internet Key Exchange). Les simulations réalisées montrent que plus le degré de sécurité est élevé (aucun chiffrement, puis ESP (*Encapsulating Security Payload*) seul, et enfin ESP + AH (*Authentication Header*)), plus le délai est important et le débit dans le réseau diminué. Il faut donc faire un compromis entre sécurité et performances, selon les besoins des clients.

Le problème du lien CE-PE est donc d'être éventuellement accessible à un intrus réalisant une attaque de type *Man in the Middle*. L'idéal serait de ne pas utiliser d'adressage entre le CE et le PE, ce qui empêcherait toute attaque au niveau 3. Mais des limitations telles que l'impossibilité d'effectuer un *ping* pour vérifier le fonctionnement du lien sont trop contraignantes pour permettre cette solution.

L'authentification par MD5 des protocoles de routage doit permettre d'empêcher toute intervention sur ceux-ci, avec les réserves énoncées dans la section 2.2.2.5. Si un seul VPN utilise le lien CE-PE, au pire l'intrus pourra écouter les données transmises, injecter des données dans le VPN en question mais pas attaquer les autres VPN de ce point à cause de la séparation des espaces d'adressage. Si par contre plusieurs VPN se partagent le lien CE-PE, il peut s'avérer nécessaire de les protéger par du chiffrement (IPSec). Aussi, l'utilisation de VLAN (*Virtual Local Area Network*) permet de séparer au niveau 2 le trafic des différents VPN. Il est cependant important dans ce cas d'éviter que l'intrus puisse se placer entre le CE et le PE, pour cela il ne faut pas utiliser de

nœuds de niveau 2 entre CE et PE. Par ailleurs, si les multiples VPN entre CE et PE sont mis en œuvre pour plusieurs clients, le CE doit absolument être administré par le fournisseur du réseau MPLS, et non par les clients. La zone de confiance va dans ce cas inclure le routeur CE.

Si la confidentialité est importante pour le client, il est possible comme suggéré par Ren, Feng et Ma d'utiliser IPsec entre les CE. Cela permet d'éviter toute révélation d'information à un intrus écoutant le lien CE-PE, et éventuellement, si le client ne fait qu'une confiance relative au fournisseur de service, de protéger ses données de ce dernier. Toutefois des dégradations en termes de performances sont à accepter en contrepartie.

Les paquets échangés sur le lien CE-PE étant purement IP et non MPLS, les problèmes qui peuvent y survenir sont les mêmes que sur n'importe quel lien IP. Au niveau de la couche 2, les risques existent (*ARP attacks*, *VLAN trucking attacks*, etc.) et c'est pourquoi même s'il y a pour chaque risque des mesures de protection de la couche 2 qui doivent être prises en compte, il est fortement déconseillé d'utiliser par exemple entre CE et PE des équipements tels que des nœuds d'échange Internet. L'étude de ces risques sort du cadre de ce mémoire, de la documentation à ce sujet étant disponible sur Internet.

2.2.2.5 Attaques sur les protocoles de signalisation

Les protocoles de routage étant les seuls autorisés à dialoguer avec tous les éléments du réseau cœur (routeurs PE, P), il est essentiel de les sécuriser afin d'empêcher tout intrus d'injecter des mises à jour de routes erronées, ce qui aurait pour effet de compromettre le fonctionnement du réseau, et éventuellement l'intégrité des données des clients VPN.

Les routeurs voisins doivent donc s'authentifier entre eux avant d'accepter du trafic de routage. Pour cela, l'authentification avec MD5 est fortement conseillée. Celle-ci est

possible pour BGP (Heffernan, 1998), OSPF (Murphy, Badger et Wellington, 1997) et RIPv2 (Baker et Atkinson, 1997). Les protocoles de routage ne sont pas les seuls à pouvoir être authentifiés, le protocole de distribution LDP utilise lui-aussi MD5 pour prévenir de la mystification d'étiquettes.

L'avantage de MD5 est que seule une empreinte composée de la clé et d'un message est transmise, sans cette clé il est impossible de recalculer une empreinte. L'inconvénient est que MD5 n'est plus sûr au niveau cryptographique : dès 1996, des failles ont pu être trouvées (Dobbertin, 1996) ; en 2004 MD5 a été considéré comme cassé après découverte de collisions réelles (c'est-à-dire qu'une même empreinte peut être obtenue en utilisant deux messages différents) par une équipe chinoise (Wang et Yu, 2005).

D'autres mécanismes peuvent être utilisés en plus de l'authentification afin de sécuriser les protocoles de routage. BGP propose un mécanisme de contrôle par TTL (Gill, Heasley et Meyer, 2004) afin de protéger les sessions eBGP d'attaques de déni de service par surcharge sur les routeurs. En vérifiant que les paquets de mise à jour des protocoles de routage possèdent une valeur de TTL supérieur à un minimum fixé, cela empêche tout paquet IP de routage BGP provenant d'un élément distant, extérieur au réseau MPLS, d'être considéré comme valide.

2.2.3 Des points de vue extérieurs

Même si le nombre d'articles sur les VPN sur MPLS n'est pas très important, certains articles sont assez intéressants. En voici deux qui présentent des points de vue différents, considérant dans le premier article la sécurité obtenue par application de la RFC2547 sur les réseaux privés virtuels sur MPLS et la nécessité d'y apporter des modifications, et l'impact de cette technologie sur les performances du réseau ainsi qu'une comparaison avec les VPN sur IPsec dans le second article.

2.2.3.1 Intégrité des VPN

Randy Bush et Timothy G. Griffin, qui contrairement à Behringer, ne sont pas liés à Cisco, ont réalisé une étude (Bush et Griffin, 2003) portant leur attention sur la notion d'intégrité des informations circulant dans les VPN, afin de garantir une isolation entre les différents tunnels VPN. Cette notion d'intégrité signifie que la spécification est correcte et que l'implémentation est bien réalisée. Les erreurs humaines qui peuvent intervenir (mots de passe par défaut, etc.) ne font toutefois pas partie de leurs considérations. Leur but était de trouver des ambigüités dans la spécification de la RFC2547 (Rosen et Rekhter, 1999), la précédente version de la RFC4364, et de proposer quelques solutions alternatives à celles-ci.

La RFC2547 propose d'isoler les VPN en utilisant des tables d'acheminement par site et l'assurance de l'adresse source. Mais cette isolation ne peut être garantie en tout temps. Afin de résoudre ce problème, l'utilisation de tables d'acheminement par VPN fut proposée, elle a d'ailleurs été adoptée dans la RFC4364.

Bush et Griffin suggèrent, afin d'améliorer l'intégrité des VPN, d'employer des tables d'acheminement entrantes et sortantes pour chaque interface, ou alors une table d'acheminement étendue pour chaque interface, ne transmettant le trafic vers la destination que s'il provient d'une source définie. Ce dernier type de table constitue cependant un sérieux challenge dans son implémentation, de par le nombre d'entrées. Toutefois, l'isolation permise par les solutions suggérées par les auteurs correspond à celle obtenue en utilisant des tables d'acheminement par VPN.

Bush et Griffin ont remarqué un point intéressant : comme la spécification (RFC2547) était à l'époque incomplète, les manques de la spécification étaient plus ou moins rattrapés par les implémentations de chaque fabricant. C'est pourquoi – en particulier avant la sortie de la RFC4364 plus complète – les différents produits sur le marché

n'étaient pas tous équivalents et nécessitaient d'être individuellement testés pour en vérifier les propriétés, et donc la garantie de l'isolation des VPN.

Outre les considérations de performances quant à la mise à l'échelle du réseau MPLS et les effets de la quantité de tunnels VPN sur le fonctionnement du réseau, un point soulevé par les auteurs ayant trait à la sécurité et pouvant être important concerne le temps de convergence des protocoles de routage comme BGP en cas de modifications sur le réseau. Il est important que cette convergence soit rapide, pour éviter d'obtenir des chemins LSP rompus et une isolation des VPN brisée.

2.2.3.2 Performances des VPN sur MPLS

Palmieri a réalisé une étude (Palmieri, 2003) comparant les performances, forces et faiblesses des VPN utilisant IPsec ou MPLS.

D'après l'auteur, le point qui pose problème et qui peut se révéler négatif pour les VPN basés sur MPLS est la nécessité de pouvoir faire une totale confiance au fournisseur de service. Cela est aussi vrai pour ATM. Par contre, parmi les avantages, la latence est très réduite car il n'y a avec MPLS aucune encapsulation importante ni aucun chiffrement des données.

La sécurité de MPLS/VPN est obtenue par l'approche distincte plan de données / plan de contrôle. Le plan de données empêche un paquet appartenant à un VPN d'en sortir et au trafic extérieur d'y rentrer, notamment en examinant l'étiquette du paquet. Le plan de contrôle permet de s'assurer que les clients ou intrus ne puissent injecter des routes dans le réseau MPLS, il protège aussi les routeurs en empêchant tout accès non autorisé.

L'auteur précise toutefois que si la séparation de trafic à la couche 2.5 (MPLS) et les chemins réservés ne sont pas considérés comme une sécurité suffisante pour le client, ou

que la confidentialité est critique même vis-à-vis du fournisseur de service, alors l'emploi d'IPsec est fortement conseillé.

Des tests fonctionnels ont été réalisés par Palmieri pour tenter de montrer que MPLS/VPN est aussi sûr que les VPN classiques utilisant le chiffrement. Des paquets ont par exemple été injectés dans un VPN à destination d'un autre VPN sans que ce dernier ne soit touché. L'invisibilité du réseau a été testée quant à elle en réalisant un *traceroute* montrant l'impossibilité d'atteindre les routeurs du réseau MPLS.

Des tests de performances ont permis de montrer que l'approche MPLS/VPN est en terme de latence beaucoup plus rapide que IPsec, surtout avec de gros paquets, et au même niveau qu'une transmission classique de paquets IP. De même, MPLS/VPN perd beaucoup moins de paquets qu'IPsec. L'utilisation du processeur des CE est augmentée uniquement en utilisant IPsec, pas avec MPLS. Par contre, et ce résultat est plus surprenant, la bande passante mesurée de bout en bout est similaire avec IPsec et avec MPLS/VPN, mais bien moindre (à peine un tiers) que sans encapsulation et chiffrement. Cela est étonnant, car MPLS ne fait qu'ajouter un entête de 4 octets quand IPsec ajoute 20 octets. La surcharge est donc supérieure avec IPsec, et cela ne se traduit pas dans les résultats.

La conclusion de l'auteur est que MPLS/VPN est très bon en termes de performances, fiabilité, mise à l'échelle et offre une sécurité comparable aux VPN utilisant ATM/FR, ce qui, en faisant confiance au fournisseur de service, peut être considéré aussi sécuritaire que des tunnels chiffrés par IPsec.

2.2.4 Comparaison avec ATM/FR

Plusieurs acteurs de la communauté scientifique (Miercom, 2001), (Cisco, 2004) reconnaissent qu'un réseau MPLS proposant uniquement des VPN, c'est-à-dire sans

accès partagé à Internet, offre un niveau de sécurité similaire aux VPN de niveau 2 utilisant ATM et FR parce que les raisons qui permettent de considérer les technologies ATM/FR comme sûres s'appliquent aussi à MPLS :

- la séparation de l'espace d'adressage, du routage et des données
- l'invisibilité du réseau cœur depuis l'extérieur
- un réseau résistant aux attaques

La grande différence entre MPLS/VPN et ATM/FR est qu'ATM et Frame Relay fonctionnent à la couche 2, alors que MPLS utilise la couche 3. La séparation des VPN dans ATM est réalisée grâce à l'utilisation de la couche 2 dans le cœur, ce qui permet aux informations de couche 3 d'être complètement ignorées ; alors que MPLS utilise les VRF afin de séparer les VPN à la couche 3.

La séparation de l'adressage, du routage et du trafic vient naturellement dans ATM/FR car la couche réseau n'est jamais consultée lors du transport des trames, la seule information sollicitée pour la commutation des trames étant le champ DLCI pour FR ou le couple VCI/VPI pour ATM. Dans MPLS, la séparation de l'adressage est réalisée par les *route distinguishers*, permettant d'utiliser le même espace d'adressage dans plusieurs VPN disjoints. La séparation du routage et du trafic est quant à elle permise par le principe de routeurs virtuels, les tables de routages par VPN (c'est-à-dire les VRF), les règles d'import/export au sein des VRF et par l'échange des routes par MP-BGP entre les routeurs PE.

L'invisibilité du réseau est permise dans ATM/FR par l'absence de connectivité au niveau de la couche réseau entre le client et les commutateurs ATM/FR. Dans MPLS, les clients ne connaissent que l'adresse du PE, les routes du réseau n'étant pas diffusées car leur connaissance est inutile au bon fonctionnement des VPN. De plus, si la fonction MPLS *traceroute* est désactivée, le réseau MPLS entier sera vu comme un seul saut par

les clients. Cette invisibilité n'est toutefois pas possible dans certaines configurations d'accès partagé à Internet (*cf.* section 3.2).

Enfin, ATM/FR offre une bonne résistance aux attaques d'intrusion car une attaque ne peut atteindre que les participants du VPN duquel est partie l'attaque, le réseau ne faisant que diriger les trames en fonction du champ DLCI ou du couple VCI/VPI sans consulter les couches supérieures. C'est assez similaire pour MPLS, les routeurs P ne consultant pas l'adresse IP pour effectuer l'acheminement des paquets mais plutôt les étiquettes MPLS. Une fois entré dans le réseau un paquet ne peut que ressortir dans le même VPN que celui par lequel il est entré. Donc toute attaque ne peut toucher qu'un VPN, pas le réseau cœur. Les attaques indirectes doivent passer par les PE, or ceux-ci sont protégés par des listes d'accès.

Les problèmes de configuration des PE énoncés dans MPLS sont tout aussi valables pour ATM/FR, si un circuit est mal configuré par exemple.

Le seul endroit où ATM/FR a un avantage sur MPLS est dans leur possibilité de réaliser une communication de CE à CE, utilisant par exemple le protocole CDP (*Cisco Discovery Protocol*). Cette communication est permise par l'aspect point à point *full-mesh* des liaisons ATM/FR, ce qui n'est pas le cas des VPN sur MPLS. La mise à l'échelle est plus facile avec MPLS, mais ce dernier ne permet pas les communications CE-CE, qui pourraient mettre en évidence l'ajout par erreur d'un CE dans un mauvais VPN, difficilement détectable par le VPN cible. Ce n'est néanmoins qu'une erreur de configuration de la part du fournisseur de service. La connectivité CE-CE est toutefois possible avec les VPN de niveau 2 dans MPLS, comme *PseudoWire Emulation* (PWE).

Globalement, MPLS/VPN et ATM/FR se comportent de façon similaire au niveau de la sécurité, tout du moins lorsque l'accès partagé à Internet n'est pas offert. Mais dans tous les cas, il faut absolument éviter toute configuration erronée.

2.2.5 Sécurité des architectures MPLS avancées

Au delà de l'architecture simple dans laquelle il n'y a qu'un seul système autonome ou AS (*Autonomous System*), il existe des architectures plus complexes de MPLS qui possèdent des particularités rendant l'analyse de leur sécurité différente :

- réseau cœur multi-AS (*Autonomous System*), aussi appelé *Inter-AS*,
- réseaux MPLS hiérarchisés, du terme anglais *Carrier's Carrier*.

2.2.5.1 Réseau cœur multi-AS

Dans l'architecture *Inter-AS* définie dans la RFC4364 (Rosen et Rekhter, 2006), le réseau cœur se compose de plusieurs systèmes autonomes (AS), appartenant en général à différents fournisseurs de service.

Le cas de ce type d'architecture, reliant par exemple deux fournisseurs de service, est beaucoup plus complexe en termes de sécurité. Il faut dans ces situations faire confiance à l'autre fournisseur de service quant aux paquets qu'il envoie. Une nouvelle fois, la notion de confiance vis-à-vis des fournisseurs de service y compris entre eux-mêmes est importante.

Il existe trois méthodes permettant de connecter des AS entre eux :

- connexion VRF à VRF sur les ASBR (*Autonomous System Border Router*),
- redistribution avec eBGP (*exterior BGP*) des routes VPN-IPv4,
- redistribution eBGP à saut multiple de routes VPN-IPv4 inter-AS et redistribution eBGP des routes IPv4.

Les menaces pouvant affecter les VPN sont les mêmes que précédemment, par contre selon la méthode employée pour relier les différents AS, leur exposition à ces menaces est différente.

La première méthode consiste à utiliser une sous-interface de la connexion entre les ASBR pour chaque VRF. La séparation est maintenue tout au long du transport et les paquets transitant sont de classiques paquets IP. Cette méthode permettant moins d'interaction entre les AS, elle peut être considérée comme plus sûre. Cependant, celle-ci n'est pas adaptée à l'échange d'un grand nombre de VRF car pour chaque VPN inter-AS géré, un VRF et une interface spécifique doivent être configurés sur chaque ASBR.

Dans la seconde méthode, il n'y a qu'une connexion logique entre les ASBR : la différenciation se fait ici sur les étiquettes des paquets. MP-eBGP est utilisé pour redistribuer l'information entre les ASBR. Bien que plus facile à mettre à l'échelle que la première méthode, celle-ci nécessite d'échanger des paquets labélisés entre les différents AS et donc d'accepter des paquets labélisés en entrée du réseau. Le lien entre les ASBR doit être isolé, idéalement par une liaison privée, au pire dans un VLAN et ne jamais traverser des nœuds d'échange Internet (IXP, *Internet Exchange Point*), pour éviter toute attaque compromettante comme la mystification d'étiquettes VPN.

La troisième méthode transforme les ASBR en routeurs P qui n'ont aucune connaissance des VRF dans le réseau. Les deux nuages MPLS sont en quelque sorte regroupés en un seul nuage. Les réflecteurs de routes (RR, *Route Reflector*) peuvent être ici utilisés afin de permettre une mise à l'échelle encore plus grande (Bates, Chen et Chandra, 2006). Cette méthode a le désavantage d'être très ouverte dans le sens où les sessions BGP et les LSP sont établies entre PE de différents AS et non plus limitées aux ASBR comme dans la seconde méthode. Plus encore que dans cette dernière, il est primordial que la liaison entre ASBR soit sûre, car un intrus se trouvant entre les deux ASBR équivaut à un intrus ayant accès au cœur d'un réseau MPLS classique. À noter qu'au niveau de la sécurité, les réflecteurs de routes sont invisibles comme les routeurs P, et possèdent les mêmes informations que les PE, avec lesquels ils les échangent.

Ces deux dernières méthodes permettant à tout AS d'envoyer du trafic dans n'importe quel VPN d'un autre AS, elles pourraient permettre de faciliter les intrusions ou dénis de service. Il est ici fondamental de pouvoir faire confiance à chaque fournisseur de service. De même, ces derniers doivent pouvoir se faire confiance entre eux, afin d'éviter qu'un fournisseur ne compromette tous les autres. Par exemple, dans la troisième méthode, comme l'étiquette VPN n'est pas vérifiée par les ASBR lors du passage d'un AS à un autre, il serait possible au fournisseur de service du premier AS de modifier l'étiquette VPN d'un paquet à destination d'un autre AS et ainsi d'envoyer du trafic de façon unidirectionnelle vers un VPN de cet autre AS sans problème.

Cette nécessité de faire confiance à tous les fournisseurs de service ne devrait de nos jours plus exister, ne faisant qu'augmenter exponentiellement les sources de problèmes. Les technologies – comme ici MPLS, ou BGP – devraient être améliorées afin de ne plus imposer cette condition.

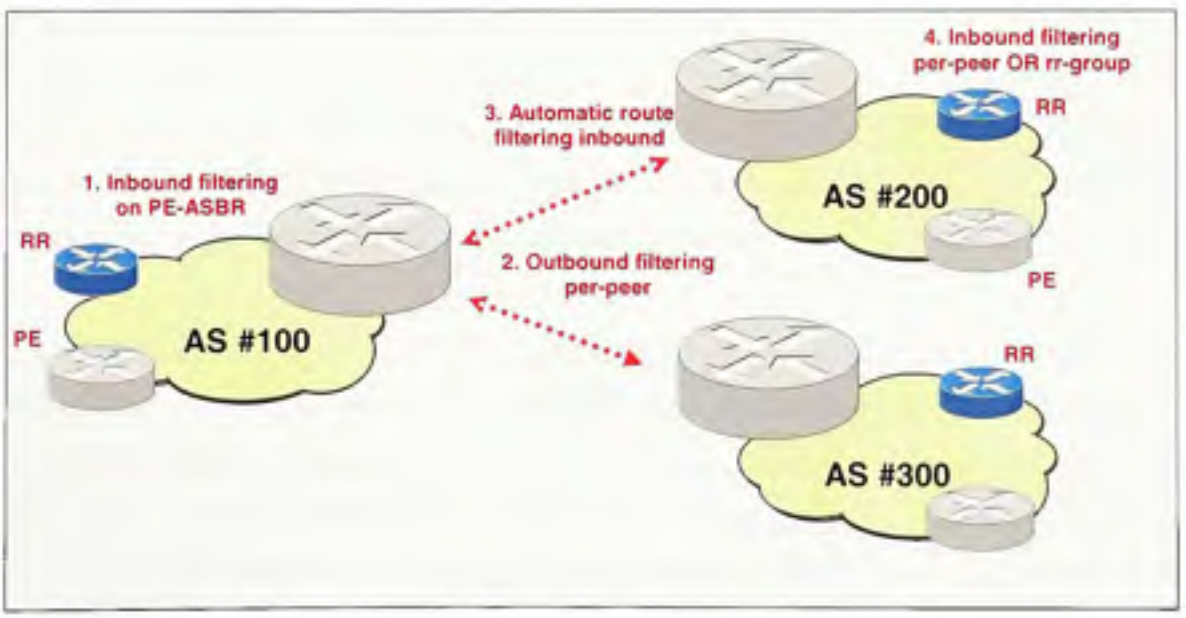

Figure 2.2 ***Les différentes possibilités de filtrage inter-AS***
(Tiré de Cisco, 2003)

Il est possible d'utiliser un filtrage à différents niveaux (en entrée, en sortie pour chaque PE partenaire, selon la route, etc.) comme le présente la Figure 2.2 ci-dessus.

Pour plus d'informations sur le routage et la sécurité des réseaux multi-AS, le lecteur est invité à consulter la présentation de Cisco *Advanced Concepts – Inter AS MPLS/VPN* (Cisco, 2003) d'où est tiré ce schéma.

2.2.5.2 Réseaux MPLS hiérarchisés

L'architecture *Carrier's Carrier* est aussi définie dans la RFC4364. Elle correspond à une hiérarchisation des réseaux MPLS. Les différents réseaux inférieurs sont reliés par leurs CE à des PE du réseau de niveau supérieur par des VPN, il y a une encapsulation VPN dans VPN qui est réalisée, ce qui au niveau de la sécurité est avantageux. Le réseau de niveau supérieur n'a aucune visibilité sur le contenu des paquets qui transitent, puisqu'il ne s'intéresse qu'à l'adresse du PE auquel il doit envoyer les paquets et ne regarde que les deux premières étiquettes (comme dans le cas d'un réseau MPLS/VPN simple, sauf que les données transportées dans le réseau de niveau supérieur sont encapsulées à deux reprises). La seconde étiquette (normalement l'étiquette VPN) représente le CE de sortie du réseau supérieur, ce dernier ne s'occupant en fait que de transporter les paquets MPLS pour les réseaux inférieurs.

La sécurité dans cette architecture se ramène globalement à celle d'un réseau MPLS mono-cœur. Par contre, dans ce cas les PE du réseau de niveau supérieur sont amenés à accepter des paquets portant des étiquettes. Cela est possible uniquement parce que ces paquets quitteront le réseau de niveau supérieur sans que ces étiquettes n'aient été ôtées (*cf.* RFC4364). Les PE doivent vérifier que les étiquettes des paquets reçus d'un CE du réseau inférieur correspondent bien aux étiquettes distribuées pour ce CE. La mystification de l'étiquette VPN extérieure (représentant le VPN créé dans le réseau supérieur) par le fournisseur du réseau inférieur est alors impossible : si elle est

incorrecte, le paquet est détruit ; si elle est correcte, le paquet ressortira nécessairement dans le réseau inférieur prédéfini, quelles que soient les données et la valeur de l'étiquette VPN interne. Le réseau supérieur est donc sécurisé de la même façon que l'est un réseau MPLS mono-cœur. Cela provient du fait que le CE appartient au fournisseur de service et il fait ainsi partie de la zone de confiance.

Les seules attaques sur le réseau supérieur pourraient être liées aux protocoles de signalisation utilisés : n'importe quel IGP, LDP ou BGP. Ceux-ci doivent être protégés pour éviter des attaques de déni de service ou l'envoi de mises à jour erronées. Le protocole BGP fera l'objet d'une étude dans le chapitre 4.

CHAPITRE 3

TESTS

Ce chapitre a pour objectif de présenter le cas d'architectures MPLS/VPN avancées. Il décrit dans un premier temps les menaces liées à la connectivité Extranet et Internet, puis les tests pratiques menés sur le réseau de Bell Canada après la découverte d'une possibilité de faille dans l'architecture Extranet, présentée dans la partie 3.1.

3.1 Menaces liées à la connectivité Extranet

Un Extranet est une extension d'un réseau privé permettant de partager de l'information avec des utilisateurs extérieurs. Un Extranet peut par exemple être créé lorsqu'une entreprise permet à ses sous-traitants d'avoir accès à ses propres bases de données. Leur accès se fait généralement via Internet en utilisant un procédé d'authentification.

Dans MPLS, un Extranet peut se voir sous la forme d'une ressource partagée par plusieurs VPN. Leur création est simple, il suffit de manipuler les imports/exports de *route targets* afin de donner accès à chaque client à la ressource partagée tout en évitant de relier les différents VPN entre eux. La ressource commune va ainsi voir les réseaux de tous les clients qui y sont connectés, par contre chaque client ne pourra voir que les routes appartenant à la ressource partagée. La seule contrainte de la connectivité Extranet est l'obligation d'utiliser des espaces d'adressage distincts, puisqu'il y a communication avec l'extérieur des réseaux privés des clients.

Il est cependant important d'utiliser des pare-feux dans une connectivité Extranet, car malgré la configuration correcte des imports/exports de *route targets* il peut être possible d'envoyer du trafic de façon unidirectionnelle d'un VPN à l'autre, ce qui peut permettre l'envoi de vers.

La Figure 3.1 ci-dessous présente une possibilité de réseau Extranet. Le client 1 (site 1) échange des informations avec le client 2 (site 2), tandis que ce dernier échange des informations avec le client 3 (site 3). Les VRF pour les sites 1, 2 et 3 (voir schéma) montrent bien que le client 1 ne voit pas les routes du client 3 et inversement. Pourtant il pourrait sous certaines conditions envoyer du trafic de façon unidirectionnelle au client 3. Il en va de même avec le client 4, situé au site 4, toutefois pour simplifier cet exemple nous ne considérons pas le site 4 et les imports/exports de routes liés au VPN C.

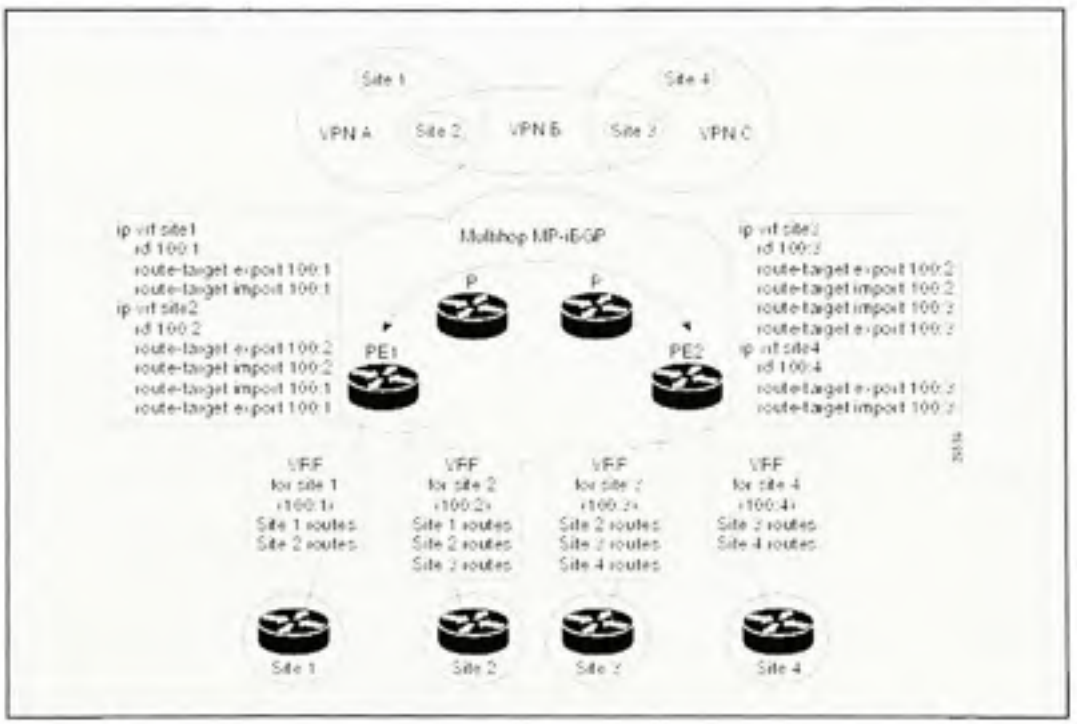

Figure 3.1 ***Sites clients dans plusieurs VPN***
(Tiré de Cisco, 2006)

Afin d'analyser ce qui se passe dans ce réseau Extranet, rappelons les conditions sur le réseau MPLS :

- Les sites 1 et 3 représentent deux clients, le site 2 représente la ressource partagée,
- Utilisation des *route-targets* import/export,

- La visibilité des sites (minimale pour l'exemple) est donnée dans le Tableau 3.1,
- Les sites 1 et 3 n'ont aucune visibilité entre eux,
- Implémentation par Cisco (version de l'IOS : 12.3(8r2)T) sur 3725 et 7206.

Par ailleurs, les hypothèses suivantes sur l'environnement sont prises :

- L'intrus se trouve dans le site 1, la cible dans le site 3,
- L'intrus connaît ou devine une adresse IP appartenant au site 3,
- Il y a une route par défaut du CE (site 1) vers le PE (VRF site 1),
- Il y a une route par défaut PE (VRF site 1) vers une adresse du site 2,
- Il n'y a pas d'attaquant dans le site 2,

La topologie du réseau présenté dans la Figure 3.1 au niveau du site 2 peut être interprétée de plusieurs façons, présentées ci-après. Dans un premier cas (*cf.* Figure 3.2), le site 2 contient les deux VPN distincts A et B, ce qui nous intéresse peu car dans ce cas nous n'avons pas de ressource partagée. Nous obtenons deux VPN A et B disjoints par l'utilisation de VLAN séparés entre le PE et le CE du site 2. Il faut néanmoins faire attention dans ce cas à la bonne configuration du CE, afin d'empêcher le trafic d'aller d'un VPN à l'autre. Cela nécessite l'utilisation de listes d'accès au sein de ce routeur, car les CE ne font pas de séparation du trafic ou du routage au niveau 3 comme les PE MPLS. L'autre possibilité, meilleure, consiste à effectuer un routage statique entre chaque interface de VPN et l'interface du VLAN reliée au PE.

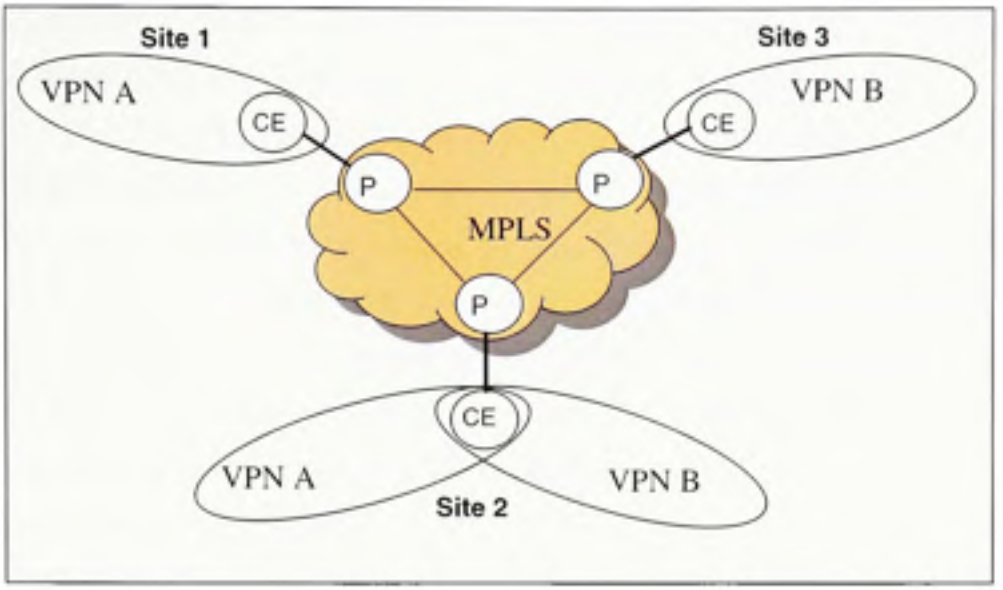

Figure 3.2 ***Représentation de la connectivité Extranet - Cas 1***

Le tableau ci-dessous présente la visibilité des sites, déterminée par les imports et exports de route réalisés.

Tableau 3.1

Configuration des vrf pour les sites 1, 2 et 3 de la connectivité Extranet

```
ip vrf site 1                          ip vrf site 2
      rd 100:1                               rd 100:2
      route-target export 100:1              route-target export 100:1
      route-target import 100:1              route-target import 100:1
ip vrf site 3                                route-target export 100:2
      rd 100:3                               route-target import 100:2
      route-target export 100:2
      route-target import 100:2
```

Le second cas (*cf.* Figure 3.3) est plus intéressant. Il représente le principe d'une ressource partagée, donc d'une connectivité Extranet, en donnant accès à un même

Le second cas (*cf.* Figure 3.3) est plus intéressant. Il représente le principe d'une ressource partagée, donc d'une connectivité Extranet, en donnant accès à un même réseau (le site 2) à deux VPN différents, A et B et par conséquence aux deux sites 1 et 3. Il serait faux de penser que le simple fait de réaliser cette configuration particulière est directement synonyme de bris d'étanchéité ou de liberté de circulation entre le site 1 et le site 3. La notion des VPN A et B est ici assez subjective, puisqu'en fait MPLS réalise des imports/exports de routes pour permettre à chaque site de voir certaines routes et d'autres pas. Les membres du site 1 vont ainsi voir les routes du site 2, mais pas les routes du site 3, et inversement les membres du site 3 ne pourront voir que les routes du site 2, mais pas celles du site 1.

Par contre, la présence d'une route par défaut vers la ressource partagée peut permettre à un intrus placé dans le site 1 d'envoyer des paquets de façon unidirectionnelle du site 1 au site 3. Bien que le plan de contrôle soit correct (les routes du site 3 ne sont pas dévoilées au site 1), il n'y a rien qui empêche la transmission des paquets du site 1 vers le site 3. Les paquets à destination du site 3 vont suivre la route par défaut vers le site 2, or ce dernier étant la ressource partagée, il connaît les routes des sites 1 et 3 et peut donc acheminer ces paquets vers le site 3. Si en plus la route par défaut vers la ressource partagée est acquise pour tous les clients, alors la transmission de paquets peut être bidirectionnelle entre les sites 1 et 3.

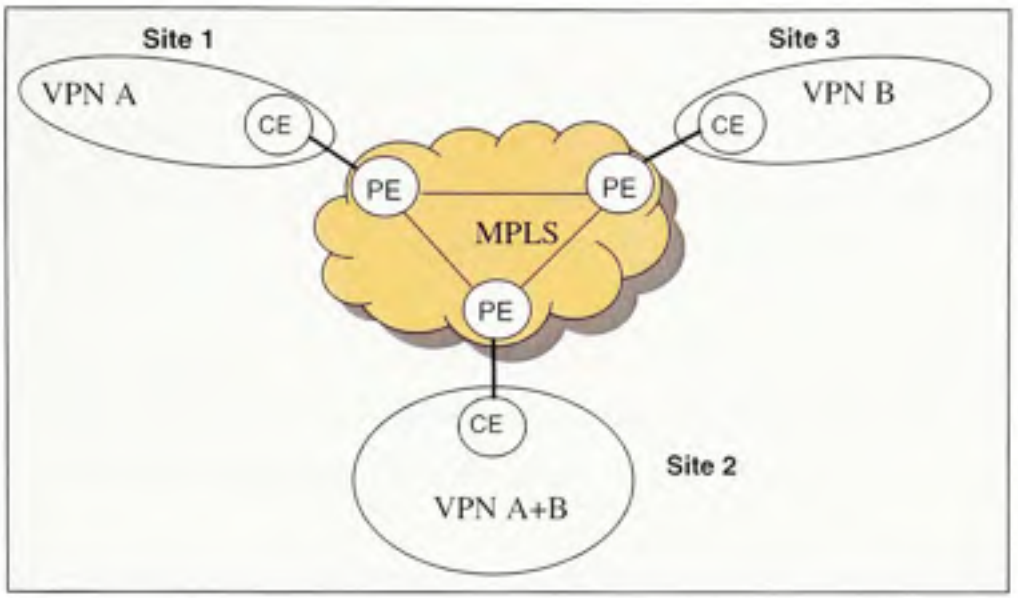

Figure 3.3 ***Représentation de la connectivité Extranet - Cas 2***

Des tests ont été menés avec succès sur le réseau de *Bell Canada* pour vérifier la réalisation de cette attaque. La partie 3.3 présente ces tests ainsi que les résultats obtenus.

La question qui demeure concerne la légitimité d'une route par défaut. Si elle a sa raison d'exister, alors l'attaque est possible. Le fournisseur de service étant le seul à gérer les PE où cette route doit être ajoutée, il n'est pas impossible que des erreurs de configuration existent. En outre, l'attaquant pourrait tromper le fournisseur en faisant de l'ingénierie sociale, lui demandant d'ajouter la route par défaut dans un VRF lui appartenant vers une ressource sur laquelle il a le droit d'accès, ce qui semblerait légitime au fournisseur. Si ce dernier ne se laisse pas avoir, le seul moyen resterait l'injection de cette route, via le protocole MP-BGP. Afin de vérifier si une telle injection est possible, nous avons dans le chapitre 4 réalisé une étude de la sécurité du protocole BGP.

Par ailleurs, il ne faut pas faire confiance au CE de la ressource partagée. Étant géré par le client, des erreurs de configurations volontaires ou pas peuvent être présentes. Mais même si ce dernier est bien géré et n'annonce pas de routes ne lui appartenant pas, l'attaque reste possible. Toutefois, s'il est corrompu, la route par défaut n'est plus nécessaire.

L'utilisation de pare-feux est en tout cas indispensable dans une telle architecture. Le partage d'une ressource est possible en utilisant l'architecture MPLS/VPN, mais cela sort du cadre classique présenté dans la RFC4364.

L'accès à Internet présenté dans la partie suivante peut poser un problème similaire, tout en simplifiant la légitimité de l'existence de la route par défaut entre les PE. Cette architecture est cependant plus complexe à analyser, car des passerelles, NAT et pare-feux sont déjà présents pour bloquer les attaques en provenance d'Internet.

3.2 Menaces liées à une connectivité Internet

Souvent, les clients d'un fournisseur de service MPLS/VPN souhaitent un accès à Internet en plus de leur VPN. Il existe plusieurs façons de fournir cet accès.

La première méthode consiste à placer Internet dans un VRF. Cette méthode ne remet pas en question la sécurité du cœur du réseau, mais exige beaucoup de mémoire dans les PE afin de stocker dans les VRF toutes les routes Internet. Si les routes d'Internet sont stockées dans un routeur CE supplémentaire situé entre le PE et le fournisseur d'accès Internet, cela permet d'économiser de la mémoire d'une part, un préfixe stocké dans un VRF prenant plus de place que dans la table de routage globale, d'autre part le routeur CE permet de protéger le routeur PE, en étant la seule interface publique visible. Si l'espace d'adressage CE-PE n'est pas annoncé (ce qui inclut l'adresse du PE), aucune

attaque ne pourra se porter directement sur le PE, ce qui renforce encore plus la sécurité du réseau contre les attaques provenant de l'Internet.

La seconde méthode suppose d'effectuer le routage Internet directement dans le cœur. Le cœur du réseau MPLS/VPN devient semblable au cœur d'un réseau IP : les tables de routage de chaque routeur (P, PE) sont utilisées afin de réaliser le routage. Le cœur n'est plus invisible d'Internet et comme des VPN utilisent le cœur, il faut empêcher avec des listes d'accès situés sur les PE de pouvoir joindre tout routeur P ou PE du cœur. Cette méthode reste tout de même plus dangereuse pour le réseau que la précédente.

La troisième possibilité utilise MPLS seul pour établir des LSP entre les PE des clients souhaitant se connecter à Internet et le PE d'accès à Internet. Des sessions iBGP permettent aux PE de communiquer entre eux les tables de routage Internet sans que les routeurs P ne s'en préoccupent, ces derniers n'ont donc pas à maintenir de l'information quant au routage Internet. Par contre, ces derniers sont joignables de façon unidirectionnelle depuis Internet au travers du PE d'entrée (ce dernier connaissant les routes menant aux routeurs P du cœur), ce qui nécessite là aussi l'utilisation de listes d'accès adéquates pour éviter les attaques de type déni de service.

Quelle que soit la méthode employée (VPN, IP, MPLS), la séparation des VPN n'est pas remise en cause. Cependant, le réseau MPLS devient sensible aux attaques de déni de service en provenance d'Internet, et selon la méthode employée le cœur du réseau peut être attaqué. La connectivité à Internet doit être considéré avec prudence, les clients concernés se retrouvant face aux mêmes types d'attaques que dans un réseau IP classique, le fournisseur du réseau doit donc prendre les mesures nécessaires pour se protéger (pare feu, IDS, antivirus).

Nonobstant, les attaques ne proviennent pas uniquement d'Internet. En utilisant la première méthode (Internet dans un VRF), le même type d'attaque que dans la

connectivité Extranet peut se produire. Si l'adressage des clients est public, la Figure 3.4 montre la configuration à réaliser. Le pare-feu, situé dans le CE Internet, doit alors impérativement filtrer tous les paquets, quelle que soit leur provenance pour éviter que des paquets provenant du VPN d'un client pénètrent le VPN d'un autre client (voir les tests réalisés dans la partie 3.3 pour plus de détails).

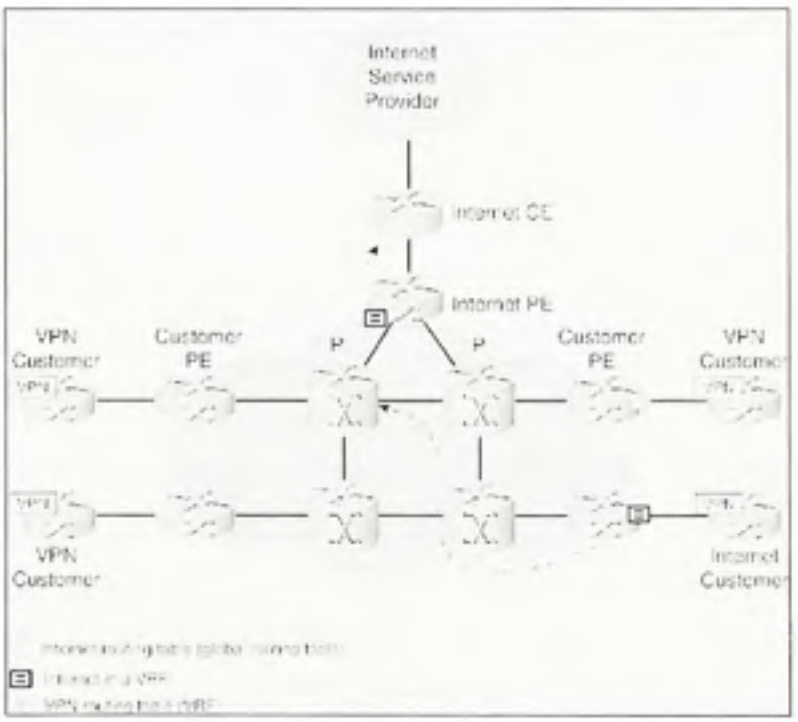

Figure 3.4 ***Connectivité Internet dans un VRF***
(Tiré de Behringer et Morrow, 2005)

Si l'adressage des clients est privé, la situation est différente car un NAT doit être employé pour faire la traduction d'adresses privées en adresses publiques. La Figure 3.5 présente le cas de plusieurs clients qui partagent un accès à Internet ainsi que le NAT chargé de faire la traduction d'adresses publiques/privées. Si les espaces d'adressage des différents clients (ici 1, 2 et 3) ne se recoupent pas, ils peuvent partager le même VRF puis la même passerelle Internet.

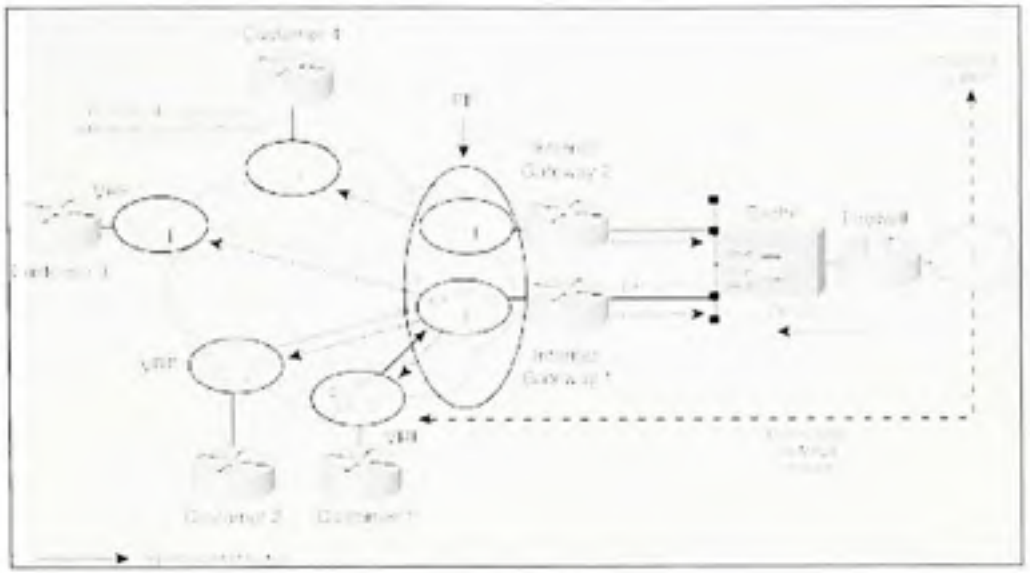

Figure 3.5 ***Accès partagé à Internet***
(Tiré de Behringer et Morrow, 2005)

La sécurité dans cette situation peut être garantie uniquement si les paquets provenant d'un client sont forcés de se rendre au moins jusqu'au pare-feu avant de pouvoir être routés. Si la passerelle Internet effectue un routage dynamique en fonction de la destination des paquets au lieu de se limiter à la traduction d'adresse, il peut être possible à un des clients d'envoyer des paquets aux autres clients partageant le VRF Internet. Cela ne sera par contre pas possible en forçant les paquets à se rendre au-delà du pare-feu avant d'être routés.

En conclusion sur la connectivité Internet, le maintien de la sécurité du réseau et de la séparation des VPN se limite donc dans certains cas à la robustesse d'une liste d'accès. Pour respecter le principe de défense en profondeur, il serait nécessaire d'ajouter d'autres éléments comme un IDS ou des pare-feux à la bordure du réseau. Ou d'utiliser la première méthode, qui n'expose aucun élément du cœur du réseau mais nécessite plus de mémoire.

Concernant l'attaque d'un VPN vers un autre VPN, la connectivité Internet rend valide une des hypothèses/conditions de la connectivité Extranet, la route par défaut. En l'absence de pare-feu, cette attaque est ici possible. Cependant, le fait d'avoir Internet impliqué rend indispensable l'utilisation de pare-feux. La sécurité peut finalement être garantie en respectant quelques règles, comme l'obligation de filtrer tous les paquets et non pas seulement les paquets en provenance d'Internet, et en imposant à tous les paquets de se rendre au-delà du pare-feu avant d'être routés.

3.3 Tests d'étanchéité de l'architecture Extranet

Nous voulons montrer dans ces tests l'existence de failles dans la technologie Extranet (aussi dénommée *hub-and-spoke*), dans laquelle plusieurs VPN ont accès à une ressource partagée. Normalement il devrait être impossible pour un client d'un VPN de pouvoir communiquer avec un client ou n'importe quelle machine d'un autre VPN au travers de la ressource partagée, c'est-à-dire en utilisant la ressource partagée comme *proxy*. Le fait d'avoir accès à une ressource partagée n'inclut pas la possibilité de laisser l'accès aux ressources d'un site appartenant à un autre VPN, grâce aux imports/exports de route tel que présenté dans la section 3.1.

La Figure 3.6 présente un exemple d'architecture Extranet. Les VPN A et B sont indépendants et communiquent avec la ressource partagée. Les imports/exports de routes sont réglés de telle façon que les VPN A et B ne s'échangent pas leurs routes.

Figure 3.6 ***Schéma de l'architecture Extranet***
(Tiré de Behringer et Morrow, 2005)

Or, d'après Behringer et Morrow, il semble possible que si un client du VPN A connaît ou devine l'adresse d'un client du VPN B (dans l'exemple, 193.0.1/24), il puisse envoyer de façon unidirectionnelle des paquets vers le VPN B. Ceci serait suffisant pour envoyer un ver ou un virus.

Nos tests vont consister à tenter de reproduire cette expérience. Pour cela nous allons utiliser le réseau MPLS de test de Bell Canada. Il s'agit d'une plate-forme de routeurs Cisco interconnectés par différentes technologies de niveau 2 (ATM et Ethernet) et implémentant MPLS (RFC4364). Les LER (routeurs PE) sont des 3725, les LSR (routeurs P) sont des 7206. La version de l'IOS est 12.3(8r2)T. La configuration nécessaire pour les tests est présentée ci-dessous.

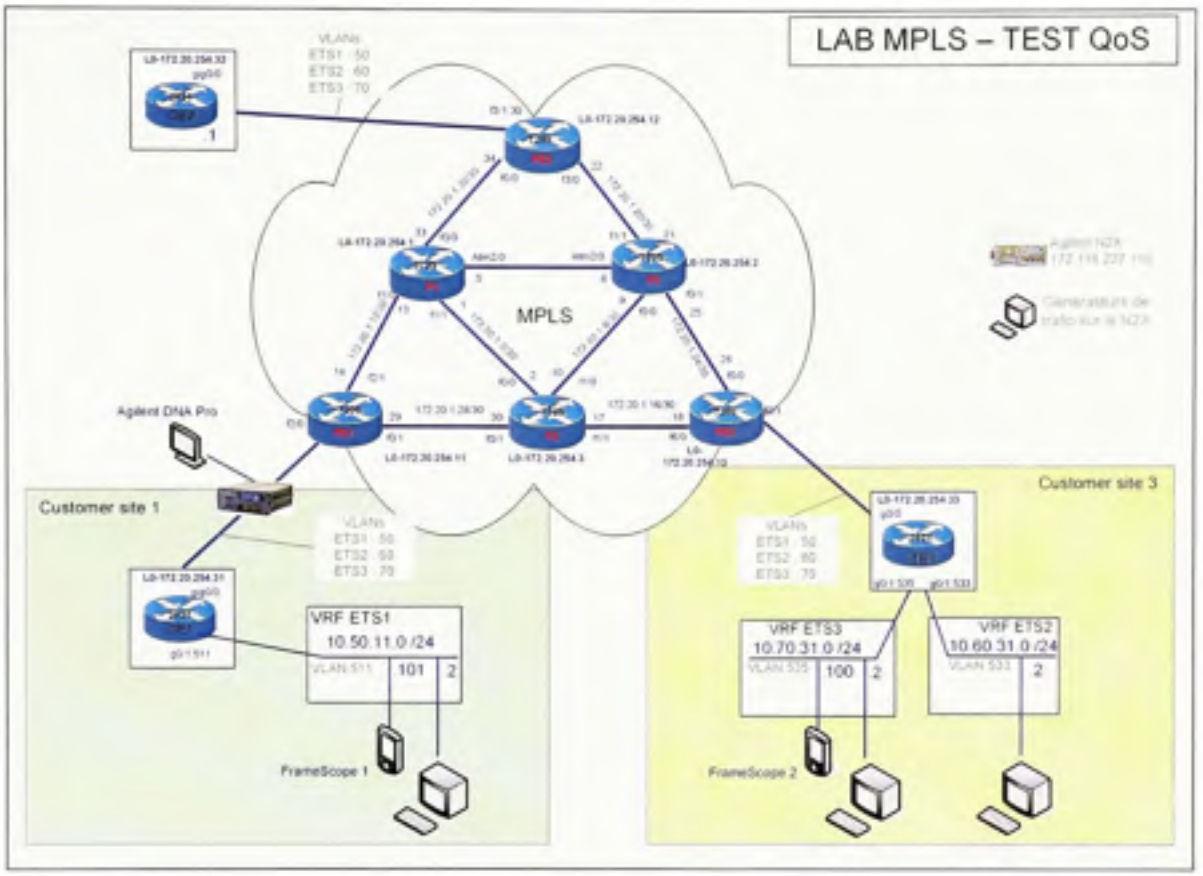

Figure 3.7 ***Schéma Visio du réseau de test de Bell Canada***

Sur le *customer site* 3, deux instances VRF ETS2 et ETS3 sont configurées pour représenter deux clients indépendants. La ressource partagée est ici représentée dans le *customer site* 1, dans le VRF ETS1. Les VRF ETS2 et ETS3 exportent leurs routes au VRF ETS1 située sur le Customer Site 1, et importent les routes du VRF ETS1 selon les tableaux présentés ci-dessous. De même, le VRF ETS1 importe les routes des VRF ETS2 et ETS3 et exporte ses propres routes.

Tableau 3.2

Configuration des VRF sur le PE1

```
ip vrf ETS1
 rd 65000:50
 route-target export 65000:50
 route-target import 65000:50
 route-target import 65000:60
 route-target import 65000:70
!
ip vrf ETS2                                    ip vrf ETS3
 rd 65000:60                                    rd 65000:70
 route-target export 65000:60                   route-target export 65000:70
 route-target import 65000:60                   route-target import 65000:70
```

Tableau 3.3

Configuration des VRF sur le PE3

```
ip vrf ETS1
 rd 65000:50
 route-target export 65000:50
 route-target import 65000:50
!
ip vrf ETS2                                    ip vrf ETS3
 rd 65000:60                                    rd 65000:70
 route-target export 65000:60                   route-target export 65000:70
 route-target import 65000:60                   route-target import 65000:70
 route-target import 65000:50                   route-target import 65000:50
```

Dans ces tableaux les informations essentielles, autrement dit les imports/exports de routes ajoutés à une configuration classique de VPN indépendants qui permettent de partager une ressource située dans le VRF1 du *customer site* 1, sont indiqués en gras.

Afin de réaliser les tests, nous utilisons des appareils mobiles « à tout faire » FrameScope Pro de Agilent. Bien que ces appareils soient capables de réaliser une multitude d'actions (tests de connectivité, génération de trafic, etc.), nous allons nous limiter à la fonctionnalité *traceroute* afin d'observer ce qui se passe lorsque nous tentons de communiquer entre différents VPN. Les FrameScope Pro sont branchés respectivement derrière CE1 et CE3 avec les détails présentés dans le tableau ci-dessous.

Tableau 3.4

Disposition des FrameScopePro dans le réseau

FrameScope	Position	VLAN	VPN correspondant	Adresse IP
1	Derrière CE1	511	ETS1	10.50.11.101
2	Derrière CE3	535	ETS3	10.70.31.100

Afin d'observer le contenu des paquets transitant sur le réseau, nous utilisons en outre un *sniffer* Agilent DNA Pro positionné entre PE1 et CE1.

Dans un premier temps nous allons vérifier que le réseau fonctionne bien en envoyant un paquet dans un même VPN d'un site à l'autre. Ensuite, nous générerons des paquets dans le VRF ETS3 à destination d'un poste dans le VRF ETS2, en utilisant une adresse IP de destination appartenant au VRF ETS2. La commande « *traceroute* » va être utilisée. Elle permettra de tester la connectivité entre les VRF ETS2 et ETS3, et en outre d'afficher le chemin suivi.

3.3.1 Test de communication avec la ressource partagée

Afin de voir ce qui se passe lors d'une communication légitime, nous réalisons d'abord un *traceroute* du FrameScope 2 vers le FrameScope 1. Étant donné que le VRF ETS1 dans PE1 exporte ses routes vers le VRF ETS3 et que le VRF ETS3 dans PE3 importe

toutes les routes du VRF ETS1, les deux FrameScope peuvent se parler bien qu'étant dans des VRF séparés. Cela est normal, ETS1 est la ressource partagée donc atteignable par ETS3.

La commande *traceroute* donne le résultat contenu dans le tableau ci-dessous.

Tableau 3.5

Résultat de la commande *traceroute* vers la ressource partagée

#traceroute 10.50.11.101	
1. 10.70.31.1	(CE3 – interface VLAN 535)
2. 10.70.3.1	(PE3 – interface VLAN 70)
3. 172.20.1.17	(P3 – signifie que le MPLS *traceroute* est actif)
4. 10.50.1.1	(PE1 – interface VLAN 50)
5. 10.50.1.2	(CE1 – interface VLAN 511)
6. 10.50.11.101	(FrameScope 1)

La capture d'écran suivante montre ce qui est observé par l'analyseur entre PE1 et CE1.

Src. Address	Dest Addr	Protocol	Description
172.20.1.17	10.70.31.100	VLAN	IP: 172.20.1.17 -> 10.70.31.100 Id=45046 ICMP: Time exceeded In-transit
172.20.1.17	10.70.31.100	VLAN	IP: 172.20.1.17 -> 10.70.31.100 Id=45046 ICMP: Time exceeded In-transit
10.70.31.100	10.50.11.101	VLAN	IP: 10.70.31.100 -> 10.50.11.101 Id=24 ICMP: Echo request
10.50.1.2	10.70.31.100	VLAN	IP: 10.50.1.2 -> 10.70.31.100 Id=37867 ICMP: Time exceeded In-transit
10.70.31.100	10.50.11.101	VLAN	IP: 10.70.31.100 -> 10.50.11.101 Id=25 ICMP: Echo request
10.50.11.101	10.70.31.100	VLAN	IP: 10.50.11.101 -> 10.70.31.100 Id=52 ICMP: Echo reply

Figure 3.8 ***Capture d'écran d'un traceroute légitime***

Les deux premiers paquets correspondent au saut 3, certes le TTL a expiré avant d'atteindre CE1, mais comme il a expiré dans le nuage MPLS (sur le routeur P3), les

paquets ICMP sont forcés de sortir du réseau MPLS en poursuivant leur route jusqu'au CE1 avant de pouvoir retourner vers l'émetteur du paquet, situé de l'autre côté.

Les deux paquets suivants correspondent au saut numéro 5, le CE1 répond alors au message ICMP *Echo request* par un ICMP *Time Exceeded* (voir le fonctionnement de la commande *traceroute* (Hares et Wittbrodt, 1994) pour plus de détails).

Finalement, les deux derniers paquets correspondent au dernier saut, avec cette fois-ci un message ICMP *Echo Reply* en réponse puisque la destination a été atteinte.

3.3.2 Test de communication avec un VPN non partagé

Maintenant que nous avons vu ce qu'il se passe lors d'un échange légitime, nous allons tenter de faire communiquer un client de ETS3 avec un client de ETS2. Comme le VRF ETS3 dans CE3 et PE3 ne connaît aucune route vers le VRF ETS2, il est nécessaire d'ajouter une route par défaut vers le VRF ETS1. Cette route par défaut peut sembler légitime car le VRF ETS1 représente la ressource partagée et à ce titre, accepte les paquets provenant de ETS3. Le paquet devrait donc partir de ETS3 sur PE3, dans un premier temps atteindre ETS1 sur le CE1 (la ressource partagée), et en cas de succès de l'attaque rejoindre ETS2 sur PE3.

Deux routes par défaut ont donc été ajoutées. La première route par défaut a été placée dans le PE3 au niveau du VRF ETS3. Celle-ci pointe sur l'interface du VLAN 511 au niveau de CE1, c'est-à-dire l'adresse 10.50.11.1. De plus, une seconde route par défaut a été placée dans le CE3 pour diriger les paquets vers le PE3. Ainsi, il existe « une » route par défaut qui permet d'atteindre le VRF ETS1 à partir du VRF ETS3. La légitimité de cette route par défaut est discutée de façon plus approfondie dans la section 3.3.4.

Nous effectuons donc une nouvelle fois la commande *traceroute* vers une interface du VRF ETS2, en l'occurrence le port du routeur CE3 lié à ETS2. Le tableau ci-dessous montre le résultat obtenu.

Tableau 3.6

Résultat de la commande *traceroute* vers ETS2

#traceroute 10.60.31.1	
1. 10.70.31.1	(CE3 – interface VLAN 535)
2. 10.70.3.1	(PE3 – interface VLAN 70)
3. 172.20.1.17	(P3 – signifie que le MPLS *traceroute* est actif)
4. 10.50.1.1	(PE1 – interface VLAN 50)
5. 10.50.1.2	(CE1 – interface VLAN 511)
6. 10.50.1.1	(PE1 – interface VLAN 50)
7. * *	(*timeouts*)
8. * *	
…	

Les quatre premiers sauts sont identiques au test précédent. Les paquets ICMP se rendent alors jusqu'au routeur CE1, ce qui semble logique puisque la route par défaut dans le PE3 pointe vers le VLAN 511 du VRF ETS1. Au sixième saut, nous constatons que le TTL des paquets est expiré en arrivant au niveau du PE1. Ils semblent alors poursuivre leur chemin en retournant vers le réseau MPLS. Par la suite, aucune réponse n'est reçue. Tous les essais suivants, malgré l'augmentation de la valeur du TTL du paquet *echo request*, ne reçoivent aucune réponse, et il en est ainsi jusqu'au nombre maximal de sauts paramétré dans la commande *traceroute*.

Même si la requête n'aboutit pas, elle montre déjà un premier élément positif : une fois rendus au CE1 dans le VPN ETS1, les paquets ICMP semblent retourner vers le site 3. Nous allons vérifier sur la capture d'écran de l'analyseur lors de ce second test que les paquets font bien demi-tour une fois rendus au CE1.

La capture ci-dessous montre les paquets transitant entre le PE1 et le CE1 dans le VLAN50 (rien ne passe dans les autres VLAN entre CE1 et PE1).

Src. Address	Dest Addr	Protocol	Description
172.20.1.17	10.70.31.100	VLAN	IP: 172.20.1.17 -> 10.70.31.100 Id=16360
172.20.1.17	10.70.31.100	VLAN	IP: 172.20.1.17 -> 10.70.31.100 Id=16360
10.70.31.100	10.60.31.1	VLAN	IP: 10.70.31.100 -> 10.60.31.1 Id=119
10.50.1.2	10.70.31.100	VLAN	IP: 10.50.1.2 -> 10.70.31.100 Id=32247
10.70.31.100	10.60.31.1	VLAN	IP: 10.70.31.100 -> 10.60.31.1 Id=120
10.70.31.100	10.60.31.1	VLAN	IP: 10.70.31.100 -> 10.60.31.1 Id=120
10.70.31.100	10.60.31.1	VLAN	IP: 10.70.31.100 -> 10.60.31.1 Id=121
10.70.31.100	10.60.31.1	VLAN	IP: 10.70.31.100 -> 10.60.31.1 Id=121

Figure 3.9 ***Capture d'écran d'un traceroute vers un VPN non partagé – VLAN 50***

Les quatre premiers paquets observés sont similaires aux sauts 3 et 5 du test précédent, nous ne reviendrons donc pas dessus. Les deux lignes suivantes (Id=120) correspondent au sixième saut. Comme à ce moment précis le paquet ICMP fait d'abord le trajet PE1 → CE1 puis CE1 → PE1, il apparaît deux fois sur l'analyseur. Les adresses MAC relevées par l'analyseur sont inversées entre les deux lignes confirmant l'idée du retour. Les deux dernières lignes (Id=121) correspondent au septième saut, et sont assez similaires aux précédentes concernant l'aller-retour vers le CE1.

Les paquets correspondant aux sauts suivants n'ont pas été inclus dans la capture ci-dessus, leur trace sur l'analyseur équivalant aux quatre dernières lignes de la capture. Nous remarquons aussi que vu l'emplacement de l'analyseur, nous ne pouvons recueillir les réponses des sauts 6 et suivants, le cas échéant. En effet, lorsque le TTL de la requête ICMP devient nul en arrivant sur le PE1 au saut 6, le chemin le plus direct depuis le PE1 vers le CE3 (VRF ETS3) ne passe pas par le CE1.

Ce test met en avant un problème : même si les paquets émis parviennent à rejoindre le VPN ETS2, il est impossible d'avoir une réponse car ETS2 ne connaît pas de route pour accéder à l'adresse source des requêtes ICMP contenue dans ETS3. C'est pour cela qu'aucune réponse n'est reçue après le saut 6.

Plusieurs possibilités s'offrent à nous :

- soit nous déplaçons l'analyseur entre PE3 et CE3 afin de regarder si des requêtes passent dans le VLAN 60 (correspondant à ETS2) entre ces deux routeurs,
- soit nous ajoutons une route par défaut dans ETS2 (au niveau du PE3 et CE3) pour envoyer les paquets vers ETS1, pour éventuellement permettre une communication bidirectionnelle.

Comme il ne semble pas logique d'ajouter une route par défaut supplémentaire dans le VRF ETS2 (puisque celui-ci est la cible de l'attaque), nous allons déplacer l'analyseur entre PE3 et CE3. Cela ne permettra pas d'avoir de réponse à la commande *traceroute*, mais au moins il sera possible de voir si les requêtes ICMP se rendent jusque dans le VLAN 60.

La capture d'écran ci-dessous correspond aux paquets traversant le VLAN 60.

Src. Address	Dest Addr	Protocol	Description
172.20.1.30	10.70.31.100	VLAN	IP: 172.20.1.30 -> 10.70.31.100 Id=10548 ICMP: Time exceeded in transit
172.20.1.30	10.70.31.100	VLAN	IP: 172.20.1.30 -> 10.70.31.100 Id=10568 ICMP: Time exceeded in transit
10.70.31.100	10.60.31.1	VLAN	IP: 10.70.31.100 -> 10.60.31.1 Id=225 ICMP: Echo request
10.70.31.100	10.60.31.1	VLAN	IP: 10.70.31.100 -> 10.60.31.1 Id=226 ICMP: Echo request
10.70.31.100	10.60.31.1	VLAN	IP: 10.70.31.100 -> 10.60.31.1 Id=228 ICMP: Echo request
10.70.31.100	10.60.31.1	VLAN	IP: 10.70.31.100 -> 10.60.31.1 Id=229 ICMP: Echo request
10.70.31.100	10.60.31.1	VLAN	IP: 10.70.31.100 -> 10.60.31.1 Id=231 ICMP: Echo request

Figure 3.10 ***Capture d'écran d'un traceroute vers un VPN non partagé – VLAN 60***

Il faut noter en premier lieu que comme tous les paquets observés ne peuvent retourner à leur origine (aucune route n'étant connue dans le VPN ETS2 pour joindre le VPN ETS3), ils créent tous un timeout à la source (le FrameScope 2 dans ETS3). Celui-ci va réaliser deux tentatives pour chaque saut. Si aucune réponse n'est reçue, alors il va incrémenter le TTL de 1 et réaliser deux nouvelles tentatives.

Les deux premiers paquets correspondent au saut 7 (le routeur P3, lors du retour vers PE3). Nous observons ici la réponse car il s'agit d'un routeur MPLS qui doit faire suivre la réponse à la sortie du réseau MPLS avant de pouvoir la renvoyer à l'émetteur.

Les deux paquets suivants (Id=225, Id=226) correspondent au saut 9 (le saut 8 vers le routeur PE3 n'est pas observé à cause de la position de l'analyseur entre PE3 et CE3). Bien qu'ils atteignent leur destination (CE3, avec l'adresse 10.60.31.1), aucune réponse ne peut être émise à cause de l'absence de route par défaut dans le VRF ETS2 de CE3.

Le FrameScope ne pouvant savoir que la destination a été atteinte, il continue à envoyer des paquets en incrémentant le champ TTL. Les paquets 5 et 6 ont un TTL de 2 en sortant de PE3, le paquet 7 (dernier enregistré, mais d'autres suivraient en continuant l'expérience) a un TTL de 3.

Tableau 3.7

Déduction de la commande *traceroute* complétée vers ETS2

#traceroute 10.60.31.1	
1. 10.70.31.1	(CE3 – interface VLAN 535)
2. 10.70.3.1	(PE3 – interface VLAN 70)
3. 172.20.1.17	(P3 – signifie que le MPLS *traceroute* est actif)
4. 10.50.1.1	(PE1 – interface VLAN 50)

5. 10.50.1.2	(CE1 – interface VLAN 511)
6. 10.50.1.1	(PE1 – interface VLAN 50)
7. 172.20.1.30	**(P3 – interface du côté de PE1)**
8. 10.60.3.1	**(PE3 – interface VLAN 60)**
9. 10.60.31.1	**(CE3 – interface VLAN 533) – destination atteinte**

Grâce à ces nouvelles observations, nous pouvons maintenant obtenir le chemin complet des paquets vers ETS2. En gras sont indiqués dans le tableau ci-dessus les sauts déduits des observations subséquentes au déplacement de l'analyseur. En conclusion, il a bien été possible d'envoyer des paquets dans le VRF ETS2 en partant du VRF ETS3 en transitant par le VRF ETS1, à l'aide d'une route par défaut.

3.3.3 Vérification du succès de la communication vers ETS2

Afin de confirmer que les paquets émis par le FrameScope2 depuis le VPN ETS3 ont bien été reçus par le VPN ETS2, nous tentons une autre expérience consistant à brancher le FrameScope 1 dans le VPN ETS2 derrière CE3, c'est-à-dire sur le VLAN 533, et d'essayer de le rejoindre depuis le FrameScope 2, toujours branché dans le VPN ETS3 derrière CE3 (VLAN 535).

Nous lançons depuis le FrameScope 2 (dont l'adresse est 10.70.31.100) la commande traceroute vers le FrameScope 1 qui possède l'adresse 10.60.31.100. Bien que les résultats obtenus par le FrameScope 2 soient toujours négatifs, pour les mêmes raisons que précédemment, un évènement intéressant se produit au niveau du FrameScope 1.

Une des spécificités des FrameScopes est d'afficher par défaut leur environnement réseau, c'est-à-dire tous les équipements réseaux tels que routeurs, ordinateurs, serveurs, etc. auxquels ils sont connectés, en utilisant les paquets qu'ils

reçoivent (mises à jour des protocoles de routage, entre autres). Ces équipements peuvent être dans le même sous-réseau mais aussi distants.

Or le FrameScope 1, après le saut 9 de la commande *traceroute* émise par le FrameScope 2, affiche sur son écran une nouvelle station distante, avec l'adresse 10.70.31.100, autrement dit l'adresse du FrameScope 2. Il y a bien une connectivité entre les deux FrameScopes, donc entre les deux VRF ETS2 et ETS3, bien que celle-ci soit unidirectionnelle ETS3 → ETS2.

3.3.4 Bilan

Ces tests ont montré que sous certaines conditions une ressource partagée peut permettre à deux VPN ne se voyant pas de pouvoir communiquer entre eux, au moins de façon unidirectionnelle. La condition de réussite de cette communication est la présence d'une route par défaut vers la ressource partagée dans le VRF du CE et le PE de l'attaquant.

La possibilité de deviner une adresse IP, par essais successifs par exemple, montre que la sécurité par l'obscurité n'est pas suffisante pour garantir la sécurité d'une architecture.

Mais, si l'adresse de destination peut facilement être connue ou devinée (surtout si l'adressage est privé), il n'en va pas de même pour la route par défaut. Le PE n'est en effet pas géré par le client, et le fournisseur de service ne devrait pas implémenter de route par défaut dans les VRF, sauf pour la connectivité Internet. Par contre, il est toujours envisageable que des erreurs de configuration soient présentes, ou de façon plus élaborée le client malveillant pourrait utiliser des techniques d'ingénierie sociale pour demander au fournisseur de service d'ajouter une route vers une zone légitime (la ressource partagée). Si le fournisseur de service n'est pas au courant des complications que cela peut causer, pourquoi refuserait-il? Une route par défaut vers une ressource

légitime dans un VRF appartenant au client en faisant la demande peut sembler raisonnable…

L'autre possibilité pour l'attaquant est de tenter de corrompre le protocole MP-BGP afin d'ajouter la route par défaut. Le chapitre 4 présente à cet égard une étude de la sécurité du protocole BGP.

CHAPITRE 4

SÉCURITÉ DU PROTOCOLE BGP

Le but de ce chapitre est d'analyser la sécurité du protocole BGP, utilisé sous sa variation de MP-BGP pour réaliser l'échange de routes entre les différents VPN. Cette étude devrait aussi permettre de voir de quelle façon l'attaque dans la connectivité Extranet présentée dans les parties 3.1 et 3.3 est reproductible.

La condition nécessaire permettant la réalisation de cette attaque étant la présence d'une route par défaut dans le CE et le PE pointant vers la ressource partagée, si elle peut être considérée comme évidente dans le CE, administré en général par le client, il n'en va pas nécessairement de même concernant le PE, géré par le fournisseur de service.

Toute la difficulté de cette étude est d'établir s'il est possible d'injecter une route par défaut dans un routeur PE, depuis le client (ou son CE), mais dirigée vers la ressource partagée, située de l'autre côté de ce PE. De plus, les protocoles de routage ne sont pas toujours les mêmes de part et d'autre du PE. Le fournisseur de service utilise BGP au-delà du PE, par contre c'est généralement OSPF qui est utilisé entre CE et PE (Rosen, Psenak et Pillay-Esnault, 2006), bien que RIP, BGP ou un routage statique soient aussi possibles.

4.1 Généralités sur le protocole BGP

Le protocole BGP permet le routage inter domaine. Il est notamment utilisé pour échanger les informations de routage sur Internet afin de relier entre eux les différents fournisseurs de service, représentés par des systèmes autonomes, nommés AS. C'est en effet le seul protocole pouvant supporter un très grand nombre de routes à annoncer (actuellement, près de 225000 routes sont contenues dans les tables de routage d'Internet (Smith, 2007, 28 juin)) et qui permet de maintenir une certaine stabilité du routage. Pour

cela, BGP utilise notamment l'agrégation de routes, qui consiste à réunir en un seul préfixe (adresse réseau + masque explicite, par exemple 154.23.64.192/26) différentes adresses réseaux, en utilisant le principe de CIDR (Classless Inter-Domain Routing). Sur les 225000 routes précédentes, l'agrégation permet de limiter le nombre d'entrées à moins de 120000, soit presque deux fois moins.

Le routage dans BGP fonctionne par l'échange de messages *UPDATE* qui contiennent trois éléments :

- Les préfixes qui ne sont plus joignable par une route précédemment annoncée,
- Les attributs du chemin traversé depuis les préfixes annoncés, sous la forme d'un vecteur comportant les numéros d'AS traversés (AS_PATH),
- Les préfixes qui sont annoncés.

Chaque locuteur BGP (communément appelé BGP *Speaker*) propage les messages *UPDATE* reçus en y ajoutant son numéro d'AS dans l'attribut AS_PATH, sauf s'il y apparaît déjà. Dans ce cas, il supprime le message reçu, ce qui permet d'éviter les boucles de routage. L'échange de ces messages et des autres messages BGP (OPEN, etc.) se fait par l'intermédiaire de TCP. Les messages *UPDATE* ne sont généralement envoyés qu'en cas de changement dans le réseau.

BGP n'ayant été conçu que pour transporter des routes IPv4, cela créait une limitation pour le routage de nouvelles technologies réseau. MP-BGP, qui n'est qu'une extension de BGP, a ainsi été standardisé (Bates et al., 2007) pour permettre l'ajout d'informations supplémentaires aux messages *UPDATE* ; dans le cas des VPN sur MPLS il s'agit d'information sur les routes VPN échangées (*target VPN*, *VPN-of-origin*, *site-of-origin*).

Il n'est pas question ici de présenter dans le détail le protocole BGP, pour cela il est possible de consulter la RFC 4271 (Rekhter, Li et Hares, 2006). L'aspect qui nous intéresse plus particulièrement est la sécurité de BGP.

4.2 Évaluation de la sécurité du protocole BGP

Les faiblesses liées à la sécurité de BGP proviennent en partie du fait que ce protocole a été créé à une époque où les chercheurs étaient les seuls utilisateurs d'Internet. De nos jours, Internet est utilisé par des millions de personnes, supporte de nombreuses applications et est ainsi sujet à des attaques diverses qui remettent en cause la sécurité des protocoles de routage.

Les attaques sur BGP peuvent se produire en attaquant la communication entre deux pairs BGP, mais aussi en injectant des informations erronées qui vont être reprises par les pairs BGP. L'attaque de la communication va se faire par détournement de session, mystification d'adresse IP ; autrement dit grâce aux protocoles sous-jacents.

La RFC4272, *BGP Security Vulnerabilities Analysis* (Murphy, 2006), présente les vulnérabilités de BGP. Ce document décrit les failles possibles de BGP, ainsi que la manière de les mettre à profit.

La communication entre les pairs BGP peut être sujette à une écoute passive ou active. Le protocole de transport, TCP, peut être attaqué car non protégé, que cela concerne les données de contrôle, ou les données de la charge utile. Cela peut permettre l'injection de messages BGP sur un lien, la modification de messages BGP légitimes, ou l'annonce illégitime de routes par un émetteur BGP compromis.

Les attaques visant l'échange de messages entre pairs BGP via TCP sont le fait d'un attaquant extérieur. Mais si un des pairs BGP se met à annoncer n'importe quoi, les autres pairs vont relayer l'information sans même la vérifier. Il y a ainsi quatre types d'attaques : l'annonce de préfixes illégitimes, l'annonce de sous-préfixes illégitimes (plus dangereux et plus difficile à stopper que le précédent type car lorsqu'il a le choix

entre plusieurs préfixes de longueur différente, BGP choisit préférablement le préfixe ayant le masque le plus élevé possible), mais aussi la mystification du chemin dans les annonces de routes. Ce troisième type d'attaque, plus rare, survient lorsqu'un pair BGP annonce non pas qu'il possède un préfixe mais qu'il fait partie du chemin invalide vers ce préfixe, ce qui lui permet de lire les données qui passeront par lui. Enfin, un quatrième type d'attaque consiste à détruire des paquets de mises à jour légitimes créant ainsi des trous noirs et des boucles infinies (Ke, Xiaoliang et Wu, 2004).

Les problèmes de sécurité de BGP proviennent davantage du fait que l'information transmise par les pairs n'est pas vérifiée (par exemple : est-ce que tel pair a le droit d'annoncer telle route), plutôt que de l'authenticité des pairs BGP. Bien sûr, il est préférable qu'il n'y ait pas de pair BGP illégitime annonçant de fausses routes, mais même si c'est le cas, cela ne signifie pas pour autant que le protocole est sécurisé, comme l'a montré l'incident FLIX (*Florida Internet Exchange*, AS7007). Cet incident est survenu en 1997 lorsqu'un AS s'est mis à annoncer toutes les routes de l'Internet provoquant entre autres une explosion des tables de routage et une indisponibilité globale d'Internet. Il a été par la suite découvert que cet incident n'est lié qu'à un bug logiciel du routeur. D'autres incidents similaires (AS8584 en 1998, AS15412 en 2001, AS174 en 2005) se sont produits par la suite.

4.3 La sécurité actuellement utilisée : MD5

La sécurité dans BGP se limite plus ou moins à la phrase suivante d'après la dernière version du standard sur BGP (Rekhter, Li et Hares, 2006) : « *A BGP implementation MUST support the authentication mechanism specified in RFC 2385*».

La RFC2385, *Protection of BGP Sessions via the TCP MD5 Signature Option* (Heffernan, 1998) présente l'utilisation de MD5 (Rivest, 1992) pour empêcher l'introduction de segments TCP mystifiés dans la communication entre les voisins BGP.

Chaque segment TCP contient une empreinte de 16 octets obtenue en appliquant l'algorithme MD5 sur différents éléments du segment, dans l'ordre :

- le pseudo-entête préfixé à TCP (adresse IP source, adresse IP destination, numéro de protocole, longueur du segment),
- l'entête TCP, sans les options, et avec un checksum supposé nul,
- les données (le cas échéant),
- une clé connue par les deux voisins, et idéalement spécifique à chaque connexion.

Cette empreinte est placée dans le champ Options de l'entête TCP. Elle permet d'authentifier les pairs BGP mais pas de vérifier les informations transmises : le chemin pris par les routes ni leur origine.

Concernant les vulnérabilités de MD5 face à des attaques de recherche de collisions (montrées en 1996 par Dobbertin (Dobbertin, 1996) et en 2004 par une équipe chinoise (Wang et Yu, 2005)), la seule solution suggérée est le remplacement de MD5 par un autre algorithme plus sécuritaire, comme SHA-1 (*Secure Hash Algorithm*). Cette solution impliquerait d'ajouter un champ définissant l'algorithme utilisé, entre autres, ce qui resterait à développer. L'inconvénient, c'est que la sécurité de SHA-1 commence déjà à être remise en question, avant même d'avoir été adoptée. La même équipe chinoise a décelé en 2005 (Wang, Yin et Yu, 2005) des collisions complètes sur SHA-1 nécessitant 2^{63} opérations, ce qui bien qu'important est réalisable avec du calcul distribué. Heureusement, ces collisions ne permettent pas de trouver à partir d'une empreinte fixée un message, mais éventuellement deux messages aléatoires produisant une même empreinte. Néanmoins, les experts conviennent qu'il serait maintenant préférable d'utiliser SHA-256, comportant une clé de 256 bits au lieu de 160, à la place de MD5.

L'utilisation de MD5 pose un autre problème : celui-ci n'inclut pas de méthode de gestion des clés utilisées. Il est donc nécessaire de choisir les clés pour chaque

association de pairs BGP statiquement, ce qui est fastidieux et peut augmenter le risque d'erreur à long terme, si la clé n'est jamais changée. L'utilisation d'IPSec (Kent et Atkinson, 1998) ou de TLS (Dierks et Allen, 1999), parfois suggérée, permettrait d'améliorer quelque peu la sécurité au niveau de l'authentification des pairs. Cela n'est pourtant que très rarement effectué.

En ce qui concerne la sécurité des communications entre les voisins BGP, l'utilisation de MD5 est une solution reconnue comme faible mais utilisée actuellement. En outre, cette solution ne permet pas d'empêcher l'échange d'informations fausses par les pairs BGP légitimes. Des mécanismes plus forts devraient être utilisés dans le futur.

Comme nous pouvons le voir, la méthode actuelle, pourtant fortement conseillée (en témoigne le « *MUST* » utilisé dans la RFC4271 qui date de 2006), n'est pas infaillible ; en outre elle ne concerne qu'une partie de la sécurité du protocole (l'authenticité des pairs BGP). Il peut être nécessaire de se tourner vers les nouvelles avancées proposées par BGP, que sont *Secure BGP* (S-BGP) et *Secure origin BGP* (soBGP). La RFC4272 suggère d'ailleurs comme solutions la protection de l'origine et de l'adjacence par l'utilisation de signatures (Smith et Garcia-Luna-Aceves, 1996), la protection de la route et de l'origine (Kent, Lynn et Seo, 2000), ainsi que le filtrage basé sur les registres Internet pour vérifier certains attributs des messages UPDATE (Villamizar et al., 1999).

Il existe néanmoins en plus de MD5 quelques techniques permettant de renforcer quelque peu la sécurité actuelle de BGP. Parmi celles-ci se trouve le mécanisme de contrôle du champ TTL (Gill, Heasley et Meyer, 2004) qui s'applique surtout aux sessions eBGP en empêchant d'accepter les mises à jour de routage provenant d'éléments distants. La partie 2.2.2.5 présente le fonctionnement de ce mécanisme, qui toutefois n'améliore pas l'authentification des chemins annoncés par les routes ni l'origine de ces dernières. À part ce mécanisme, les fournisseurs de service peuvent utiliser une adresse *loopback* ou secondaire pour réaliser l'appariement avec les autres

routeurs BGP (Dubee, 2003), utiliser la commande de route *dampening* appliquant une pénalité aux routes qui changent souvent d'état, effectuer un filtrage sur les annonces de routes reçues ou émises, par exemple vérifier si telle route a le droit d'être annoncée par l'AS qui le fait, s'il est lui-même autorisé à émettre tel préfixe, mettre en quarantaine des préfixes ayant fait l'objet de mises à jour incessantes, bloquer les annonces de routes comportant des adresses privées, etc.

4.4 Les extensions proposées pour renforcer la sécurité de BGP

Cette partie présente quelques extensions proposées au protocole BGP afin de le rendre plus sécuritaire. Secure BGP a été la première proposition, et semble la plus concrète. D'autres propositions ont suivi, éventuellement plus simples à adapter à BGP.

4.4.1 Secure BGP (S-BGP)

Secure BGP (Kent, Lynn et Seo, 2000) est une extension permettant de résoudre la plupart des problèmes de sécurité du protocole BGP, en l'occurrence S-BGP permet de s'assurer du respect des propriétés suivantes :

- chaque message UPDATE reçu de la part d'un émetteur (BGP Speaker) donné provient bien de cet émetteur, n'a pas été modifié durant son transport, et ne contient pas d'informations plus anciennes que celles contenues dans un message précédemment reçu,
- le destinataire du message UPDATE s'attendait bien à le recevoir,
- l'émetteur possédait le droit au nom de son AS d'envoyer les informations de routage contenues dans le message UPDATE,
- le propriétaire de tout préfixe annoncé dans un message UPDATE possède bien l'espace d'adressage associé (enregistré auprès d'un registre Internet),
- le premier AS sur les routes annoncées est bien autorisé par les propriétaires des préfixes atteignables à annoncer ces préfixes. Ce point permet notamment d'éviter des incidents du type FLIX (*cf.* partie 4.2),

- l'émetteur supprimant des préfixes préalablement annoncés était bien autorisé à les annoncer.

Par contre, S-BGP ne garantit pas que l'émetteur du message UPDATE applique convenablement les règles de BGP et les politiques internes à l'AS de modification, d'enregistrement et de distribution du message, ainsi que de sélection de route ; de même que le pair BGP ayant reçu le message UPDATE applique correctement lui aussi les règles de BGP et politiques internes à l'AS quant à accepter ou non le message UPDATE.

Ceci n'est pas permis par S-BGP car les caractéristiques de politique locale de BGP laissent une trop grande latitude aux pairs BGP quant à la façon de traiter les messages UPDATE. Remédier à ceci nécessiterait de changer la sémantique de BGP.

S-BGP utilise deux infrastructures à clés publiques (Seo, Lynn et Kent, 2001), basées sur des certificats X.509, pour permettre de valider les identités et autorisations des pairs BGP, des propriétaires des AS et de leurs espaces d'adressage. Une de ces infrastructures est utilisée pour l'allocation d'adresse, l'autre pour l'assignation des AS et l'association des routeurs. Ces certificats permettent aussi de valider les routes annoncées. En outre, IPSec est utilisé pour protéger les informations échangées. Néanmoins, quelques vulnérabilités énoncées ci-dessus ne sont pas corrigées par S-BGP, car non détectables par les mesures proposées.

Bien que la suggestion de S-BGP comme solution aux problèmes de sécurité de BGP date de 2000, elle n'est pas concrètement utilisée aujourd'hui. Cela parce qu'il est difficile de déployer des infrastructures à clés publiques à l'échelle de l'Internet.

4.4.2 Secure Origin BGP (soBGP)

Le but de soBGP (White, 2003) est de vérifier si l'émetteur d'un message BGP a le droit d'annoncer une route donnée, autrement dit s'il a bien un chemin valide correspondant à la route annoncée. Il ne dépend pas d'une autorité centralisée et ne se base pas sur le routage pour sécuriser BGP. Il propose l'utilisation d'un réseau de confiance (*web-of-trust*).

Afin de rester compatible avec BGP, il ne modifie pas les messages actuels mais ajoute un type de message supplémentaire, dénommé SECURITY. Celui-ci transporte des certificats authentifiant les pairs BGP (*entity certificate*), les espaces d'adressage qu'ils possèdent (*authorization certificate*) et des politiques s'y rapportant (*policy certificate*).

Selon Cisco, soBGP ajoute à S-BGP la possibilité de choisir quelles routes accepter dans un message UPDATE reçu, c'est-à-dire la possibilité d'appliquer des politiques permettant de trier l'information reçue. En outre, soBGP est présenté comme flexible, pouvant se déployer de façon incrémentielle (bien que le niveau de sécurité dépende de la complétion du déploiement). Par contre, la cryptographie (IPSec par exemple) n'est pas utilisée pour protéger les messages UPDATE.

Le déploiement de soBGP nécessite de mettre à jour les logiciels de routage dans les routeurs, d'ajouter une infrastructure permettant de générer des certificats, et une entité d'authentification des certificats provenant de l'extérieur. En 2003, le code pour l'IOS Cisco était en développement, aussi des *drafts* ont été soumis à l'IETF, mais à date aucune RFC n'est sortie à ce sujet.

4.4.3 Pretty Secure BGP (psBGP)

Pretty Secure BGP (Kranakis, van Oorschot et Wan, 2005) est une proposition d'extension à BGP créée en 2005. Elle est supposée combiner le meilleur de S-BGP et

de soBGP. Un de ses avantages est de pouvoir se défendre contre des attaques de pairs BGP mal configurés ou mal intentionnés.

PsBGB approuve l'idée de S-BGP de créer une entité PKI centralisée pour authentifier les numéros d'AS, se basant sur les autorités compétentes telles l'IANA (*Internet Assigned Number Authority*), l'ICANN (*Internet Corporation of Assigned Numbers and Names*) et les registres Internet régionaux (RIR, *Regional Internet Registry*). PsBGP utilise un modèle de confiance centralisé pour réaliser l'authentification des numéros d'AS. Chaque AS obtient un certificat public de l'une des entités de certification comme les RIR, associant une clé publique à un numéro d'AS.

Par contre, PsBGP part du principe qu'il est difficile de créer une PKI centralisée pour vérifier l'appartenance des préfixes aux AS. PsBGP utilise donc un modèle de confiance décentralisé tel que soBGP pour vérifier cette appartenance des préfixes aux AS. Chaque AS doit ainsi vérifier que les associations de préfixes et d'AS qu'il connaît sont les mêmes que celles de ses voisins.

PsBGP permet donc d'authentifier les numéros d'AS, d'authentifier les pairs BGP, de garantir l'intégrité des données par l'utilisation d'IPsec ou de MD5, de vérifier l'origine des préfixes et de vérifier la pertinence du paramètre AS_PATH (attributs du chemin traversé depuis les préfixes annoncés, sous la forme d'un vecteur comportant les numéros d'AS traversés). La surcharge en termes de ressources existe néanmoins, tout comme pour sBGP, principalement concernant la signature ou le chiffrement des messages transmis.

4.4.4 Pretty Good BGP (PGBGP)

Pretty Good BGP (Karlin, Forrest et Rexford, 2006) est une amélioration du protocole BGP qui permet de ralentir la diffusion de routes erronées en privilégiant les chemins

déjà connus pour ces routes. Les routes suspectes sont détectées par les routeurs en consultant une table d'informations de routage valides construite à partir de diverses informations parmi lesquelles le contenu des messages UPDATE reçus auparavant. L'introduction d'un délai permet à l'administrateur de l'AS ou à des systèmes automatisés de vérifier les routes suspectes détectées. Un système d'alerte d'attaques par courriel est proposé, afin de donner la possibilité aux opérateurs de pouvoir réagir durant la phase de délai.

Le fait d'imposer un délai aux nouvelles routes n'est pas dommageable grâce à la redondance offerte par Internet, c'est-à-dire grâce aux multiples chemins permettant de se rendre au même point. Au contraire, cela permet de ne pas tenir compte des problèmes temporaires tout comme les oscillations de routes ; il est aussi possible de vérifier pendant ce temps la validité des routes nouvelles ou suspectes.

Lorsqu'une nouvelle route est annoncée pour un préfixe déjà connu dans la table de « confiance », elle est considérée pendant une durée S (par exemple 24 heures) comme suspecte. Si quand cette durée est écoulée la route annoncée pour ce préfixe est toujours présente dans les mises à jour, elle sera considérée comme valide et sera insérée dans la table de confiance. Enfin, les préfixes n'étant plus annoncés depuis une durée H (variable, par exemple 10 jours) sont supprimés de la table de confiance.

Un avantage de PGBGP est de ne requérir aucune modification du protocole BGP mais simplement une mise à jour logicielle des routeurs. Les désavantages de cette amélioration de BGP sont les fausses alertes positives (un changement de fournisseur de service par exemple), mais surtout la possibilité qu'un attaquant effectue juste avant l'annonce illégitime une attaque de déni de service empêchant l'annonce de la route légitime et permettant à la route illégitime d'être immédiatement considérée comme valide. D'autres solutions comme S-BGP devraient être utilisées conjointement pour éviter ce genre de problème.

4.4.5 Inter-Domain Routing Validator (IRV)

D'autres solutions ont été proposées pour améliorer BGP. Goodell, par exemple, a développé un protocole appelé *Inter-Domain Routing Validator* (IRV) (Goodell et al., 2003), permettant d'améliorer la sécurité et l'exactitude de BGP en combinant des fonctionnalités de S-BGP et du registre de routage Internet (IRR, *Internet Routing Registry*). Chaque AS crée un serveur IRV qui a autorité sur l'information de routage inter-domaine de son AS. Les serveurs IRV peuvent s'interroger pour vérifier et valider les messages UPDATE échangés. Cela permet de détecter une origine de préfixe de même qu'un chemin AS_PATH impropres, en débusquant les éventuelles inconsistances avec les réponses des autres serveurs IRV. La communication entre IRV doit être authentifiée ou chiffrée pour ne pas dévoiler de l'information sensible à n'importe qui.

Un avantage de cette technologie est sa capacité à avoir un déploiement incrémental, puisqu'elle ne nécessite aucun changement dans l'infrastructure de routage. Mais sa limitation principale provient de la nécessité d'un nombre important d'IRV dans des AS distincts afin de pouvoir comparer et vérifier l'information. Une autre limitation est liée à la validité des informations entrées manuellement dans les IRV, pouvant différer de la configuration réelle des routeurs. Des outils automatiques devraient être utilisés lors de la modification de la configuration des routeurs.

4.4.6 Listen and Whisper

Listen and Whisper (Subramanian et al., 2004) représente deux mécanismes utilisés conjointement permettant de protéger le plan de données et le plan de contrôle de BGP. *Listen* écoute passivement le plan de données, vérifie si les données envoyées sur les routes annoncées parviennent à destination et décèle les routes invalides en détectant les connexions TCP douteuses (un paquet SYN qui n'est pas suivi de paquets de données (DATA) dans un laps de temps donné, par exemple 2 minutes).

Whisper détecte les annonces illégitimes de routes au niveau du plan de contrôle en décelant une inconsistance parmi les routes annoncées par plusieurs messages UPDATE, originaires d'un même AS mais utilisant différents chemins (par exemple, le chemin légitime et le chemin illégitime).

Ces deux mécanismes sont faciles à déployer, et ne reposent pas sur une infrastructure à clés publiques ou une autorité centralisée comme l'ICANN. Toutefois, ils ne peuvent que signaler un problème, sans pouvoir identifier sa source. Ils ne peuvent pas non plus prévenir des pairs BGP corrompus écoutant le trafic, injectant ou supprimant des données.

4.4.7 Secure Path Vector (SPV)

Le protocole *Secure Path Vector* (Hu, Perrig et Sirbu, 2004), utilise des primitives cryptographiques efficaces comme les arbres d'authentification et les chaînes de hachage pour protéger les attributs du chemin traversé depuis les préfixes annoncés (le vecteur AS_PATH). Ce dernier est signé à chaque passage par un pair BGP, le contenu du vecteur reçu n'étant alors pas modifiable par les AS subséquents. L'authentification des pairs se fait au saut par saut. Les différentes opérations réalisées utilisent des clés par AS, par époque (les messages UPDATE ayant ici une durée de vie limitée) et par préfixe.

Ce protocole est censé être plus efficace que S-BGP, en remplaçant une cryptographie asymétrique couteuse en temps de calcul par une cryptographie symétrique plus légère et par quelques simplifications. Par exemple, pour authentifier les messages des préfixes, il n'est pas nécessaire d'avoir de PKI, les préfixes devenant alors les clés publiques. Ceci est permis par la cryptographie basée sur l'identité (IBC, *Identity Based Cryptography*).

Il suffit alors à l'autorité de certification de créer les clés privées correspondantes, utilisant de la même façon les préfixes comme clés publiques.

4.4.8 Topology-based detection of anomalous BGP messages

Kruegel (Kruegel et al., 2003) suggère une technique permettant de détecter et de bloquer les annonces de routes illégitimes en écoutant passivement le trafic de contrôle BGP. En utilisant les informations de localisation géographique disponibles dans les bases de données *whois*, une distinction est faite entre les AS de la dorsale Internet (les nœuds cœurs) et les autres AS (nœuds périphériques). Un chemin légitime doit contenir au plus une seule séquence de nœuds cœurs traversés, ce qui signifie qu'un chemin traversant plusieurs nœuds cœurs puis un nœud périphérique et à nouveau des nœuds cœurs a toutes les chances d'être illégitime et détourné par un AS malveillant. Par ailleurs, un chemin légitime ne doit passer que par des nœuds périphériques géographiquement proches les uns des autres. En construisant un graphe de connectivité des AS et en analysant le contenu de l'attribut AS_PATH, il est alors possible de déterminer si le chemin reçu est légitime ou pas, et donc s'il faut l'accepter ou le bloquer.

Cette méthode a l'avantage de fonctionner sans aucune modification de l'infrastructure et ne nécessite pas un déploiement important pour être performante localement, se basant sur la connectivité des AS pour vérifier la cohérence des annonces de routes avec la topologie du réseau. C'est donc une méthode simple à implanter. Les limitations de cette solution sont liées à la modification de la topologie réseau, l'ajout de nouvelles connexions entre AS par exemple pouvant être perçu comme un détournement du chemin. Il serait nécessaire avec cette solution de recréer le graphe de connectivité lorsqu'un changement dans la topologie survient.

4.5 Bilan

BGP est un protocole qui n'a pas été conçu avec l'idée d'être sécuritaire, mais fonctionnel et efficace. Ce qui au départ n'était pas un obstacle se révèle aujourd'hui être un problème pour l'Internet tout entier, car celui-ci dépend de ce protocole pour réaliser les annonces de routes à travers la planète.

Bien que plusieurs extensions aient été proposées pour améliorer la sécurité de BGP (S-BGP, soBGP, psBGP, PGBGP, mais aussi IRV, SPV, *Listen&Whisper*, etc.), elles ne sont pas encore mises en œuvre de façon pratique. Des problèmes de gestion et de performance (Zhao, Smith et Nicol, 2005) restent à être résolus, la surcharge créée par l'ajout de la sécurité en termes de bande passante, d'utilisation de la mémoire et du processeur étant loin d'être négligeable. La sécurisation de BGP existe donc aujourd'hui principalement sous la forme de surveillance manuelle et de l'utilisation de filtres (par exemple, le mécanisme de TTL élevé) par certains fournisseurs de service. Bien que cela ne permette pas d'empêcher les attaques, toute irrégularité peut à tout le moins être détectée (Dubois et al., 2004). La seule notion de sécurité qui a été ajoutée à BGP depuis ses débuts est l'obligation d'utiliser MD5 pour authentifier les pairs BGP. Mais cette solution (*cf.* section 4.3) ne rend pas le protocole BGP complètement sécuritaire. Elle permet tout au plus d'éviter l'injection de messages dans la communication entre deux pairs et aucunement de vérifier la légitimité des pairs.

En comparant les extensions actuellement proposées, il est évident que les plus avancées semblent être S-BGP et soBGP. Pour parvenir à un objectif similaire à S-BGP (sécuriser le protocole BGP), soBGP emploie une méthode différente avec l'ajout d'un nouveau type de message (SECURITY), alors que S-BGP ne change pas la sémantique ou le vocabulaire utilisé. S-BGP n'est pas pour autant plus simple à mettre en œuvre. Cela est dû aux choix de conception architecturaux dans les deux cas, les infrastructures

hiérarchiques à clés publiques. Par ailleurs, de l'avis de la plupart des experts travaillant sur la sécurisation de BGP, S-BGP est trop lourd pour être déployé.

PsBGP, une idée plus récente, se situe à mi-chemin entre S-BGP et soBGP, essayant de combiner leurs meilleures idées – architecture centralisée et décentralisée. Mais comme ces deux extensions, psBGP essaye de se concentrer sur la sécurité au détriment des performances. La cryptographie utilisée dans ces extensions ajoute une surcharge non négligeable, voire trop importante, tout comme la nécessité d'employer des infrastructures à clés publiques, lourdes à mettre en place.

PGBGP apporte la simplicité, sans nécessiter d'architecture lourde ou de chiffrement des messages, mais induit un délai avant acceptation des mises à jour. La convergence du protocole est alors moins rapide, ce qui est une limitation importante, surtout dans le cadre de MPLS, pouvant créer des associations d'étiquettes VPN rompues.

La solution est peut-être parmi les propositions plus légères à mettre en place, comme IRV, SPV, *Listen&Whisper*, etc. Il reste à voir si ces solutions vont être développées dans le futur.

Pour la plupart des solutions, c'est la centralisation de l'information qui pose problème : qui doit jouer ce rôle? À qui est-il possible de faire confiance? En outre, la plupart des solutions impliquent une utilisation de la cryptographie, la modification du protocole BGP, du logiciel des routeurs, etc. Vu le déploiement actuel de BGP, il est ainsi aisé de comprendre pourquoi aucune n'a été jusqu'ici adoptée.

4.6 Lien avec les tests réalisés

Concernant le point qui a suscité cette étude, à savoir si la faille trouvée dans les tests précédents est valable, et quelles mesures adopter pour la prévenir, considérons différents cas :

- Si la ressource partagée est utilisée pour accéder à Internet, une route par défaut est obligatoire pour permettre l'accès à Internet. L'utilisation de pare-feux est indispensable.
- Si BGP est correctement configuré sur le réseau, il n'est normalement pas possible d'injecter une route dans le PE depuis un routeur qui ne fait pas partie des pairs BGP légitimes, même sans utiliser des versions améliorées de BGP comme S-BGP ou SecureBGP. De simples listes d'accès doivent suffire.
- La seule possibilité consisterait à se faire passer pour un voisin (*BGP neighbor*) en mystifiant l'adresse IP (*IP spoofing*) d'un routeur du réseau MPLS. Est-ce toutefois réalisable? Dans notre cas, les signatures MD5 ou l'authentification de l'origine (Aiello, Ioannidis et McDaniel, 2003) devraient être utilisées, afin d'éviter des mises à jour par un utilisateur non autorisé.

Il faut noter que dans le cas de notre étude, il n'y a qu'un seul AS. Mais ici, ce n'est pas BGP qui est utilisé pour faire le routage inter-domaine, mais son extension MP-BGP pour réaliser l'échange de routes VPN entre les routeurs PE. Nonobstant, MP-BGP se comporte exactement de la même façon que BGP et ne change pas les problèmes de sécurité existant dans ce dernier.

MPLS ne donnant pas accès au cœur du réseau, la méthode permettant d'attaquer MP-BGP en se plaçant entre deux pairs et en attaquant le protocole TCP pour injecter des mises à jour est difficilement réalisable. MP-BGP ne s'exécutant qu'entre les routeurs PE et non pas à l'extérieur du cœur, il n'y a aucun point d'accès pour un attaquant. De plus, le vol de session TCP n'est pas nécessairement évident, bien que faisable.

L'autre méthode, qui consiste à corrompre un pair BGP pour émettre des mises à jour illégitimes nécessite de prendre le contrôle d'un routeur PE. En respectant les conseils précédemment énoncés et les recommandations du chapitre 3, il ne devrait pas être possible de réaliser cette opération.

CHAPITRE 5

PRÉCEPTES FONDAMENTAUX

Ce chapitre a pour objectif de suggérer des principes de base à suivre afin de permettre de garantir le fonctionnement sécuritaire des réseaux privés virtuels sur MPLS en considérant l'état actuel des standards et les moyens aujourd'hui disponibles. Quelques conseils ont déjà été émis tout au long de ce mémoire, en particulier au fil de l'analyse des failles possibles se basant sur des réseaux existant. Certains de ceux-là, déjà évoqués, sont néanmoins examinés de nouveau, sous un angle différent cette fois, puisque cette partie propose d'évaluer au pas à pas l'élaboration d'un plan de sécurité sur MPLS en suivant les étapes de la création de ce dernier. Bien entendu, ils sont également enrichis d'autres principes couvrant certains points qui n'ont jusqu'à maintenant toujours pas été abordés. Concrètement, la création d'un VPN dans un réseau MPLS est analysée. À chaque étape, les failles possibles et des conseils sont présentés. Ensuite, des recommandations plus générales sont données.

5.1 Sécurité de la création d'un VPN dans un réseau MPLS/VPN

Cette partie présente une étude de la sécurité du design de MPLS/VPN. Chaque étape nécessaire à la création d'un VPN sur le réseau MPLS/VPN est dépendante de protocoles, qu'il s'agisse de protocoles de routage, de signalisation, etc. Ces protocoles peuvent contenir des failles exploitables sous certaines circonstances.

L'objectif de cette étude est de présenter pour chaque étape majeure de la création du réseau MPLS/VPN les failles possibles, et les recommandations sous forme de conseils permettant d'éviter qu'un attaquant ne puisse exploiter quelque faille que ce soit.

Cette étude se base sur un réseau MPLS/VPN mono-cœur, et ne tient pas compte des réseaux évolués de type multi-cœurs ou hiérarchisés (*Carrier's Carrier*). Aussi, seuls

des VPN simples sont envisagés. Le cas de VPN partagés (accès à Internet, Extranet, etc.) a fait l'objet d'une étude particulière dans les parties 3.1, 3.2 et 3.3. Bien que l'environnement utilisé soit celui de Cisco, cette étude ne considère pas les bugs et failles possibles de l'IOS Cisco.

La première étape consiste à effectuer le routage des routeurs du réseau cœur MPLS, afin que les routeurs PE puissent se parler entre eux. Ensuite, il faut créer au niveau des PE une instance de VRF puis transmettre les informations sur le VRF ainsi créé aux autres PE. En outre, il faut établir les LSP qui vont pouvoir échanger les données par la suite dans le réseau MPLS. Le routage entre PE et CE doit aussi être considéré, puisqu'il faut bien diriger les paquets de la porte de sortie du client (le routeur CE) à la porte d'entrée du réseau MPLS (le routeur PE).

5.1.1 Routage intra-cœur MPLS

Il s'agit du routage utilisé au sein du réseau cœur MPLS, c'est-à-dire entre les différents routeurs P et PE. Il permet aux routeurs du réseau de communiquer les uns avec les autres.

5.1.1.1 Protocoles utilisés

Un protocole de routage IGP va être utilisé, tel que RIP ou OSPF. Plus le réseau est grand, plus OSPF va être conseillé de par sa convergence plus rapide et sa meilleure stabilité.

5.1.1.2 Failles possibles

Les failles vont ici concerner le protocole de routage utilisé, RIP ou OSPF. Les deux protocoles, bien que fonctionnant de manière assez différente (à vecteur de distance pour RIP, à état de lien pour OSPF), vont pouvoir être trompés si un routeur espion (*rogue*

router) est ajouté dans le réseau. RIPv1 ne propose aucune protection, par exemple, contre l'annonce de routes inexistantes ou déformées.

Un déni de service peut ainsi être créé, mais surtout lire le contenu de tous les paquets échangés (en maintenant le routage des paquets). Si aucune mesure de sécurisation des échanges du protocole de routage RIP n'est prise, le réseau MPLS/VPN va alors pouvoir fonctionner de manière totalement transparente, sans trouble apparent, alors que toutes les informations qui transitent par le cœur vont pouvoir être lues par le routeur espion. C'est une attaque du type *Man in the middle*.

OSPF est plus complexe car les messages que peut transmettre un routeur espion ne vont pas nécessairement être pris en compte étant donné le fonctionnement de ce protocole. Néanmoins, avec une inondation prolongée, il semblerait possible de créer une attaque similaire à RIP décrite ci-dessus.

Si le routage IGP est compromis, l'attaquant va pouvoir recevoir les données de tout le monde – quitte à les redistribuer par la suite pour que l'attaque soit transparente. Les étapes subséquentes en subiront les conséquences : il y a possibilité de brèche entre plusieurs VPN.

5.1.1.3 Conseils

En premier lieu, nous pouvons fortement suggérer l'utilisation des dernières versions des protocoles de routage, comblant certains manques ou éventuellement certains problèmes de sécurité. Mais ce n'est pas suffisant. Bien que RIPv2 supporte l'authentification, celle-ci se limite à l'utilisation d'un mot de passe transmis en clair. Si cela permet au routeur recevant l'annonce RIP non authentifiée de ne pas en tenir compte, il suffit d'écouter le trafic circulant sur le réseau pour connaître le mot de passe, et ainsi l'utiliser dans un routeur espion. OSPF supporte aussi cette authentification simple.

Idéalement, afin de ne pas permettre à un routeur espion de s'ajouter dans le réseau, il est nécessaire de réaliser une authentification des voisins. Ainsi chaque routeur peut être certain que les annonces de routes reçues sont légitimes. Deux RFC présentaient déjà en 1997 pour RIP (Baker et Atkinson, 1997) et OSPF (Murphy, Badger et Wellington, 1997) des méthodes d'authentification, utilisant MD5 ou les signatures numériques. OSPFv2 (Moy, 1998) peut pour sa part utiliser une authentification par secret partagé, utilisant MD5, similaire à la signature des messages TCP par MD5 (Heffernan, 1998).

Par contre, une authentification avec l'adresse IP source ne suffit pas. Il est possible à un attaquant de réaliser une mystification de l'adresse IP et donc de passer outre cette authentification. Il ne faut pas se fier uniquement au simple contenu des entêtes ajoutés par les différentes couches pour réaliser une authentification. Cela peut permettre de filtrer une partie des attaques, en supprimant les paquets provenant de sources non autorisées, mais pas de garantir une sécurité absolue.

Finalement, parce qu'il est plus difficile de briser le fonctionnement normal d'un protocole à état de liens comme OSPF comparativement à un protocole à vecteur de distance comme RIP, il est préférable d'utiliser OSPF comme protocole de routage pour le réseau cœur MPLS.

5.1.2 Le routage CE-PE

Le routage dans le réseau cœur MPLS/VPN a cet avantage d'être protégé naturellement à partir du moment où il est impossible d'accéder au réseau cœur. Par contre, le routage entre PE et CE est différent : le CE est en général administré par le client du service MPLS/VPN et le lien PE-CE n'est pas protégé.

5.1.2.1 Protocoles utilisés

Le protocole de routage CE-PE peut être soit dynamique avec RIP, OSPF, mais aussi eBGP ou tout simplement une route statique.

5.1.2.2 Failles possibles

Si un attaquant peut intercepter les échanges CE-PE, il peut réaliser une attaque *Man in the Middle*. Mais il n'est pas nécessaire pour cela de briser le protocole de routage, il suffit de se placer entre le CE et le PE. Ce qui est par contre important est d'éviter que des routes inexistantes soient envoyées au PE, afin de ne pas compromettre le VPN concerné. Cela ne compromet toutefois pas l'étanchéité des VPN, sauf si sur le lien CE-PE passent plusieurs VPN sous la forme de VLAN par exemple (si Ethernet est utilisé au niveau 2). Dans ce cas, un attaquant pourrait, tout comme il pouvait éventuellement changer les étiquettes VPN dans le réseau cœur, modifier les tags VLAN des paquets et ainsi briser l'étanchéité des VPN. C'est le même problème que pour le changement d'étiquette VPN (voir partie 2.3), mais au niveau 2 cette fois-ci. Toutefois la présence du checksum de l'entête Ethernet rend cette pratique plus difficile.

Les failles de RIP, OSPF décrites dans la partie précédente (routage intra-cœur) sont aussi valables ici.

5.1.2.3 Conseils

Généralement, l'authentification mutuelle du CE avec le PE est réalisée avec MD5. Ou du moins, il est fortement conseillé d'utiliser MD5, alors qu'en pratique, cela est rarement effectué. Si PPP est utilisé au niveau 2, il est aussi possible d'utiliser une authentification par PPP (Lloyd et Simpson, 1992).

OSPF étant en général employé comme protocole de routage IGP chez le client, la RFC4577 (Rosen, Psenak et Pillay-Esnault, 2006) suggère son utilisation sur le lien PE-CE comme une simplification pour le client. Au niveau sécurité par contre, cela n'apporte pas grand-chose. Idéalement, le routeur CE et le routeur PE doivent être reliés directement.

Le routage statique est le plus sûr, aucune route ne peut alors être introduite par un intrus. BGP a aussi ses avantages, proposant d'autres mécanismes tels que la commande *maximum-prefix* qui limite le nombre de routes que le routeur doit accepter afin d'éviter un déni de service par surconsommation des ressources du processeur ou de la mémoire.

Enfin, s'il n'est pas possible de faire autrement, le chiffrement des communications entre CE et PE par IPsec est possible, bien que s'il est effectué, ce sera généralement de CE à CE. Ce chiffrement permet de protéger un VPN contre des écoutes, intrusions ou injections de trafic. Il ne protège par contre pas contre les attaques internes aux VPN ou sur le cœur. Nonobstant, il faut s'attendre avec ce chiffrement à des dégradations en termes de performances.

5.1.3 Création des VPN

Pour permettre la création de VPN sur MPLS dans une architecture Cisco, il est nécessaire d'employer des *Route Distinguisher* (RD), transformant les adresses IPv4 en adresses VPNv4 (voir le détail dans la partie 1.2.5.1), ainsi que des *Route Target* (RT). Ce processus est réalisé manuellement sur chaque routeur PE. Les *route distinguishers* créent ainsi l'isolation entre les différents VPN et rendent possible l'emploi d'espaces d'adressage se chevauchant. Le but d'un RT est de permettre d'importer les routes correspondant au VPN qui lui est lié d'un ou de plusieurs routeurs PE distants au routeur PE local afin de pouvoir réaliser l'acheminement des paquets au sein du VPN. Une

étiquette spécifique est attribuée par chaque routeur PE *egress* par instance de VRF, éventuellement par interface de sortie ou FEC.

5.1.3.1 Protocoles utilisés

Afin de transmettre à travers le réseau MPLS les annonces de routes, le protocole MP-BGP est utilisé. Il fonctionne sur le même principe que BGP, en lui ajoutant des attributs supplémentaires, connus sous le nom d'informations étendues (*extended communities*).

Les PE utilisent MP-BGP pour transmettre leurs mises à jour sur le réseau MPLS. Ces mises à jour, qui sont des redistributions de routes apprises par le routage PE-CE pour chaque VPN, contiennent les informations exportées par chaque instance de VRF (représentée par une table de routage virtuelle dans un PE) avec, entre autres, le(s) préfixe(s) réseau(x), les RD-RT, le prochain saut, ainsi que l'étiquette VPN à utiliser. Ainsi, chaque routeur PE sait quel est le prochain saut permettant d'atteindre un préfixe donné au sein d'un VPN. Il faut noter que la séparation toute entière est basée sur l'étiquette VPN. Lors de la réception d'un paquet depuis le cœur du réseau, MPLS consultera l'étiquette VPN pour savoir dans quelle table VRF regarder, autrement dit à quel VPN le paquet est associé.

5.1.3.2 Failles liées à MP-BGP

S'il est possible d'intervenir dans l'échange des messages des sessions MP-BGP, le contenu des préfixes annoncés de même que la valeur des étiquettes, etc. peuvent être modifiés. Cependant, pour y parvenir, il faut pouvoir accéder au cœur, et attaquer au bon moment (en interceptant le premier échange MP-BGP par exemple, ou en supprimant des routes existantes en envoyant d'autres préfixes pour un même VPN).

5.1.3.3 Attaque directe sur l'étiquette

Étant donné l'absence de chiffrement tant au niveau des données que des entêtes des paquets VPN circulant sur le réseau, s'il est possible d'intercepter des paquets, il va être possible en changeant l'étiquette VPN de les diriger vers une autre destination que celle prévue ; donc de briser l'étanchéité des VPN. Et le plus intéressant est que cette technique d'attaque est indétectable, car il n'y a pas de contrôle de somme (*checksum*) réalisé sur l'entête MPLS. Par contre, cette attaque est à sens unique (Rey, 2006). Il n'est possible que d'envoyer des données d'un VPN vers un autre, mais pas de recevoir de réponse. Cela suffit cependant à transmettre des vers.

Néanmoins, cela suppose la possibilité d'accéder aux routeurs du cœur, du moins à un PE. Ce qui est généralement présenté comme impossible.

5.1.3.4 Conseils

Les failles ne deviennent exploitables que s'il est possible de communiquer avec le cœur. Il faut donc le rendre invisible. Pour cela il existe un moyen assez simple : il suffit de désactiver la fonctionnalité MPLS *traceroute* qui permet, tel la commande *traceroute* du monde IP, de déterminer les points de passage des paquets dans le réseau MPLS. Si cette commande est activée, il est possible de déterminer l'adresse IP des routeurs traversés dans le réseau cœur MPLS. En la désactivant, le champ TTL de IP n'est pas copié dans le champ correspondant de l'entête MPLS, et par conséquence le nuage MPLS apparait comme transparent.

Afin d'empêcher l'accès au cœur, au cas où les adresses des routeurs du cœur pourraient être connues ou devinées, il faut utiliser des listes d'accès (*access list*, ACL) situées à l'entrée des routeurs PE. Lorsqu'un paquet IP provenant d'un VPN ou de l'extérieur a comme adresse de destination une adresse du réseau cœur, il doit être automatiquement

détruit. En outre, il peut aussi être utile de filtrer les paquets entrants qui possèdent une adresse source différente de l'espace alloué ou utilisé par le VPN concerné.

Au sujet des *route distinguishers*, il est conseillé de choisir un RD unique par routeur et par VRF. Bien qu'en général un RD unique par VPN puisse suffire, dans le cas où des réflecteurs de route sont présents dans le réseau, ou bien pour effectuer de l'ingénierie de trafic, la première solution est préférable.

Au niveau des PE, il faut porter une attention particulière à la configuration des interfaces liées au VRF. Rien ne sert de bien réaliser la configuration des VPN dans le réseau cœur si au niveau des PE l'interface de sortie vers le CE est mal configurée.

Hormis l'attribut de *route target* qui permet au routeur recevant une annonce MP-BGP de savoir dans quelle instance de VRF il doit ajouter les routes reçues, l'attribut SOO (*Site Of Origin*) permet de s'assurer de la provenance des annonces de routes, c'est-à-dire de quel site provient la route annoncée et d'éviter à un site de recevoir une route qu'il a lui-même émise. Ceci peut être valable si BGP est utilisé entre CE et PE avec de multiples connections d'un site au réseau MPLS, ou encore en cas d'attaque sur le protocole MP-BGP.

Enfin, les recommandations faites dans l'étude de BGP (*cf.* chapitre 4) sont aussi valables. Le protocole MP-BGP pourrait par exemple être protégé par l'utilisation de S-BGP ou d'une autre des extensions susmentionnées.

5.1.4 Établissement des LSP dans le réseau MPLS

Une autre étape nécessaire à la création de VPN est l'établissement des LSP dans le réseau MPLS. Ceux-ci permettent de créer des chemins virtuels entre les PE. Ils sont créés soit à la demande, lorsqu'un chemin doit être établi entre 2 PE, soit

automatiquement, pour permettre à chaque PE de posséder un chemin vers tous les autres PE.

5.1.4.1 Protocoles utilisés

Il y a plusieurs protocoles qui peuvent être utilisés afin de créer les LSP. Le principal est LDP. Si l'ingénierie de trafic est activée, CR-LDP, RSVP-TE peuvent aussi être choisis.

Quand un PE établit un LSP, il utilise son protocole de signalisation (par exemple LDP). Il indique l'adresse du PE à rejoindre en tant que destination, et attache l'identificateur VPN lié à ce LSP (en plus d'un *time stamp*, et idéalement d'une signature numérique via MD5 pour la sécurité).

5.1.4.2 Failles possibles

LDP est vulnérable à des attaques de type mystification, les messages échangés pouvant être interceptés et supprimés, et ne permet pas de garantir la confidentialité des étiquettes échangées. Concernant le premier point, elles pourraient permettre à un routeur espion de récupérer des paquets IP et ainsi de les modifier puis de les réacheminer ou de les supprimer. Il s'agit alors du même type de problème que pour le routage du cœur ou la création des VPN : une attaque *Man in the Middle*.

5.1.4.3 Conseils

Il est conseillé d'utiliser MD5 (voire SHA-1) pour authentifier les messages échangés par le protocole adopté (LDP, RSVP-TE, etc.). Les mises à jour de ce protocole ne doivent être acceptées que sur les interfaces qui possèdent un routeur du cœur à l'autre extrémité.

Pour éviter toute manipulation d'étiquettes, il faut d'une part empêcher tout accès au cœur, grâce à des listes d'accès (voir les conseils de la partie précédente), et d'autre part ne pas accepter de paquet IP portant des étiquettes MPLS provenant de l'extérieur du cœur. La seule exception à cette règle concerne les réseaux de topologie *Carrier's Carrier*, où des paquets portant des étiquettes MPLS peuvent être acceptés sous certaines conditions (*cf.* partie 2.2.5.2).

5.1.5 Autres considérations

Dans cette partie sont présentés quelques autres considérations intéressantes comme la nécessité d'une authentification de CE à CE, proposée dans un brouillon en 2003, ainsi que quelques remarques au sujet de la création de VPN dans MPLS/VPN.

5.1.5.1 Authentification CE à CE

Malgré les possibilités d'authentification d'un CE avec le PE auquel il est relié en utilisant MD5 ou l'authentification PPP (*cf.* section 5.1.2.3), rien ne garantit qu'un client est bien relié à son propre VPN au niveau du routeur PE (en cas de mauvaise configuration des interfaces par VRF par exemple). Autrement dit, rien ne garantit l'étanchéité au client en cas de faute, délibérée ou non, du fournisseur de service.

C'est cette impossibilité de détection d'éventuelles brèches dans la configuration des VPN qui motive la création d'un mécanisme permettant de s'assurer que tous les membres appartenant à un VPN sont bien autorisés à l'être. L'authentification CE à CE a été proposée dans un brouillon (Bonica et al., 2003), il suggère le recours à des jetons comme méthode d'authentification. Un jeton est émis par chaque site connecté à un VPN depuis le CE vers le PE qui lui est lié. Ce dernier ajoute le jeton aux annonces des routes apprises depuis ce site lors des mises à jour MP-BGP. Les autres sites appartenant au même VPN peuvent ainsi, à la réception de ce jeton, vérifier l'appartenance du site au VPN. Si celui-ci n'est pas conforme, un signal d'alarme est lancé et le site en question

est ignoré jusqu'à ce que le problème soit réglé. Ce mécanisme ne permet toutefois que d'avertir d'un problème de configuration, pas de l'empêcher.

Concernant le transport des jetons, au sein du réseau MPLS ceux-ci font partie des annonces MP-BGP grâce à un nouvel attribut des communautés étendues. Si BGP est mis à profit entre CE et PE, c'est ce même attribut qui est exploité. Si un autre protocole est adopté comme protocole CE-PE, un nouveau protocole de distribution de jetons doit être créé. Les auteurs proposent à cet égard un protocole basé sur UDP permettant de propager le jeton entre CE et PE dans les deux directions.

Il est évidemment possible d'utiliser un chiffrement IPsec de CE à CE, permettant en outre de s'affranchir des considérations de confidentialité des données échangées. Toutefois, la lourdeur apportée par cette solution ne la destine pas à tous les usages, en particulier ceux liés au temps réel. Par ailleurs, avec cette solution se pose la question du fonctionnement d'une autorité de certification et de distribution de clé de sécurité au sein du réseau MPLS, pas nécessairement évidente : comment les CE pourraient-ils recevoir de l'information provenant du cœur du réseau alors qu'ils ne sont pas censés pouvoir communiquer avec celui-ci?

5.1.5.2 Problème des *Route Targets*

Les *route targets* sont utilisées pour déterminer les routes à importer et à exporter. Si dans le cas de VPN simples (un seul client, deux PE concernés ou plus), cela ne pose pas de problème ; dans le cas de VPN partagés (deux clients accèdent à un VPN partagé, pour accéder à Internet par exemple), le mécanisme des RT est tel qu'il peut être possible de réaliser une attaque d'un VPN vers un autre VPN (*cf.* partie 3.1).

Ce bris de l'étanchéité n'est certes possible que sous certaines conditions mais montre qu'il n'y a que très peu d'écart entre le fonctionnement normal de MPLS et un

fonctionnement erroné. La recherche future pourrait offrir de nouvelles solutions permettant de ne pas rencontrer ce problème, éventuellement en imaginant une autre méthode permettant l'échange des routes dans le réseau MPLS/VPN.

5.1.5.3 Recette selon Cisco

Afin de configurer correctement un réseau MPLS/VPN au niveau des routeurs PE, Cisco propose une marche à suivre (Lewis, 2004) qui est présentée ci-dessous. Elle indique les étapes à effectuer, sans donner plus d'informations ou de recommandations. Dans cette étude, nous avons considéré la plupart de ces étapes pour en analyser les problèmes et solutions possibles.

Tableau 5.1

Configuration d'un réseau MPLS sécuritaire
(Tiré de Lewis, 2004)

Step 1 Configure the loopback interface to be used as the BGP update source and LDP router ID.
Step 2 Enable CEF.
Step 3 Configure the label distribution protocol. *cf. partie 5.1.4*
Step 4 Configure the TDP/LDP router-id (optional).
Step 5 Configure MPLS on core interfaces.
Step 6 Configure the MPLS VPN backbone IGP. *cf. partie 5.1.1*
Step 7 Configure global BGP parameters.
Step 8 Configure MP-BGP neighbor relationships. *cf. partie 5.1.3*
Step 9 Configure the VRF instances. *cf. partie 5.1.3*
Step 10 Configure VRF interfaces. *cf. partie 5.1.3*
Step 11 Configure PE-CE routing protocols / static routes. *cf. partie 5.1.2*
Step 12 Redistribute customer routes into MP-BGP. *cf. partie 5.1.3*

Le fait de suivre cette recette ne garantit pas la création d'un réseau sécuritaire. Il est nécessaire de porter une attention soutenue à chacune des étapes afin de ne pas réaliser d'erreur de configuration.

5.1.6 Bilan

Finalement, pour créer un réseau MPLS/VPN sécuritaire, il est nécessaire de suivre des recommandations, dont quelques-unes ont été énoncées dans cette étude, et de respecter quelques principes de sécurité évidents, aussi simples parfois que de ne pas laisser les mots de passe par défaut sur les routeurs.

Dans cette étude n'a été considéré que le cas d'un réseau MPLS/VPN mono-cœur. Une grande difficulté au niveau de la sécurité survient lorsque plusieurs réseaux MPLS sont reliés, qui plus est lorsque ceux-ci appartiennent à différents fournisseurs de service. Il existe trois méthodes d'interconnexion recommandées (*cf.* partie 2.2.5.1), mais quelle que soit la méthode le défi de rendre le tout fonctionnel, performant et sécuritaire n'est pas évident.

Il ne faut pas toujours croire délibérément un constructeur ou un fournisseur de service qui prétend que son produit est à 100% sûr. Les erreurs de configurations, mêmes involontaires, sont possibles, et semblent même suffisamment problématiques pour avoir suscité la réflexion de plusieurs chercheurs sur l'authentification CE à CE. Plus récemment, des chercheurs chinois (Yi et Yaping, 2006) ont d'ailleurs repris l'idée d'authentification des VPN basée sur les CE, permettant de détecter les mauvaises configurations ou les interconnexions délibérées entre VPN. Toutefois, lors de l'écriture de ce mémoire leur article n'était toujours pas disponible à la lecture.

L'attaque possible dans l'architecture Extranet/Internet (*cf.* parties 3.1 et 3.3) pose un problème supplémentaire en étant faiblement documentée. De plus, même en suivant les recommandations énoncées dans cette étude, elle ne peut pas être systématiquement empêchée. L'existence de VPN partagés, pour un accès Extranet ou Internet nécessite obligatoirement d'installer des pare-feux afin d'empêcher toute intrusion inter-VPN. Généralement, il est conseillé d'utiliser un VPN particulier uniquement pour l'accès Internet, pour séparer le trafic intra-VPN du trafic Internet. Éventuellement, une méthode différente permettant l'échange de routes VPN entre les différents sites en remplacement de l'import/export des *route targets* pourrait être développée à l'avenir afin de combler ce problème.

Finalement, concernant MP-BGP, ce qui est finalement le plus important est de s'assurer que la convergence du protocole MP-BGP est rapide, car même si les changements dans un réseau MPLS/VPN ne sont pas aussi fréquents que sur Internet, il faut à tout prix éviter de relier différents VPN ensemble à cause d'une étiquette qui n'aurait pas été mise à jour parce que le protocole convergerait trop lentement dans un grand réseau.

5.2 Recommandations générales

Cette partie présente des recommandations générales visant à garantir non pas une architecture MPLS/VPN absolument sans faille mais un fonctionnement sécuritaire de celle-ci.

5.2.1 Respect d'un modèle sécuritaire

Le respect d'un modèle de sécurité est incontournable pour concevoir un réseau sûr. Il existe différentes approches permettant de développer un modèle de sécurité pour un réseau (Canavan, 2001) :

- la sécurité par l'obscurité, qui part du principe qu'il n'est pas possible d'attaquer ce qui ne peut être vu, masquant donc le contenu du réseau de l'extérieur,

- la défense périmétrique, consistant à protéger les pourtours du réseau par des pare-feux, des listes d'accès sur les routeurs de bordure contre les intrusions de la même façon que des douves protégeaient les châteaux forts des envahisseurs,
- la défense en profondeur, qui repose sur différents niveaux ou couches de sécurité, permettant de continuer à garantir la sécurité du réseau même si un des systèmes de défense tombe.

La sécurité par l'obscurité vient naturellement dans un réseau MPLS/VPN. L'inconvénient de cette approche est que toute la sécurité ne repose que sur l'invisibilité du réseau. Le simple fait de deviner par essais successifs une adresse d'un élément du réseau peut la remettre en cause.

La défense périmétrique permet d'empêcher les intrusions provenant de l'extérieur. Elle est fortement recommandée mais non obligatoire dans l'architecture MPLS/VPN. Bien qu'empêchant toute intrusion si correctement implantée, elle n'est pas suffisante utilisée seule car elle ne protège pas contre les attaques internes, et dans le cas où une erreur de configuration permet par exemple une intrusion, une fois à l'intérieur du réseau l'intrus est libre de toute action puisque la sécurité n'est appliquée qu'en bordure.

La défense en profondeur est l'approche la plus sécuritaire, permettant de ne pas mettre tous ses œufs dans le même panier. L'utilisation combinée de différentes couches de sécurité permet de ne pas faire reposer la sécurité du réseau sur un seul système de défense, et donc se prémunir des failles, bugs ou mauvaises configurations. Cette approche peut se révéler plus difficile à mettre en application que les précédentes, mais le niveau de sécurité offert vaut cette complexité supplémentaire. En se limitant aux standards, l'architecture MPLS/VPN n'applique que peu le principe de défense en profondeur. Certes la séparation de l'adressage, du routage et du trafic permet d'isoler les VPN entre eux, mais une simple erreur de configuration peut remettre toute la sécurité en question, en connectant par exemple un site dans le mauvais VPN. Ceci

montre bien l'absence d'une complète défense en profondeur. Des techniques avancées pourraient être utilisées, telle que celle d'authentification de CE à CE par jetons présentée dans la partie 5.1.5.1. Le chiffrement des communications représente aussi une couche supplémentaire de sécurité pouvant être considérée, néanmoins celui-ci implique des diminutions de performances notables, non nécessairement compatibles avec les applications temps réel.

Enfin, le modèle de sécurité se doit d'être dynamique et non passif. L'utilisation d'un système de détection d'intrusion ou IDS permet de réagir à une attaque dès ses prémices et de la bloquer au lieu de simplement la détecter et avertir l'administrateur réseau de la situation, une fois que le mal est fait.

5.2.2 Respect d'un modèle de sécurité utilisant la défense en profondeur

L'approche de défense en profondeur présentée précédemment implique l'emploi de différentes couches de sécurité. À la sécurité par l'obscurité, obtenue par le masquage de l'adressage du réseau MPLS, il est essentiel d'ajouter une défense périmétrique empêchant quiconque de s'introduire dans le réseau. L'utilisation de pare-feux et de systèmes de détection d'intrusion est aussi fortement conseillée.

Il est primordial de protéger le réseau cœur en bloquant toute tentative d'accès. Un premier mécanisme empêchant l'accès au cœur ou aux autres VPN est l'utilisation d'espaces d'adressage distincts entre chaque VPN et avec le cœur, rendant inefficace l'utilisation d'une adresse IP de destination comme étant celle d'un routeur P du cœur ou appartenant à un autre VPN. Un second mécanisme consiste à empêcher de prendre le contrôle du seul point d'accès au réseau cœur, le routeur PE, afin de lancer une attaque vers le cœur depuis celui-ci. Pour y parvenir, des listes d'accès doivent être utilisées sur l'interface du PE liée au CE afin d'éviter les intrusions. Pour limiter les effets des attaques de déni de service, un filtrage étendu du trafic ainsi que la répartition des

ressources par VRF peut être réalisé par les PE. Le filtrage du trafic doit aussi permettre de refuser tout paquet avec une étiquette provenant de l'extérieur du réseau MPLS, sauf dans le cas des architectures avancées avec certaines restrictions (voir partie 2.2.5). Le document *Security in core networks* (Vyncke, 2003) donne de plus amples détails et conseils afin de protéger les routeurs PE et le réseau cœur.

Concernant le routage entre PE et CE, le routage statique est conseillé. Si un routage dynamique doit être utilisé, il doit au minimum être sécurisé par MD5. Le protocole eBGP est à privilégier si les liens PE-CE ne sont pas directs afin d'éviter les attaques *Man in the middle*, sinon OSPF est préférable. Des limites sur le nombre de préfixes par VRF et par site doivent être fixées, des listes d'accès doivent limiter l'accès aux routeurs aux paquets de routage, les interfaces de configuration (console, SSH, telnet) ne doivent être accessibles que par leurs ayant droits (le fournisseur de service pour le PE, le client pour le CE sauf cas particuliers). À ce propos, l'accès par telnet devrait être banni sauf si SSH n'est pas disponible, auquel cas des listes d'accès doivent aussi contrôler l'accès telnet. Il en va de même pour la diffusion de messages SNMP qu'il faut limiter par des ACL. Afin de détecter toute tentative d'attaque, l'utilisation de journaux d'évènements ou *logs* est essentielle.

Lorsque le lien CE-PE ne peut être direct et traverse des équipements de niveau 2, il peut être souhaitable de chiffrer les communications de CE à CE en utilisant IPsec. Cette méthode est plus lourde mais elle seule est capable de garantir la confidentialité des données entre CE et PE et vis-à-vis du fournisseur de service si les données transportées sont sensibles.

Si un système de gestion du réseau (NOC) est utilisé, il doit lui aussi se trouver à l'intérieur du réseau MPLS afin de ne pas créer une nouvelle cible attaquable à l'extérieur du réseau. Il est toutefois recommandé d'utiliser une couche supplémentaire de sécurité pour celui-ci en effectuant les opérations de gestion non pas dans un VPN

particulier mais hors-bande, en utilisant une connexion différente depuis l'extérieur du réseau MPLS. La section 1.2.4.3 présente les différentes techniques de gestion et les mesures qui doivent être considérées pour effectuer la gestion des éléments du réseau MPLS.

CONCLUSION

La conception d'une architecture sécuritaire n'est pas une sinécure. Pourtant, les réseaux privés fonctionnant sur MPLS, en utilisant des technologies reconnues comme MPLS et BGP, proposent une sécurité équivalente à ATM/FR en offrant une bonne résistance aux attaques à condition de respecter quelques règles et principes. Supportant de plus la qualité de service et les services différenciés, ils offrent de nombreux bénéfices à l'utilisateur final comme la simplicité et le faible coût d'une solution performante.

La spécification des VPN utilisant MPLS et BGP, décrite dans la RFC4364, permet de s'assurer de l'étanchéité des VPN dans le cas simple d'un réseau MPLS mono-cœur. Il n'est pas possible à un VPN de recevoir ou d'envoyer des informations dans un autre VPN, ni vers le cœur, ni vers l'équipement de gestion. Le nuage MPLS est transparent pour le client du VPN. De même, avec des méthodes de protection simples à mettre en place (listes d'accès, *policing/shaping*, partage des ressources), il est possible d'empêcher les attaques de type déni de service sur le réseau MPLS en provenance d'un VPN ou d'un intrus ayant réussi à se connecter sur le lien CE-PE. Le lien CE-PE doit être protégé tant au niveau du routage que concernant la confidentialité des données s'il n'est pas direct mais traverse des équipements de niveau 2.

Un des points les plus importants pour garantir l'étanchéité des VPN est l'assurance d'une bonne configuration. Une simple erreur de configuration sur un routeur PE peut remettre en cause toute la sécurité du réseau. Des outils de configuration automatique existent pour aider l'opérateur du réseau et éviter les mauvaises configurations. Cependant l'erreur humaine est toujours possible. La récente proposition de deux chercheurs d'une université chinoise (Yi et Yaping, 2006) suggérant une méthode pour authentifier les membres des VPN, vérifier automatiquement la configuration du réseau et détecter les erreurs éventuelles semble intéressante pour compenser ces bévues humaines.

Certaines architectures élaborées comme la connectivité Extranet ou Internet sont plus délicates et nécessitent une attention particulière. Nos tests ont montré qu'il était possible sous certaines conditions de réaliser une attaque via le routeur CE de la ressource partagée. L'utilisation de pare-feux est essentielle dans ce type d'architecture. Il en est de même lorsque plusieurs réseaux MPLS sont liés les uns aux autres, à cause de l'échange d'information entre différents fournisseurs de service. Ceux-ci doivent d'une part pouvoir se faire confiance, tout comme les clients doivent faire confiance à tous les fournisseurs de service, et d'autre part protéger les liaisons inter-réseaux MPLS, qui peuvent être vulnérables. L'architecture Inter-AS suggère plusieurs méthodes de liaison entre nuages MPLS dont la complexité de mise en œuvre et le niveau de sécurité varient.

Parmi les règles devant être respectées, il convient de s'assurer que les routeurs PE n'acceptent jamais de paquets labélisés sauf dans les architectures avancées multi-cœurs, selon des conditions très précises et limitées. Le routage doit lui aussi être protégé. Il s'agit en effet du seul type de trafic autorisé à voyager librement au sein du réseau MPLS et entre les routeurs CE et PE. L'authentification MD5, le champ TTL et éventuellement d'autres méthodes de sécurisation doivent être employés afin d'éviter les attaques.

Les menaces inhérentes au niveau 2 qui pourraient permettre à un intrus de pénétrer par exemple le lien CE-PE n'ont pas été détaillées dans ce mémoire. Si des équipements de niveau 2 sont utilisés sur les liens CE-PE ou entre les réseaux MPLS, les moyens de protection adéquats de niveau 2 doivent être utilisés.

Au-delà de la sécurité de la spécification, il est primordial que l'implémentation réalisée par chaque constructeur soit efficace et respecte bien la spécification. Or il est difficile de créer un système d'exploitation à toute épreuve. De la même manière que chaque

mois des mises à jour sont disponibles pour combler les failles des produits Microsoft ou Apple, il n'est pas impossible que des bugs ou failles soient découverts dans les versions de l'IOS utilisées sur les routeurs du réseau MPLS. En conséquence, le système d'exploitation des routeurs doit être tenu à jour, et les bugs corrigés dès leur découverte.

La distinction qui existe entre un réseau sécuritaire et un réseau compromis est parfois très faible, surtout dans le cas d'architectures évoluées comme la connectivité Extranet et Internet. Ceci montre la nécessité d'appliquer une sécurité en profondeur lors de la conception d'une technologie, ou lors de son implémentation. L'utilisation de pare-feux ou d'IPsec est par exemple facultative dans une architecture simple mais devient primordiale dans une connectivité Extranet ou en présence d'équipements de niveau 2 entre PE et CE.

Certains avantages des VPN sur MPLS peuvent être source de désagréments. L'absence de chiffrement implique que les clients doivent faire entièrement confiance au fournisseur de service. Cela ne constituera en général pas un obstacle pour les clients dont les données transportées ne sont pas sensibles. Mais qu'en est-il réellement du respect du secret professionnel et de la vie privée, alors que de plus en plus les fournisseurs de service doivent légalement garder des traces de tous les paquets transitant sur leur réseau? Font-ils réellement une distinction entre paquets échangés avec Internet et paquets appartenant aux VPN de leurs clients? Cette notion de confiance qui est devenue plus problématique avec le Web 2.0 et des sites comme Google qui parcourent automatiquement les courriels reçus et envoyés via leur interface Gmail, ou comme Facebook, Myspace, etc. dans lesquels les gens exposent leur vie, leurs photos et leurs informations personnelles? Arrivera-t-il un jour où Google possédera des dossiers sur chaque internaute contenant son profil, ses habitudes de navigation, etc.?

C'est pourquoi le chiffrement des données a toujours son utilité, dans le cadre des réseaux privés virtuels ou pour un usage personnel. Un réseau privé n'est plus privé à

partir du moment où une seule personne extérieure a accès aux données et non lorsque tout le monde y a accès, car cet individu pourrait très bien dupliquer l'information pour la rendre disponible. En permettant au fournisseur de service de voir les données qui transitent dans les VPN, MPLS remet finalement en question la notion de VPN. Néanmoins, du point de vue du fournisseur de service, la question ne se pose pas : la technologie est efficace et sécuritaire, celui-ci doit simplement faire attention à la configuration de son réseau et au respect des règles énoncées précédemment.

Lors de la recherche exhaustive de méthodes d'attaques sur le réseau, une idée quelque peu farfelue a été considérée. Toute l'impossibilité de réaliser une attaque sur l'équipement du réseau cœur est due à la séparation du trafic par VPN en fonction de l'adresse de destination. Cette séparation est permise par l'ajout d'une étiquette VPN au paquet original. Mais qu'en serait-il s'il était possible de changer en cours de route cette étiquette ou toute une partie de l'entête? Peut-on imaginer qu'il soit possible qu'une portion de l'entête se désagrège lors du transport du paquet? Un virus dans un routeur du réseau pourrait y parvenir, mais serait-ce toujours possible sans aide extérieure?

Finalement, il n'est pas simple de dire si telle situation est sécuritaire ou pas. Comme nous avons pu le voir, bien que la plupart le soient en théorie, des attaques peuvent être réalisables sous certaines conditions. Ce sont ces conditions particulières qu'il faut éviter pour rester dans un environnement sécuritaire.

RECOMMANDATIONS

Ce mémoire présentait une étude de la sécurité des VPN sur MPLS au niveau 3 et ne considérait pas les VPN utilisant MPLS au niveau 2 (VPLS ou VPWS, *Virtual Private Wire Service*). Permettant des avantages attrayants comme l'émulation d'un réseau local unique malgré la séparation physique des sites, ceux-ci pourraient faire l'objet d'une recherche approfondie.

Lorsque le détail de leur recherche sera disponible, il pourrait aussi être intéressant d'analyser la méthode retenue (Yi et Yaping, 2006) pour authentifier les membres des VPN et vérifier la configuration du réseau. Éventuellement, une nouvelle technique combinant les avantages de leur méthode et de la technique des jetons permettant l'authentification PE à PE pourrait être développée.

Par ailleurs, il serait important de vérifier les effets de l'ingénierie de trafic utilisée conjointement avec les VPN. Bien que le concept des VPN dans ce cas ne change pas, les paramètres supplémentaires apportés par la gestion du balancement de charge et des protocoles RSVP-TE par exemple pourraient rendre plus complexe la bonne configuration du réseau. Une étude statistique du nombre de configurations erronées pour des VPN utilisés seuls et lors de l'association des VPN avec l'ingénierie de trafic constituerait un bon point de départ à cette étude. À cet égard, l'outil QMA développé récemment (Truong, 2006) pourrait avec quelques modifications réaliser cette étude et surtout vérifier la configuration correcte du réseau.

Le problème des *route targets* à l'origine du bris de l'étanchéité dans l'architecture Extranet et Internet montre que bien que fonctionnel, le principe d'échange de routes pourrait être amélioré ou remplacé. La recherche future pourrait offrir de nouvelles solutions permettant de ne pas rencontrer ce problème, éventuellement en imaginant une autre méthode permettant l'échange des routes dans le réseau MPLS/VPN.

Enfin, la technologie MPLS devrait être optimisée afin de ne plus imposer la condition de confiance qui doit être faite aux fournisseurs de service pour assurer la confidentialité du contenu des réseaux privés virtuels. D'autres idées devraient éventuellement être développées pour permettre de garantir à la fois l'intégrité des VPN et la confidentialité des données transportées y compris vis-à-vis du fournisseur de service.

LISTE DE RÉFÉRENCES

Aiello, W., J. Ioannidis et P. McDaniel. 2003. « Origin authentication in interdomain routing ». In *Proceedings of the 10th ACM conference on Computer and communications security*. Washington D.C., USA: ACM Press.

Anderson, L., P. Doolan, N. Feldman, A. Fredette et B. Thomas. 2001. « LDP Specification ». RFC 3036. <http://www.ietf.org/rfc/rfc3036.txt>. Consulté le 22 mai 2007.

Awduche, D., L. Berger, D. Gan, T. Li, V. Srinivasan et G. Swallow. 2001. « RSVP-TE: Extensions to RSVP for LSP Tunnels ». RFC 3209. <http://www.ietf.org/rfc/rfc3209.txt>. Consulté le 22 mai 2007.

Baker, F., et R. Atkinson. 1997. « RIP-2 MD5 Authentication ». RFC 2082. <http://www.ietf.org/rfc/rfc2082.txt>. Consulté le 23 mai 2007.

Bates, T., R. Chandra, D. Katz et Y. Rekhter. 2007. « Multiprotocol Extensions for BGP-4 ». RFC 4760. <http://www.ietf.org/rfc/rfc4760.txt>. Consulté le 22 mai 2007.

Bates, T., E. Chen et R. Chandra. 2006. « BGP Route Reflection : An Alternative to Full Mesh Internal BGP (IBGP) ». RFC 4456. <http://www.ietf.org/rfc/rfc4456.txt>. Consulté le 29 juin 2007.

Behringer, Michael H. 2006. « Analysis of the Security of BGP/MPLS IP Virtual Private Networks (VPNs) ». RFC 4381. <http://www.ietf.org/rfc/rfc4381.txt>. Consulté le 25 mai 2007.

Behringer, Michael H., et Monique Morrow. 2005. *MPLS VPN security*. Indianapolis, Ind.: Cisco, xxi, 286 p.

Berkowitz, H. 2003. « L3VPN Tutorial ». In *Braindumps*. En ligne. <http://www.braindumps.com/index.cfm?do=hardware&hardid=1371>. Consulté le 12 juillet 2007.

Bonica, R., Y. Rekhter, R. Raszuk, E. Rosen et D. Tappan. 2003. « CE-to-CE Member Verification for Layer 3 VPNs ». Internet Draft. <http://tools.ietf.org/html/draft-ietf-ppvpn-l3vpn-auth-03>. Consulté le 10 juillet 2007.

Bush, R., et T. G. Griffin. 2003. « Integrity for virtual private routed networks ». In. Vol. 2, p. 1467-1476 vol.2.

Canavan, J. E. 2001. *Fundamentals of Network Security*, 1st. Edition. Artech House Publishers, 319 p.

Chau, Hang. 2004. « Network Security – Defense Against DoS/DDoS Attacks ». En ligne. <http://www.infosecwriters.com/text_resources/pdf/Defense_DDoS.pdf>. Consulté le 2 novembre 2007.

Cisco. 2003. « Advanced Concepts – Inter AS MPLS/VPN ». En ligne. <www.cisco.com/warp/public/732/Tech/mpls/docs/interasadvanced.ppt>. Consulté le 22 juin 2007.

Cisco. 2004. « Analysis of MPLS-based IP VPN security : Comparison to traditional L2VPNs such as ATM and Frame Relay, and deployment guidelines ». Livre blanc. <http://www.cisco.com/warp/public/cc/so/neso/vpn/prodlit/mpvpn_wp.pdf>. Consulté le 22 juin 2007.

Cisco. 2006. « Cisco IP Solution Center MPLS VPN User Guide, 4.2 - IP Solution Center MPLS VPN ». In *Cisco Systems, Inc.* En ligne. <http://www.cisco.com/en/US/products/sw/netmgtsw/ps4748/products_user_guide_chapter09186a008069aaad.html#wp1039413 >. Consulté le 12 juillet 2007.

De Clercq, J., D. Ooms, M. Carugi et François Le Faucheur. 2006. « BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN ». RFC 4659. <http://www.ietf.org/rfc/rfc4659.txt>. Consulté le 29 juin 2007.

Dierks, T., et C. Allen. 1999. « The TLS Protocol Version 1.0 ». RFC 2246. <http://www.ietf.org/rfc/rfc2246.txt>. Consulté le 22 mai 2007.

Dobbertin, Hans. 1996. « Cryptanalysis of MD5 Compress ». En ligne. Vol. 96. <http://www.cs.ucsd.edu/users/bsy/dobbertin.ps>.

Dubee, N. 2003. « BGP et DNS: attaques sur les protocoles critiques de l'Internet ». En ligne. <http://actes.sstic.org/SSTIC03/BGP_et_DNS/SSTIC03-article-Dubee-BGP_et_DNS.pdf>. Consulté le 11 juillet 2007.

Dubois, N., M. Capelle, S. Chou et B. Fondeviole. 2004. « The benefits of monitoring routing protocols in live networks ». In., p. 9-15.

Easttom, C. 2006. *Network Defense and Countermeasures: Principles and Practices*. Pearson Prentice Hall, 448 p.

Everett, Bernard. 2007. « Tapping into fibre optic cables ». *Network Security*, vol. 2007, no 5, p. 13-16.

Gill, V., J. Heasley et D. Meyer. 2004. « The Generalized TTL Security Mechanism (GTSM) ». RFC 3682. <http://www.ietf.org/rfc/rfc3682.txt>. Consulté le 26 juin 2007.

Goodell, G., W. Aiello, T. Griffin, J. Ioannidis, P. McDaniel et A. Rubin. 2003. « Working around BGP: an incremental approach to improving security and accuracy of interdomain routing ». In., p. 11 pp. Coll. « 10th Annual Network and Distributed System Security Symposium ». San Diego, CA, USA: Internet Soc. <http://www.isoc.org/isoc/conferences/ndss/03/proceedings/papers/5.pdf>. Consulté le 29 juin 2007.

Hares, S., et C. Wittbrodt. 1994. « Essential Tools for the OSI Internet ». RFC 1574. <http://www.faqs.org/rfcs/rfc1574.html>. Consulté le 13 juillet 2007.

Heffernan, A. 1998. « Protection of BGP Sessions via the TCP MD5 Signature Option ». RFC 2385. <http://www.ietf.org/rfc/rfc2385.txt>. Consulté le 22 mai 2007.

Hu, Yih-Chun, Adrian Perrig et Marvin Sirbu. 2004. « SPV: Secure path vector routing for securing BGP ». In, 4. Vol. 34, p. 179-192. Coll. « Computer Communication Review ». Portland, OR, United States: Association for Computing Machinery, New York, NY 10036-5701, United States. <http://dx.doi.org/10.1145/1030194.1015488 >.

Ixia. 2004. « Multi-Protocol Label Switching (MPLS) Conformance and Performance Testing ». In *Ixia : Leader in IP performance testing*. En ligne. <http://www.ixiacom.com/library/white_papers/display?skey=mpls>. Consulté le 12 juillet 2007.

Karlin, J., S. Forrest et J. Rexford. 2006. « Pretty Good BGP: Improving BGP by Cautiously Adopting Routes ». In., p. 290-299. <http://www.ieee-icnp.org/2006/papers/s8a3.pdf>.

Ke, Zhang, Zhao Xiaoliang et S. F. Wu. 2004. « An analysis on selective dropping attack in BGP ». In., p. 593-599.

Kent, S., et R. Atkinson. 1998. « Security Architecture for the Internet Protocol ». RFC 2401. <http://www.ietf.org/rfc/rfc2401.txt>. Consulté le 22 mai 2007.

Kent, Stephen, Charles Lynn et Karen Seo. 2000. « Secure Border Gateway Protocol (S-BGP) ». *IEEE Journal on Selected Areas in Communications*, vol. 18, no 4, p. 582-592.

Kranakis, E., P.C. van Oorschot et T. Wan. 2005. « Pretty Secure BGP ». In *12th Annual Net. and Distrib. Sys. Sec. Symp.* (Feb. 2005). San Diego, CA.

Kruegel, C., D. Mutz, W. Robertson, F. Valeur, G. Vigna et E. Jonsson. 2003. « Topology-based detection of anomalous BGP messages ». In *International symposium on recent advances in intrusion detection No6*. p. 1-20. Pittsburgh PA: Springer, Berlin, Germany.

Le Faucheur, François, L. Wu, B. Davie, S. Davari, P. Vaananen, R. Krishnan, P. Cheval et J. Heinanen. 2002. « Multi-Protocol Label Switching (MPLS) Support of Differentiated Services ». RFC 3270. <http://www.ietf.org/rfc/rfc3270.txt>. Consulté le 17 avril 2007.

Lewis, M. 2004. *Troubleshooting Virtual Private Networks*. Cisco Press, 840 p.

Lloyd, B., et W. Simpson. 1992. « PPP Authentication Protocols ». RFC 1334. <http://www.ietf.org/rfc/rfc1334.txt>. Consulté le 6 juillet 2007.

McGehee, B. 2003. « Security in IPv6 ». En ligne. <www.usipv6.com/ppt/IPsec-BrianMcGehee.pdf >. Consulté le 31 mai 2007.

Miercom. 2001. « Cisco MPLS Based VPN: Equivalent to the Security of Frame Relay and ATM ». Livre blanc. <http://www.paetec.com/downloads/mpls_compare_frame_atm.pdf>. Consulté le 22 juin 2007.

Mitnick, K. D., et W. L. Simon. 2002. *The Art of Deception: Controlling the Human Element of Security*. John Wiley & Sons, Inc. New York, NY, USA, 366 p.

Moy, J. 1998. « OSPF Version 2 ». RFC 2328. <http://www.ietf.org/rfc/rfc2328.txt>. Consulté le 5 juillet 2007.

Murphy, S., M. Badger et B. Wellington. 1997. « OSPF with Digital Signatures ». RFC 2154. <http://www.ietf.org/rfc/rfc2154.txt>. Consulté le 25 mai 2007.

Murphy, Sandy. 2006. « BGP Security Vulnerabilities Analysis ». RFC 4272. <http://www.ietf.org/rfc/rfc4272.txt>. Consulté le 22 mai 2007.

Palmieri, F. 2003. « VPN scalability over high performance backbones Evaluating MPLS VPN against traditional approaches ». In *Proceedings of the Eighth IEEE International Symposium on Computers and Communications*. p. 975- 981. vol. 2. IEEE Computer Society.

Panko, R. R. 2004. *Sécurité des systèmes d'information et des réseaux*. Pearson Education, 469 p.

Rekhter, Y., T. Li et S. Hares. 2006. « A Border Gateway Protocol 4 ». RFC 4271. <http://www.ietf.org/rfc/rfc4271.txt>. Consulté le 22 mai 2007.

Rekhter, Y., et E. Rosen. 2001. « Carrying label information in BGP-4 ». RFC 3107. <http://www.ietf.org/rfc/rfc3107.txt>. Consulté le 22 mai 2007.

Ren, R., D. G. Feng et K. Ma. 2004. « A detailed implement and analysis of MPLS VPN based on IPSec ». In *Proceedings of 2004 International Conference on Machine Learning and Cybernetics*. Vol. 5, p. 2779- 2783.

Rey, Enno. 2006. « MPLS and VPLS security ». En ligne. <http://www.blackhat.com/presentations/bh-europe-06/bh-eu-06-Rey-up.pdf>. Consulté le 18 juin 2007.

Rivest, R. 1992. « The MD5 Message-Digest Algorithm ». RFC 1321. <http://www.ietf.org/rfc/rfc1321.txt>. Consulté le 1 juin 2007.

Rosen, E. 2001. « Multiprotocol Label Switching ». RFC 3031. <http://www.ietf.org/rfc/rfc3031.txt>. Consulté le 17 avril 2007.

Rosen, E., P. Psenak et P. Pillay-Esnault. 2006. « OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs) ». RFC 4577. <http://www.ietf.org/rfc/rfc4577.txt>. Consulté le 18 juin 2007.

Rosen, E., et Y. Rekhter. 1999. « BGP/MPLS VPNs ». RFC 2547. <http://www.ietf.org/rfc/rfc2547.txt>. Consulté le 21 juin 2007.

Rosen, E., et Y. Rekhter. 2006. « BGP/MPLS IP Virtual Private Networks (VPNs) ». RFC 4364. <http://www.ietf.org/rfc/rfc4364.txt>. Consulté le 17 avril 2007.

Rosen, E., D. Tappan, G. Fedorkow, Y. Rekhter, D. Farinacci, T. Li et A. Conta. 2001. « MPLS Label Stack Encoding ». RFC 3032. <http://www.ietf.org/rfc/rfc3032.txt>. Consulté le 22 mai 2007.

Seo, K., C. Lynn et S. Kent. 2001. « Public-key infrastructure for the Secure Border Gateway Protocol (S-BGP) ». In *DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings*. Vol. 1, p. 239-253.

Smith, B. R., et J. J. Garcia-Luna-Aceves. 1996. « Securing the border gateway routing protocol ». In., p. 81-5. Coll. « IEEE GLOBECOM 1996. Communications: The Key to Global Prosperity. GLOBAL INTERNET'96. Conference Record (Cat.

No.96CH35942) ». London, UK: IEEE. <http://dx.doi.org/10.1109/GLOCOM.1996.586129 >.

Smith, P. 2007, 28 juin. *BGP Routing Table Analysis*. En ligne. <thyme.apnic.net>. Consulté le 28 juin 2007.

Subramanian, L., V. Roth, I. Stoica, S. Shenker et R. H. Katz. 2004. « Listen and Whisper: security mechanisms for BGP ». In *First Symposium on Networked Systems Design and Implementation (NSDI '04)*. p. 127-140. San Francisco, CA, USA: USENIX Assoc.

Truong, O. 2006. *Étude et développement d'outils d'optimisation de gestion de services dans les réseaux MPLS*. MG, 17. Québec: École de technologie supérieure. Consulté le 21 juillet 2007.

Venema, W. 1996. « Murphy's Law and Computer Security ». En ligne. <http://insecure.org/stf/wietse_murphy.html>. Consulté le 1 juin 2007.

Villamizar, C., C. Alaettinoglu, D. Meyer et S. Murphy. 1999. « Routing Policy System Security ». RFC 2725. <http://www.ietf.org/rfc/rfc2725.txt>. Consulté le 22 mai 2007.

Vyncke, E. 2003. « Security in core networks ». En ligne. <http://www.cisco.com/global/HU/rendezvenyek/presentations/SecurityinCoreNetworks.pdf>. Consulté le 4 novembre 2007.

Wang, Xiaoyun, Yiqun Lisa Yin et Hongbo Yu. 2005. « Finding Collisions in the Full SHA-1 ». In *Advances in Cryptology – CRYPTO 2005*. p. 17-36. <http://www.infosec.sdu.edu.cn/paper/sha1-crypto-auth-new-2-yao.pdf>.

Wang, Xiaoyun, et Hongbo Yu. 2005. « How to Break MD5 and Other Hash Functions ». In *Advances in Cryptology – EUROCRYPT 2005*. p. 19-35. <http://www.infosec.sdu.edu.cn/paper/md5-attack.pdf>.

Wayne, C. Summers, et Bosworth Edward. 2004. « Password policy: the good, the bad, and the ugly ». In *Proceedings of the winter international synposium on Information and communication technologies*. Cancun, Mexico: Trinity College Dublin.

White, R. 2003. « Securing BGP through secure origin BGP (soBGP) ». *Business Communications Review*, vol. 33, no 5, p. 47-8.

Yi, Ji, et Deng Yaping. 2006. « A scheme to enhance the security of BGP/MPLS VPN ». In *IET International Conference on Wireless Mobile and Multimedia Networks*

Proceedings. ICWMMN 2006, Nov 6-9 2006. Vol. 525, p. 404. Institution of Engineering and Technology, Stevenage, SG1 2AY, United Kingdom. <http://dx.doi.org/10.1049/cp:20061569 >.

Zhao, M., S. W. Smith et D. M. Nicol. 2005. « The performance impact of BGP security ». *Network, IEEE*, vol. 19, no 6, p. 42-48.