Système et méthode de gestion de flux sécurisés entre plusieurs sites distants

La présente invention concerne un système et une méthode de gestion de flux sécurisés entre plusieurs sites distants, réseaux locaux ou métropolitains.

L'invention concerne le domaine des architectures de télécommunications des réseaux et notamment les réseaux présentant de fortes contraintes en termes de sécurité. De telles architectures peuvent comporter à la fois des réseaux privés sensibles interconnectés avec des réseaux publics non sensibles. Les réseaux sensibles présentent de fortes capacités de résilience pour l'acheminement des flux sensibles au profit des usagers. Les réseaux publics non sensibles assurent l'acheminement des flux non sensibles au profit d'autres usagers. Par flux sensibles, on entend aussi bien les flux à caractère de confidentialité que de contraintes d'acheminement ou à caractère opérationnel. La protection en confidentialité des flux est assurée par les applicatifs ou par d'autres moyens mis en œuvre dans les réseaux de dessertes (campus) et qui n'influent pas directement sur l'architecture du système.

Le transport dans les dessertes (c'est-à-dire des LAN, « Local Area Network » pour réseaux locaux et/ou des MAN, « Metropolitan Area Network » pour réseaux métropolitains) des flux sensibles et non sensibles se caractérise par le fait que l'ensemble des flux est véhiculé sur un réseau MAN unique non sensible (les flux non sensibles sont par nature plus volumineux et touchent un plus grand nombre d'usagers). Pour assurer la protection d'acheminement sur des réseaux étendus WAN (« Wide Area Network ») de l'ensemble des flux (sensibles et non sensibles), ces derniers sont transportés chiffrés sur lesdits réseaux WAN par l'intermédiaire de tunnels IPsec (« Internet Protocol Security »).

Les moyens à fortes capacités de résilience sont des moyens d'infrastructure terrestres à grande capacité de ressources ou des moyens d'infrastructure satellitaires à plus faible capacité de ressources et ayant des contraintes de qualité de service (désignée aussi par l'acronyme QoS pour « Quality of Service) par exemple en termes de temps de latence, de temps de transit, de perte de paquets.

La communication entre les usagers situés dans les dessertes est contrainte par l'emploi de chiffreurs IPsec et elle obéit à des règles de communications établies généralement de manières statiques, ces règles définissent les ayant droits à communiquer (généralement des sous réseaux) et les sites distants (les équipements de sécurité IPsec) que ces ayant droits peuvent atteindre. Ces informations sont contenues dans une base de donnée appelée SPD (« Security Policy Database »). La base SPD n'est pas modifiable dynamiquement et nécessite des opérations manuelles de configuration de la part d'un opérateur. L'ensemble des règles inscrites dans la base SPD est appelée la « politique de sécurité des flux ».

Les flux circulant entre deux réseaux locaux distants sont de natures différentes, ils sont identifiés par une classe de trafic, par exemple à l'aide du mécanisme de classification DiffServ, le champ DiffServ étant un champ de l'en-tête d'un paquet IP. Les équipements en bordure de réseaux n'effectuent pas de traitement sur les flux en fonction de la classe de trafic, mais par rapport à une classe de service, une classe de service étant un regroupement d'un ensemble de classes de trafic. Ce principe permet de procéder à un traitement égalitaire sur les flux ayant des contraintes techniques identiques comme le temps de transit par exemple.

Avec les systèmes actuels, le chiffrement s'effectue avant le routage. Il est nécessaire de disposer de deux plans de routage, un plan de routage dans la partie rouge du réseau (avant les chiffreurs) et un plan de routage dans la partie noire du réseau (après les chiffreurs). Par contre il n'est pas possible de faire une corrélation entre ces deux plans de routage, car le plan de routage noir est masqué et inaccessible du fait de l'emploi de réseaux virtuels privés VPN IPsec (« Virtual Private Network Internet Protocol Security »).

Une technique connue est d'utiliser deux réseaux étendus WAN en fonction « backup » c'est à dire que le second réseau WAN ne sera utilisé que si le premier est en défaut de connectivité. Dans les autres cas et notamment en cas de saturation du réseau WAN, les flux continuent à emprunter le réseau WAN saturé.

Enfin, pour permettre un usage simultané des deux réseaux WAN, il est nécessaire de rétablir une topologie de routage à partir du plan de routage rouge, cette solution utilise un tunneling des flux par l'emploi de

tunnels GRE qui permettent de rétablir une connectivité entre les équipements routeurs rouges et d'élaborer le plan de routage rouge par l'utilisation d'un protocole à état de lien tel que le protocole IGP (OSPF par exemple).

L'art antérieur nécessite la mise en œuvre de plusieurs produits distincts (Switch, Firewall, Routeur et Chiffreur). Les opérations de gestion et de sécurité sont distinctes et nécessitent une corrélation entre les opérateurs pour définir l'établissement des politiques de sécurité et celles du routage (tunnels GRE). L'exploitation est rendue complexe sur les réseaux importants puisqu'il est nécessaire d'établir des tunnels GRE entre tous les sites.

La mise en œuvre d'une politique de gestion des flux est très limitée par le simple fait qu'il y a une visibilité limitée sur le contenu des paquets (champ DSCP) et non sur l'origine et la destination des flux. Ce qui implique de prendre les décisions de routage en amont (plan rouge).

L'offset engendré par les tunnels IPsec ne permet pas d'assurer un SLA cohérent entre les réseaux MAN (usagers) et WAN (transit), c'est pourquoi, il est nécessaire d'avoir un routeur (appelé dans certains cas routeur QoS) entre les WAN et les chiffreurs dont l'objectif principal est d'assurer une cohérence entre les flux en provenance du WAN et à destination des MAN et inversement.

Plusieurs problèmes demeurent non résolus par les systèmes de l'art antérieur. Notamment, l'élongation variable de la taille des paquets (overhead) apportée par le chiffreur ne permet pas d'avoir une cohérence sur la QoS. La politique de gestion des flux n'est pas effectuée selon le type de flux opérationnel. Il n'y a pas de politique de répartition des flux entre les WAN. Il n'y a pas de réservation et préemption des ressources sur les WAN qui mettent en œuvre des protocoles comme RSVP.

Les équipements de bordure de réseaux intègrent des fonctionnalités de gestion des classes de services par l'utilisation de plusieurs files d'attente et ils associent à ces files d'attente un processus particulier qui garantit aux usagers de ces services un traitement approprié de leurs flux lors des congestions dans les réseaux. Ces principes de QoS et les règles associées sont appelées « la politique de traitement des flux ».

La figure 1 présente une architecture de réseaux interconnectés entre eux. Un objectif d'une telle architecture est d'assurer l'établissement sécurisé d'une ou plusieurs liaisons de communication entre un premier réseau local S1, encore appelé enclave réseau, et un second réseau local S2. Ces deux enclaves réseau distantes sont interconnectées au moyen d'un ou plusieurs réseaux étendus public WAN_C ou privé WAN_M, filaires ou satellitaires. Les flux transmis entre les deux réseaux locaux S1, S2 sont chiffrés, respectivement déchiffrés, par un dispositif Z_S1, Z_S2 de chiffrement disposé entre chaque réseau local et le ou les réseaux étendus. Un ou plusieurs routeurs rouges R1_S1, R2_S2 assurent l'aiguillage des flux à destination et en provenance des enclaves réseaux S1, S2. Un ou plusieurs routeurs noirs R2_S1, R2_S2 assurent l'aiguillage des flux chiffrés à travers le ou les réseaux étendus vers l'enclave réseau distante.

Un premier problème lié à ce type d'architecture concerne le cloisonnement entre les réseaux étendus WAN d'une part et les réseaux locaux d'autre part du fait du chiffrement des flux de données. Seuls les flux de données d'une enclave réseau peuvent atteindre une autre enclave réseau en conformité avec le contenu de la base de données SPD. En d'autres termes aucun flux de données ne peut circuler entre une enclave réseau S1,S2 et un réseau étendu WAN. Les communications autorisées sont nécessairement entre deux équipements de chiffrement. Cette absence de communication directe possible entre un réseau local et un réseau étendu pose un problème lorsque l'on souhaite déterminer le type de réseau étendu à utiliser pour établir une liaison de communication en fonction des caractéristiques intrinsèques d'un flux de données provenant d'une enclave réseau. En effet, les flux transmis peuvent être classés en fonction d'une qualité de service qui leur est attribuée par exemple par rapport à leur degré de priorité (flux vitaux ou non) , à leurs besoins en bande passante et débit ou encore aux contraintes de délai, de gigue et/ou de pertes paquets qu'ils peuvent supporter. Pour pouvoir déterminer le canal de communication, parmi les réseaux étendus WAN disponibles, le plus adapté aux flux de données à transmettre, il est donc nécessaire d'établir une communication entre l'enclave réseau et les réseaux étendus afin de communiquer les besoins identifiés. Ce type de communication n'est pas possible avec les

architectures connues du fait de la présence des équipements de chiffrement.

Un deuxième problème lié aux architectures sécurisées connues concerne le routage des flux de données à travers les différents réseaux étendus. Les protocoles de routage actuels, par exemple le protocole OSPF, permettent de router les flux en fonction du coût des liens. Cependant pour pouvoir utiliser un protocole de routage à état de lien entre les réseaux locaux S1,S2 distants il est nécessaire d'établir des liaisons directes entre ces réseaux permettant de s'abstraire de la présence des équipements de chiffrement. Une telle liaison directe est, par exemple, mise en œuvre à l'aide du protocole GRE (Generic Routing Encapsulation). Les protocoles de routage implémentés dans les réseaux étendus WAN n'ont aucune interaction avec le protocole de routage à état de liens mis en œuvre par les routeurs R1_S1, R1_S2, en effet, ils sont masqués par les tunnels IPsec. Aussi, les incidents qui interviennent dans les différents réseaux WAN ne seront pris en compte au niveau des routeurs R1_S1, R1_S2 que sur détection par le protocole à état de lien d'un dysfonctionnement. Le dysfonctionnement observé par le routeur pour changer le routage est une rupture du lien, c'est à dire une rupture du tunnel GRE. Dans ce cas, le protocole à état de lien peut router les flux vers un autre réseau WAN. Le partage de charge entre les différents réseaux WAN peut se faire à condition que les coûts des liens soient identiques.

Ce type de fonctionnement ne permet pas de router intelligemment les flux en tenant compte de critères sur l'un et l'autre des réseaux étendus WAN. Il ne permet pas non plus d'optimiser la capacité en transit des réseaux WAN. Cela revient à n'utiliser que les réseaux WAN en deçà de leur capacité de transit ou à provisionner de la ressource en excédant sur l'un ou l'autre des réseaux WAN.

Un troisième problème des architectures sécurisées connues concerne l'aiguillage des flux vers les différents réseaux WAN disponibles en fonction de la sensibilité de leur contenu. En effet les flux sensibles doivent être dirigés vers un réseau étendu privé sécurisé alors que les flux non sensibles peuvent être dirigés vers un réseau étendu public. Pour réaliser cet

aiguillage, il est nécessaire d'analyser les applicatifs qui sont au dessus de la couche IP ou de recourir à une identification précise de la source et de la destination des flux. Les sites hébergent des usagers ayant des fonctions administratives ou opérationnelles, ces usagers sont considérés soit comme des usagers vitaux (en nombre restreint) ou non vitaux et ils génèrent des flux sensibles et non sensibles. Il n'existe pas de corrélation entre usagers vitaux et flux sensibles, un usager non vital peut générer des flux sensibles.

Les flux en provenance des réseaux locaux LAN et/ou MAN sont chiffrés pour des raisons de niveau de sécurité de ces flux. Dans ce cas, l'analyse des paquets ne peut être réalisée que sur le champ DSCP (« Differentiated Services Code Point ») du paquet IP, qui bénéficie d'une recopie intégrale sans altération de la part des équipements de chiffrement. Aussi, l'aiguillage des flux vers l'un ou l'autre des réseaux WAN ne peut être réalisé qu'à partir de ce champ DSCP ce qui est limitant pour réaliser une analyse précise de la sensibilité des flux.

Les trois problèmes précités sont liés directement ou indirectement aux contraintes techniques introduites par la présence d'équipements chiffreurs qui limitent les échanges possibles entre la partie noire (réseaux locaux) et la partie rouge (réseaux étendus) du réseau.

La figure 2 illustre une topologie, similaire à celle de la figure 1, d'architecture de réseau sécurisé selon l'état de l'art.

Une telle architecture comprend des usagers de la desserte d'un premier réseau local S1, qui sont respectivement les abonnés A1_S1 et abonnés A2_S2. Ces usagers disposent d'adresses IP différentes, identifiables par leur préfixe. Les usagers du site S2 disposent également d'adresses différentes entre abonnés B1_S2 et B2_S2 et vis à vis du réseau local S1. Les flux entre les usagers des réseaux locaux enclavés S1 et S2 sont aiguillés vers les routeurs de sortie R1_S1, R1_S2, ou routeurs rouges, de chaque réseau local. Les routeurs R1_S1 et R1_S2 sont optionnels. Ils permettent, par exemple, de gérer les abonnés des enclaves réseau sous forme de plusieurs communautés ayant des attributs différents. Ils permettent aussi de gérer la bande passante théorique disponible en affectant des priorités aux abonnés.

Le système de la figure 2 comprend également des chiffreurs Z_S1, Z_S2. Le chiffreur Z_S1 assure une protection des flux en provenance du routeur R1_S1 à destination du routeur R2_S1. La protection est par exemple mise en œuvre à l'aide du protocole IPSec en mode tunnel. La politique de sécurité affectée à chaque chiffreur permet de cloisonner les flux en provenance du réseau local S1 et à destination des usagers du réseau local S2. L'encapsulation IPSec permet de masquer aux réseaux étendus WAN_C et WAN_M les adresses des réseaux locaux S1 et S2. Le chiffreur Z_S2 assure un rôle équivalent au chiffreur Z_S1 pour le réseau local S2. Les adresses IP sur l'interface noire des chiffreurs sont les seules adresses visibles par les réseaux étendus WAN_M et WAN_C. Ce sont ces adresses qui sont utilisées par ces réseaux WAN pour router les flux en provenance et à destination des routeurs R2_S1 et R2_S2.

Les routeurs noirs R2_S1, R2_S2 sont situés entre les dispositifs de chiffrement Z_S1, Z_S2 et les réseaux étendus. Ils permettent l'aiguillage des flux vers les réseaux étendus en fonction de leur politique de traitement des flux. Une telle politique consiste, par exemple, à aiguiller les flux sensibles vers le réseau privé WAN_M et les flux non sensibles vers le réseau public WAN_C. Par ailleurs, les routeurs noirs R2_S1, R2_S2 ajustent la valeur du champ DSCP des paquets en fonction des classes de service offertes par les réseaux étendus WAN. Ils assurent également la mise en forme des paquets pour compenser la redondance introduite par les chiffreurs.

Le réseau étendu privé WAN_M véhicule les flux entre les réseaux locaux S1 et S2 selon un routage qui lui est propre. Le réseau étendu public WAN_C réalise les mêmes fonctions de routage en fonction de ses propres paramètres (topologie, protocoles de routage, QoS, etc.). Dans l'exemple d'architecture de la figure 2, le système comprend seulement deux réseaux étendus WAN_M, WAN_C, mais il pourrait s'appliquer également à un plus grand nombre de réseaux étendus. Les réseaux étendus WAN_M et WAN_C sont des fournisseurs de services de transport qui présentent les fonctionnalités suivantes :

- « Reporting » en temps réel de l'état des liaisons établies par le fournisseur de services. Si par exemple, suite à une intempérie, il devait y avoir une congestion au niveau du réseau WAN_C, les flux continueraient à

être aiguillés vers ce dernier alors qu'ils auraient pu être acheminés, au moins pour les plus vitaux d'entre eux, vers le réseau WAN_M. Le « Reporting » permet de mettre en œuvre ce type de politique d'aiguillage.

- « Pre-emption & Priority Management » : Les problèmes internes au niveau d'un WAN se traduisent dans la grande majorité des cas par une réduction de la bande passante équivalente et très rarement par une coupure franche de la transmission. La bande passante restante doit donc être gérée au mieux. Cette fonctionnalité permet une gestion stricte de la priorité, au niveau des au flux et non des paquets, et offrent des mécanismes de préemption permettant d'attribuer la bande passante restante au flux les plus vitaux.

- « Protection and Restoration (P&R) » : Certaines applications exigent qu'il n'y ait aucune interruption au niveau du transport des flux ou plus exactement que les interruptions restent inférieures à 50ms. Par ailleurs, cette exigence est totalement indépendante de la criticité de l'application (vitale ou non vitale). Le P&R permet d'exprimer auprès du WAN_C ou WAN_M le souhait d'un chemin de « back-up » de type 1 pour 1, 1 pour N voire P pour N. Il est aussi possible de mettre en œuvre ce type de mécanisme au niveau « overlay ». En d'autres termes, les chemins nominaux peuvent être établis sur un WAN et les chemins de « back-up » sur l'autre WAN.

- « Make before Break » : Cette fonctionnalité s'avère intéressante lorsque des opérations de maintenance doivent être conduites sur un WAN et que ces dernières impactent la continuité des liaisons établies. Il s'agit ici de « prévenir plutôt que de guérir ». De nouvelles routes sont calculées et mises en œuvre avant d'interrompre celles qui étaient en place. Ce type de mécanisme peut aussi être relayé au niveau « overlay ». Au lieu de trouver une alternative d'acheminent au sein d'un même WAN, le deuxième WAN est mis à contribution.

Les architectures de réseau selon la figure 2 permettent de solutionner partiellement le troisième problème décrit ci-dessus concernant l'aiguillage des flux chiffrés. En effet, il est possible de mettre en place une politique de routage basée sur le couple adresse IP destination et valeur du champ DSCP. Le chiffreur masque les adresses IP source et destination des

abonnés mais pour des raisons évidentes de routage ajoute en clair des adresses IP source et destination correspondant aux chiffreurs émetteur et récepteur. En d'autres termes, il s'agit de créer un nouvel en-tête de niveau de la couche réseau. Dans ce nouvel en-tête, la valeur du champ DSCP correspond à celle présentée en entrée.

Cependant, cette solution est très insuffisante pour opérer des politiques d'aiguillage avancées. En effet, la valeur du champ DSCP permet d'identifier le type de flux (temps réel / temps élastique, voix / data, ...) mais en aucun cas le niveau de criticité du flux. De plus, les politiques d'aiguillage ne peuvent s'appliquer qu'à l'ensemble du trafic allant d'un chiffreur à un autre, il n'y a plus de visibilité sur les abonnés ou groupe d'abonnés.

La figure 3 illustre le routage des flux dans un réseau du type de celui de la figure 2.

Chaque système autonome met en œuvre des protocoles de routage IGP (Interior Gateway Protocol) et EGP (Exterior Gateway Protocol) pour router les flux. Un exemple de protocole IGP est le protocole BGP (Border Gateway Protocol). Un exemple de protocole EGP est le protocole OSPF.

Les systèmes autonomes représentant les enclaves S1, S2, S3, S4 mettent en œuvre le protocole OSPF dans un domaine de routage qui comprend les routeurs rouges R1_S1, R1_S2, R1_S3, R1_S4 mais exclut les chiffreurs Z_S1, Z_S2, Z_S3, Z_S4. Les chiffreurs n'implémentent pas le protocole OSPF et ne sont pas capables d'établir une topologie de routage à partir de la source (eux mêmes) vers les destinataires. Le routage des flux dans les chiffreurs est réalisé par la politique de routage Security Policy (SP) et Security Association (SA), informations contenues dans la base de données SPD (« Security Policy Database »).

Les routeurs noirs R2_S1, R2_S2, R2_S3, R2_S4 mettent en œuvre le protocole OSPF pour permettre de prendre en compte dans les architectures complexes une entité indépendante administrativement du site principal, mais utilisant les ressources communes aux différents WAN. Les routeurs QoS étant gérés (Administration / Supervision) par l'entité du site principal. L'ensemble des routeurs QoS des sites de la même entité organisationnelle forment un fédérateur de transit vis à vis des sites de

desserte qu'ils raccordent et ceci pour une catégorie de flux donné (sensibles ou non sensibles).

Le protocole BGP est implémenté entre les routeurs R2_S1, R2_S2, R2_S3, R2_S4 et les réseaux WAN_M et WAN_C. Il permet de communiquer aux différents WAN les préfixes des sous réseaux présents dans les dessertes.

Les réseaux WAN implémentent un protocole de routage (OSPF par exemple). Il assure le routage des flux entre les différentes dessertes interconnectées. Ce protocole permet d'établir une topologie de routage en affectant des coûts aux chemins empruntés. Le choix de la route étant celui de moindre coût. Les préfixes indiqués dans les tables de routage des routeurs des réseaux WAN sont les préfixes des adresses noires de chiffreurs, les adresses du plan usager étant masquées par les chiffreurs.

Le protocole OSPF est un protocole à état de liens, pour fonctionner, il nécessite que les routeurs qui utilisent ce protocole soient adjacents, ce que l'on peut traduire par « être connexe par un lien direct », or, les chiffreurs ne permettent pas d'avoir un lien direct entre une entité non protégée et une entité protégée. Pour rétablir une connectivité entre les routeurs R1_S1, R1_S2, R1_S3, R1_S4 il est nécessaire d'utiliser des tunnels GRE, puis de mettre en œuvre le protocole OSPF sur ces « interfaces GRE ». Les tunnels GRE sont implémentés en surcouche de la couche IPsec (protocole ESP) et ils génèrent un surdébit de 4 octets supplémentaires. De lors il est possible de reconstruire une topologie de routage OSPF entre les dessertes au travers les tunnels GRE.

La gestion de la qualité de service est implémentée dans les routeurs R2_S1, R2_S2, R2_S3, R2_S4 . Dans chaque routeur elle doit être conforme à la politique de qualité de service vis-à-vis des réseaux WAN, WAN_M et WAN_C ainsi que celle des routeurs R1_S1, R1_S2, R1_S3, R1_S4, installés sur le site au profit des entités administratives. La cohérence globale de la qualité de service au profit d'un usager collectif qui doit véhiculer des flux sensibles et non sensibles n'est réalisable que par des opérations de configuration indépendantes des routeurs QoS, chaque routeur a à traiter des flux sensibles ou non sensibles.

Un but de l'invention est de résoudre au moins un des problèmes précités. La solution proposée permet de prendre les décisions de routage avant de chiffrer les informations et d'intégrer dans un seul et même produit toutes les fonctions nécessaires à l'interconnexion du MAN aux WANs. Les directives de routage sont établies du coté rouge du réseau et sont appliquées du coté noir.

Un avantage de la solution proposée est de pouvoir réaliser l'interconnexion d'un MAN avec des WANs en apportant des fonctions de résilience opérationnelles. L'emploi du routeur selon l'invention pour gérer des flux sécurisés de données comporte notamment les avantages suivants :

- permettre une coopération entre les plans de routage rouge et l'établissement des tunnels IPsec ;
- permettre un usage simultané des deux réseaux WAN en tenant compte des caractéristiques « instantanées » de ces WAN, taux d'occupation des ressources, délais de transit des paquets, gigue (QoS indicateurs) ;
- aiguiller les flux en provenance des dessertes en fonctions des états des WAN et selon le caractère de ces flux (priorité, type de flux, etc.) ;
- garantir l'acheminement d'une certaine catégorie de flux (flux vitaux) ;
- garantir la qualité de service de bout en bout, d'usager à usager ;
- offrir des fonctions de résilience opérationnelles ;
- assurer une cohérence du routage de bout en bout sur les réseaux VPN sécurisé ;
- optimiser les ressources de transit.

L'invention a notamment pour objet un système de gestion de flux sécurisés transmis entre un premier réseau local (S1) et au moins un second réseau local (S2) interconnectés par l'intermédiaire d'une pluralité de réseaux étendus WAN (WAN M, WAN C), caractérisé en ce que le dit système comporte au moins :

- un module d'observation (OB) recevant les flux de données émis depuis ledit premier réseau local (S1) et à destination d'au moins un desdits second réseau local (S2), ledit module d'observation (OB) étant adapté à associer à chaque paquet dudit flux un

tatouage permettant d'identifier les flux de données de manière unique,

- un module de chiffrement (CH) desdits paquets tatoués par ledit module d'observation (OB), l'opération de chiffrement excluant l'information tatouée,
- un module d'analyse (AN) qualitative et quantitative des flux de données émis depuis ledit premier réseau local (S1) permettant de classer les flux selon leur degré de priorité et/ou de sécurisation, ce degré étant déterminé au moins à partir de la source, de la destination ou du type d'utilisateur du flux,
- un module interface (IN) réalisant d'une part l'établissement et le maintien de liaisons de données point à point ou point à multipoint entre ledit premier réseau local (S1) et au moins un desdits réseau local (S2) distant, chaque liaison de données utilisant les moyens de transmission fournis par un ou plusieurs desdits réseaux étendus WAN et fournissant des caractéristiques de communications dans une plage de fonctionnement prédéterminées, et d'autre part l'aiguillage des flux sécurisés sur ces liaisons en fonction de règles cohérentes avec les opérations de tatouage dudit module d'observation (OB) et de chiffrement dudit module de chiffrement (CH),
- un module de décision (DE) associant à chaque flux de données, en fonction de leur degré de priorité et/ou de sécurisation déterminé par le module d'analyse (AN), une liaison de données prédéterminée parmi les liaisons de données établies par ledit module interface (IN) et en fonction de la probabilité d'acheminement correct d'un flux empruntant chaque liaison de données établie par ledit module interface (IN),
- un module d'analyse lexicale et syntaxique (ALS) des messages transmis entre ledit module de décision (DE) et ledit module interface (IN) de façon à assurer un cloisonnement des échanges entre ledit premier réseau local (S1) et lesdits réseaux étendus (WAN).

Dans une variante de réalisation de l'invention, ledit module d'observation (OB) réalise le tatouage des flux en modifiant la valeur du champ DSCP des paquets IP contenus dans lesdits flux.

Dans une variante de réalisation de l'invention, ledit module de chiffrement (CH) met en œuvre le protocole IPSec en mode tunnel.

Dans une variante de réalisation de l'invention, lesdits flux sont associés à une liaison de données utilisant un réseau étendu privé (WAN_M) ou un réseau étendu public (WAN_M) en fonction de la nature de leur source.

Dans une variante de réalisation de l'invention, les flux dont le degré de priorité est le plus élevé sont associés aux liaisons de données bénéficiant du débit disponible le plus élevé.

L'invention a également pour objet une méthode de gestion de flux sécurisés transmis entre un premier réseau local (S1) et au moins un second réseau local (S2) interconnectés par l'intermédiaire d'une pluralité de réseaux étendus WAN (RW1,WAN M,WAN C), lesdits réseaux locaux (S1, S2) comportant au moins une interface I1 d'entrée/sortie, lesdits réseaux étendus WAN comportant au moins une interface I2,I3 d'entrée/sortie, ladite méthode étant caractérisée en ce qu'elle comporte au moins les étapes suivantes pour chaque réseau local (S1, S2) :

- définir une pluralité de fonctions F1 à F9 aptes à être intégrées sur une plateforme matérielle et/ou logicielle unique connectée auxdites interfaces I1, I2, I3 desdits réseaux locaux et étendus,
- la fonction F1 assure la protection IPsec des flux en provenance des interfaces I1 et à destination des interfaces I2 et I3., la fonction F1 étant décomposée en sous fonctions F1.1 à F1.n, n représentant le nombre de réseaux étendus WAN,
- la fonction F2 assure l'établissement d'une pluralité de liaisons point à point entre lesdites plateformes matérielles connectées aux interfaces d'entrée/sortie de chaque réseau local (S1, S2),
- la fonction F3 assure l'aiguillage, selon leurs caractéristiques des flux en provenance et à destination de l'interface I1 dudit réseau local (S1) en séparant les flux en mode session des autres flux,
- la fonction F4 assure le traitement des flux en mode session,

- la fonction F5 assure le traitement des échanges entre la fonction F1 et la fonction F4, notamment en indiquant à la fonction F1, les débuts, fins et numéros de sessions compris dans lesdits flux,
- la fonction F6 assure le traitement des congestions,
- la fonction F7 assure l'interfonctionnement avec les réseaux étendus WAN, en récupérant les informations d'ingénierie de trafic (TE), en les synthétisant et en les communiquant à la fonction F1,
- les fonctions F2, F3, F4 et F5 sont des fonctions réseau dont l'administration est assurée par la fonction F8,
- la fonction F9 assure l'administration des fonctions de sécurité telle que la fonction F1.

D'autres caractéristiques apparaîtront à la lecture de la description détaillée donnée à titre d'exemple et non limitative qui suit faite en regard de dessins annexés qui représentent :

- la figure 1, un exemple d'une architecture d'un système selon l'art antérieur,
- la figure 2, une autre illustration de l'exemple d'architecture de la figure 1,
- la figure 3, une illustration du routage des flux de données dans un réseau du type des figures 1 ou 2,
- la figure 4, un synoptique de l'architecture générale du système selon l'invention dans un premier mode de réalisation,
- la figure 5, un exemple de mise en œuvre d'une première fonction F1 du procédé selon l'invention dans le premier mode de réalisation,
- la figure 6, un exemple de mise en œuvre d'une deuxième fonction F2 du procédé selon l'invention dans le premier mode de réalisation,
- la figure 7, un exemple de mise en œuvre d'une troisième fonction F3 du procédé selon l'invention dans le premier mode de réalisation,
- la figure 8, un exemple de mise en œuvre d'une quatrième fonction F4 du procédé selon l'invention dans le premier mode de réalisation,
- la figure 9, un exemple de mise en œuvre d'une cinquième fonction F5 du procédé selon l'invention dans le premier mode de réalisation,
- la figure 10, un exemple de mise en œuvre d'une sixième fonction F6 du procédé selon l'invention dans le premier mode de réalisation,

- la figure 11, un exemple de mise en œuvre d'une septième fonction F7 du procédé selon l'invention dans le premier mode de réalisation,
- la figure 12, un exemple de mise en œuvre d'une huitième fonction F8 et d'une neuvième fonction F9 du procédé selon l'invention dans le premier mode de réalisation,
- la figure 13, un synoptique de l'architecture du système selon l'invention dans un second mode de réalisation,

Le transfert de données par les réseaux IP n'est soumis à aucune garantie d'acheminement et de remise de ces données à un usager final, ce mode de fonctionnement en Best Effort est le mode de fonctionnement nominal des réseaux IP. A part quelques fonctionnalités spécifiques bâties sur le traitement du champ DSCP du paquet IP, associées à une gestion de files d'attente permettant un acheminement prioritaire de certains paquets IP par rapport à d'autres.

Pour garantir l'acheminement des données, il est implicitement nécessaire d'une part, d'établir une relation permanente entre les deux extrémités (usagers) pendant la durée de la communication. Seul un mode de fonctionnement connecté permet de garantir cette relation et d'autre part de procéder à une réservation de ressources sur les réseaux WAN correspondant aux besoins de la communication sur le trajet de celle-ci. Ces ressources étant réservées dans chaque équipement impliqué par la communication.

On décrit à présent, à l'appui des figures 4 à 12, un premier mode de réalisation d'une méthode et d'un système de gestion de flux sécurisés dans un réseau selon l'invention.

La figure 4 illustre l'architecture du système selon l'invention dans un premier mode de réalisation.

L'architecture du système selon l'invention met en œuvre un ensemble de fonctions dans le but de résoudre les limitations des architectures de réseau connues telles qu'illustrées sur les figures 1 et 2. En particulier l'invention permet, d'assurer une interconnexion sécurisée entre

un ou plusieurs réseaux locaux LAN et un ou plusieurs réseaux étendus WAN publics ou privés.

Le système selon l'invention est interfacé, d'une part avec un premier réseau local S1 par l'intermédiaire d'une interface I1 et d'autre part avec les réseaux étendus WAN disponibles, par l'intermédiaire d'une pluralité d'interfaces I2,I3,In, pour établir une liaison point à point entre ledit premier réseau local S1 et un ou plusieurs autres réseaux locaux S2 distants.

Une fonction F1 assure la protection sécurisée, par exemple par le biais du protocole IPSec, des flux en provenance des interfaces I1 et à destination des interfaces I2 et I3. La fonction F1 est décomposée en sous fonctions F1.1 à F1.n, n représentant le nombre de réseaux étendus WAN en interface avec le procédé. Une interface Ix est affectée à une sous fonction F1.x.

Une fonction F2 assure l'établissement d'une pluralité de liaisons point à point de caractéristiques de transfert prédéterminées entre le système selon l'invention connecté au premier réseau local S1 et les systèmes distants connectés aux autres réseaux locaux S2.

Une fonction F3 assure l'aiguillage et la reconnaissance des flux en provenance et à destination de l'interface I1. L'aiguillage des flux sépare les flux en mode session des autres flux.

Une fonction F4 assure le traitement des flux en mode session.

Une fonction F5 assure le traitement des relations entre la fonction F1 et la fonction F4. Elle permet notamment d'indiquer la fonction F1, les débuts et fins de sessions ainsi que les N° des sessions.

Une fonction F6 assure le traitement des aspects de congestions et le traitement des aspects relatifs au Trafic Engineering (TE) et commande l'aiguillage des flux reconnus par la fonction F3 sur les liaisons établies par la fonction F2 en fonction des états de congestion qu'elle détecte.

Une fonction F7 assure l'interfonctionnement avec les WAN noirs en traduisant les flux traversant la fonction F1 de manière à mettre en équivalence les liaisons point-à-point établies par la fonction F2 avec des chemins gérées par les réseaux WAN étendus. Elle a également en charge de récupérer les informations de TE des WAN noirs, de les synthétiser et de les communiquer à la fonction F1.

Une fonction F8 assure l'administration des fonctions réseaux. Les fonctions F2, F3, F4 et F5 sont des fonctions réseau.

Une fonction F9 assure le traitement des fonctions sécurité. La fonction F1 est une fonction de sécurité.

Des bases de données sont associées à ces fonctions, elles permettent de stocker les informations propres aux fonctions réseaux, sécurité ou des informations communes à ces deux fonctions. Ces bases de données appelées bases de données MIB (« Management Information Base ») sont les suivantes :

- une base de données MIB BD1 qui est dédiée aux opérations d'administration et de supervision des fonctions réseaux, accessible en lecture et écriture par la fonction F8.
- Une base de données MIB BD2 qui est dédiée aux opérations d'administration et de supervision des fonctions sécurité, accessible en lecture et écriture par la fonction F9.
- une base de données MIB BD3, commune aux fonctions réseaux et sécurité, accessible en lecture uniquement.

La figure 5 présente un exemple de mise en œuvre de la première fonction F1 du procédé selon l'invention. Les réseaux locaux S1,S2 sont chacun interconnectés aux réseaux étendus WAN_M,WAN_C par l'intermédiaire d'un système 501,502 selon l'invention qui met en œuvre les fonctions précitées. Les flux entrant et sortant des réseaux locaux LAN/MAN sur les interfaces I1 nécessitent une protection. Cette protection est assurée par la mise en œuvre de la fonction F1. La fonction F1 est une fonction IPsec en mode tunnel. Elle est réalisée pour chaque interface I2,I3 entre le système 501,502 selon l'invention et les réseaux étendus. Dans l'exemple de la figure 5, deux fonctions F1, respectivement notées F1.1,F1.2 sont réalisées pour chaque interface I2,I3. Les tunnels sont établis dynamiquement entre les fonctions F1.1,F1.2 exécutées par les systèmes 501,502 distants. La fonction F1 met en œuvre un procédé de découverte automatique des procédés distants. Elle assure l'authentification des procédés distants, l'entretient de la connectivité des tunnels IPsec entre les entités F1.1, F1.2 locales et distantes.

La figure 6 présente un exemple de mise en œuvre de la deuxième fonction F2 du procédé selon l'invention. L'utilisation de tunnels IPsec établis au travers de réseaux WAN nécessite de positionner d'autres tunnels GRE en superposition, ou overlay, de ces tunnels IPsec, ce principe n'est pas extensible sur des topologies réseaux importantes. Pour pallier ce défaut, la solution proposée est d'utiliser une fonction « underlay », c'est à dire de travailler au niveau inférieur à IPsec pour établir les relations entre entités distantes. Cette fonction désignée F2 permet d'établir une liaison point à point entre deux unités distantes, le protocole MPLS (« Multi-Protocol Label Switching ») est un des protocoles qui permet de satisfaire cette fonction. D'autres techniques comme les réseaux locaux virtuels VLAN peuvent également satisfaire la fonction F2. Les liaisons entre les fonctions F2 sont établies sur les interfaces I2 et I3. Les informations émises ou reçues par cette fonction F2 empruntent les interfaces I2 et I3.

La figure 7 présente un exemple de mise en œuvre de la troisième fonction F3 du procédé selon l'invention. La fonction F3 est en relation « full duplex » avec l'interface I1, c'est-à-dire en communication bidirectionnelle simultanée. Les flux en provenance de l'interface I1 sont aiguillés selon leurs caractéristiques vers la fonction F4 ou vers la fonction F2. Les flux en mode session, comme le protocole SIP (« Session InitiationProtocol ») par exemple, sont aiguillés vers la fonction F4, les autres flux sont aiguillés vers la fonction F2.

La fonction F3 permet également de prolonger vers le système selon l'invention les caractéristiques de cloisonnement entre usagers, comme les réseaux virtuels VLAN (« Virtual Local Area Network ») ou les tables de routage virtuelles VRF (« Virtual Routing and Forwarding Table »). Ces caractéristiques peuvent être acheminées par le procédé local vers les procédés distants.

La figure 8 présente un exemple de mise en œuvre de la quatrième fonction F4 du procédé selon l'invention.

La fonction F4 reçoit uniquement les flux en mode session en provenance de la fonction F3 (par exemple le protocole SIP). La fonction F4 interprète le protocole « session » et elle identifie dans le protocole le champ

qui porte les informations MLPP indiquant la priorité de la session, ces informations ont été forgées dans le champ concerné (le champ RP dans le cas du protocole SIP) par des entités fonctionnelles du réseau local LAN/MAN. Une requête RSVP (« Resource ReSerVation Protocol ») ou RSVP-TE (« Resource ReSerVation Protocol -Trafic Extension ») selon le réseau étendu WAN sous jacent est générée vers la fonction F4 du procédé distant destinataire de la session par l'intermédiaire de la fonction F3.

La fonction F4 met en œuvre un protocole de routage Internet de type IGP (« Interior Gateway Protocol ») ayant la capacité à établir une topologie de liens incluant des métriques de disponibilité de bande passante, de bande occupée, notamment. Le protocole OSPF-TE est un de ces protocoles qui peut convenir pour cette partie de fonction. Associé à ce protocole de routage internet, une sous fonction de calcul de meilleur chemin tenant compte des métriques évoquées ci-dessus permet de définir les meilleures routes pour joindre les systèmes de gestion des flux sécurisés distants. La sous fonction C-SPF est une des fonctions permettant de satisfaire ce calcul. Les informations issues de C-SPF sont indiquées comme paramètres dans la requête RSVP-TE. La fonction F4 génère des requêtes RSVP ou RSVP-TE que vers les réseaux WAN qui acceptent ces requêtes.

La figure 9 présente un exemple de mise en œuvre de la cinquième fonction F5 du procédé selon l'invention. La fonction F5 permet le dialogue entre les fonctions F4 et chaque fonction F1.1,F1.2. Cette fonction est une fonction de commande qui émet et/ou reçoit des messages en provenance ou à destination des fonctions F4 et F1. Les messages sont véhiculés par le protocole UDP (« User Datagram Protocol »). Les principaux messages permettent d'envoyer et de recevoir des informations sur les sessions de communications à ouvrir, à fermer ou sur le comportement à tenir vis-à-vis des communications en fonctions de paramètres issus de la fonction F1 et notamment de sa partie « interface noire ». La fonction F5 permet de faire le lien entre le numéro de session (par exemple, un numéro de LSP) et un contexte IPsec (par exemple un numéro de SPI, « Security Parameter Index »), informations contenues dans la SDP.

La figure 10 présente un exemple de mise en œuvre de la sixième fonction F6 du procédé selon l'invention. La fonction F6 est en relation avec les fonctions F3, F4. Elle met en œuvre plusieurs moyens et mécanismes pour gérer les congestions ou influer sur le traitement des flux, les opérations mises en œuvre par les fonctions F4 et F6 étant dénommées « politique de traitement des flux ».

La fonction F4 dispose de l'ensemble des contextes des sessions établies et en cours d'établissement, ainsi que des niveaux de priorité de ces sessions. En fonctionnement nominal, les flux sont routés vers les réseaux WAN présents en mode « actif – actif » c'est à dire que le routage choisit un des réseaux WAN selon les types de flux à router et les contraintes associées à ces flux. Ce principe permet d'utiliser toutes les capacités des réseaux WAN en même temps sans fonctionnement du type « actif – backup ». En cas de congestion signalée à la fonction F6, les principales méthodes utilisées pour influer sur le traitement des flux sont les suivantes, cette liste n'étant pas exhaustive :

- Mode DiffServ : le routage des flux est réalisé en fonction du champ DSCP et selon un nombre de classes de service ;
- Mode Bit ECN : Une congestion signalée sur positionnement du bit ECN sur une session ou une classe de service du type « données » provoque un changement du chemin de routage des flux concernés par cette congestion ;
- Mode SAA : La fonction met en œuvre des outils permettant de mesurer certaines caractéristiques des flux au travers des réseaux WAN. Ces outils permettent de mesurer la gigue, le délai de transit, la latence et ceci sur chacun des réseaux WAN. L'analyse des résultats peut provoquer un changement du chemin de routage des flux concernés par l'analyse des métriques, si ces derniers sont dans des valeurs hors des limites prescrites dans le contrat de niveau de service « SLA » ;
- Mode « déni de service ». Une attaque en déni de service est détectée par la fonction F1 et signalée à la fonction F4 au travers la fonction F5 est retransmisse à la fonction F6 qui provoque un changement du chemin de routage des flux concernés par cette attaque.

La figure 11 présente un exemple de mise en œuvre de la septième fonction F7 du procédé selon l'invention. Les flux entrant et sortant de et vers les réseaux WAN sur les interfaces I2, I3 sont véhiculés vers ces interfaces par la fonction F7. La fonction F7 est dupliquée en autant de fonctions (F7.1 à F7.n) qu'il existe de réseau WAN, cette duplication permet de rendre les actions et traitements indépendants sur les réseaux WAN.

La fonction F7, assure plusieurs sous fonctions et notamment :

- une sous-fonction de gestion du surdébit IPsec. La fonction F7 prend en compte le surdébit imposé par le chiffrement IPsec de manière implicite par une commande de gestion communiquée par la fonction F6. Le surdébit est exprimé en un nombre d'octets supplémentaires à prendre en compte dans le calcul de la qualité de service. La fonction F7 exprime un besoin utilisateur en bande passante correspondant au SLA (« Service Level Agreement », ou contrat de niveau de service) demandé par l'usager, cette expression de besoin est réalisée selon les classes de services. Un calcul est réalisé par la fonction F7 pour vérifier la cohérence entre les débits physiques des interfaces des réseaux locaux LAN/MAN et celles des réseaux étendus WAN, et les demandes exprimées par l'usager dans les classes de services exprimées.
- une sous fonction de calcul des meilleurs chemins à utiliser sur le réseau WAN à partir de la fonction F7.1,F7.2 concernée et en tenant compte des métriques de type TE (OSPF-TE et MPLS-TE).
- une sous fonction en relation avec l'extension ECN (« Notification explicite de congestion ») du protocole Internet, pour le calcul de la congestion, nombre de paquets en congestion, numéro de session incriminée, etc.

Les informations obtenues sont spécifiées dans un message à destination de la fonction F5. La fonction F1 retranscrit ces informations vers la fonction F5. Les messages sont du type TLV (« Type Length Value »), la fonction étant représentée par le champ « T » (Type).

La figure 12 présente un exemple de mise en œuvre de la huitième fonction F8 et de la neuvième fonction F9 du procédé selon l'invention.

Toutes les fonctions F1, F2, F3, F4, F5, F6 et F7 sont implémentées sur une base matérielle et logicielle commune. Les fonctions d'administration NOC et SOC peuvent cohabiter plus aisément, ce qui permet d'avoir des bases de données MIB dédiées à un domaine d'exploitation, une base MIB réseau et une base MIB sécurité ainsi qu'une base MIB commune contenant les informations « réseaux » et les informations « sécurité non sensibles ». Les informations sensibles comme les éléments de cryptologie (clés) sont contenues dans la base MIB dédiée à la sécurité. De ce fait les informations de sécurité sont toujours accessibles et elles ne nécessitent aucun équipement supplémentaire pour leurs accessibilités.

Le système selon l'invention regroupe l'ensemble des fonctions. Il constitue un seul et unique système autonome (SA). Son administration est assurée par un système autonome WAN ou par un système autonome MAN. Pour faciliter le suivi des contrats de niveau de service SLA, des informations issues de la base MIB d'administration réseau et sécurité (base MIB commune) sont accessibles en lecture seulement par le système autonome qui n'a pas la responsabilité de l'administration du procédé, afin de fournir une vision de la qualité de service au système autonome qui n'assure pas cette administration.

La fonction F8 est en relation avec les fonctions F2, F3, F4, F5 et F6 pour réaliser les opérations d'administration (configuration) et de supervision de ces fonctions. La fonction F9 est en relation avec la fonction F1 et F7 pour réaliser les opérations d'administration (configuration) et de supervision de cette fonction. La fonction F8 est en relation avec la base de données BD1. La base de données BD1 est en mode lecture et écriture. La fonction F9 est en relation avec la base de données BD2 et la base de données BD2 est en mode lecture et écriture. Enfin, la base de données BD3 reçoit des informations de la base de données DB1 et BD2, la base de données BD3 étant en mode lecture uniquement.

En résumé, selon une mise en œuvre, dans un premier mode de réalisation, de la méthode de gestion des flux sécurisés selon l'invention les étapes suivantes sont exécutées :

- Utiliser le protocole IPsec en mode tunnel pour mettre en œuvre la fonction F1 et les sous fonctions F1.x ;
- Utiliser un protocole de niveau 2 point à point entre la fonction F2 du procédé local et les procédés distants. Le protocole MPLS est un protocole candidat à cette fonction ;
- Utiliser un protocole de niveau 2 entre la fonction F2 et la fonction F1. Le protocole 802.1Q (VLAN) est ce protocole. Le numéro de VLAN permet d'établir une correspondance avec le numéro de SPI, identificateur du contexte de chiffrement de la session ;
- Aiguiller les flux en provenance des réseaux locaux LAN/MAN vers la fonction F4 et/ou vers la fonction F2. L'aiguillage vers la fonction F4 concerne les flux en mode session ;
- Générer par l'intermédiaire de la fonction F4 des requêtes RSVP vers la fonction F1. La fonction F1 interprète cette requête, la dirige vers le distant au travers du tunnel IPsec considéré et la fonction F1 génère vers le réseau étendu WAN noir la requête RSVP qui porte les attributs du contexte de la session ;
- Utiliser un protocole de communication entre les fonctions F1 et la fonction F5 pour autoriser l'échange de messages de signalisation entre ces fonctions et notamment les informations relatives aux numéros des sessions entre procédé local et distant ;
- Communiquer à la fonction F4 et F6 par l'intermédiaire de la fonction F5 les informations en provenance de la fonction F1 ;
- Utiliser, par la fonction F6, les informations issues de la fonction F7 et des sous fonctions F7.x retransmises par l'intermédiaire de la fonction F1. Ces informations sont véhiculées sous formes de messages et contiennent les informations de Qualité de Service issue des réseaux étendus WAN noirs ;
- Procéder à l'analyse des informations en provenance des réseaux étendus WAN noirs par l'intermédiaire de la fonction F7 et des sous fonctions F7.x. Communiquer ces informations à la fonction F1 ;

- Aiguiller les flux vers les fonctions F1.x en fonction de l'analyse des informations reçues ou procéder à la préemption des sessions en cours pour libérer des ressources ;
- Filtrer les informations en provenance de la fonction F7 par la fonction F1 et communiquer ces informations à la fonction F5 ;
- Administrer les informations réseaux des fonctions F2, F3, F4, F5 et F6 par l'intermédiaire de la fonction F8 et stocker ces informations dans une base de données (BD1). Rendre ces informations accessibles en mode lecture et écriture par les fonctions désignées ;
- Administrer les informations sécurité des fonctions F1, F7 par l'intermédiaire de la fonction F9 et stocker ces informations dans une base de données (BD2). Rendre ces informations accessibles en mode lecture et écriture par les fonctions désignées ;
- Faire communiquer les bases de données réseau (BD1) et sécurité (BD2) pour extraire les informations communes et les stocker dans une base de données (BD3). Rendre ces informations accessibles en mode lecture uniquement par les fonctions désignées ;

les fonctions F1 à F9 étant intégrées sur une plateforme matérielle et logicielle unique.

La répartition des fonctions F1 à F9 peut également être réalisée avec des plateformes matérielles et logicielles différentes. Le protocole de communication entre ces plateformes est un protocole de niveau 2.

Selon une mise en œuvre de la méthode selon l'invention, l'aiguillage des flux vers la fonction F4 concerne tous les flux en mode session et les tous les flux en mode non session.

Selon une mise en œuvre de la méthode selon l'invention, les informations issues de la fonction F7 concernant des informations de Traffic Engineering (TE) sont transmises vers la fonction F6 par l'intermédiaire de la fonction F1.

Selon une mise en œuvre de la méthode selon l'invention, l'administration des informations réseaux et de sécurité est consolidée dans une base de données unique.

La méthode selon l'invention comporte de multiples avantages :

- une amélioration de la résilience des communications et des services ;

- une optimisation des ressources de transmission louées (VPN Opérateurs) ;
- la possibilité de mettre en œuvre des mécanismes de préemption des flux vitaux et donc assurer la garantie d'acheminement des flux vitaux ;
- une amélioration de la qualité de service à l'ensemble des flux en discriminant les types de flux en fonction des usages.

Elle réalise les opérations de routage et notamment le choix de la route pour atteindre la cible avant de réaliser les opérations de chiffrement en tenant compte de critères qualitatifs sur l'état des chemins empruntés (qualité de service, délais de transit, taux d'occupation des ressources, perte de paquets, par exemple). Elle nécessite une collaboration étroite entre les entités de chiffrement et l'entité de routage.

L'invention est à présent décrite dans un second mode de réalisation illustré par le synoptique de la figure 13.

Le système 100 selon l'invention met en œuvre la méthode de gestion de flux sécurisés décrite ci-dessus. Le système 100 permet, notamment, une interconnexion sécurisée d'un premier réseau local S1 avec une pluralité d'autres réseaux locaux distants à travers des réseaux étendus WANs publics ou privés.

Le système 100 comporte un module d'observation OB qui reçoit les flux en provenance du réseau local S1 et les transmet à un dispositif CH de chiffrement qui assure la fonction de sécurisation desdits flux, par exemple à l'aide du protocole IPSec. Les flux chiffrés sont ensuite transmis à un module interface IN qui aiguille les flux vers un ou plusieurs réseaux étendus WAN en fonction de critères prédéterminés.

Le système 100 comporte également un module d'analyse AN qui reçoit une copie de chaque paquet reçu par le module d'observation OB et qui identifie des flux et leur associe un degré de priorité et/ou de sécurisation ainsi que des exigences en terme de qualité de service, et un module de décision DE qui reçoit des informations du module d'analyse AN concernant chacun des flux identifiés et des informations sur la disponibilité de liaisons point-à-point ou point-à-multipoint entre modules interface IN et de

caractéristiques prédéterminés par l'intermédiaire d'un module d'analyse lexicale et syntaxique ALS.

Un des buts du système 100 selon l'invention est d'assurer un aiguillage des flux transmis depuis le réseau local S1 vers un ou plusieurs réseaux étendus WANs en assurant une différentiation des services et une transmission de chaque flux vers le réseau étendu WAN le plus adapté en fonction de contraintes prédéterminées et de l'état de ces réseaux étendus. La difficulté d'une telle adaptation réside dans la présence du dispositif de chiffrement CH qui impose un cloisonnement entre les flux coté rouge (réseau local) et coté noir (réseau étendu) et donc un empêchement d'échange d'informations entre les routeurs rouges R1_S1 et les routeurs noirs R2_S1.

Chaque module du système 100 selon l'invention est à présent décrit plus en détail.

Le module d'observation OB réalise deux fonctions. La première fonction consiste à dupliquer chaque paquet reçu depuis le réseau local S1 et à transmettre une copie de chaque paquet vers le module d'analyse AN. La seconde fonction consiste à associer à chaque paquet, un tatouage spécifique sous forme d'un champ de l'entête du paquet ou de la trame qui transporte ce paquet lors des échanges entre modules de façon à identifier les flux de manière unique dans la suite de traitements effectués par les différents modules. L'identification des flux permet de prendre en compte les contraintes de transmission propres à chaque flux. Par contrainte de transmission on entend notamment le débit nécessaire à l'acheminement du flux vers sa destination ou les contraintes en termes de délai, de gigue ou de taux de pertes paquets qu'un flux peut supporter tout en garantissant son acheminement ou encore le degré de sécurisation qui doit être pris. En fonction de ces contraintes de transmission, on choisit le medium de transmission, en l'occurrence une des liaisons de module IN à module IN à travers des réseaux étendus WANs disponibles la plus adaptée à chaque flux de façon à garantir son acheminement jusqu'à sa destination. Le tatouage de chaque paquet se fait, par exemple en modifiant la valeur du champ DSCP (Differentiated Services Code Point) d'un paquet IP ou en fixant des adresses MAC de la trame transportant le paquet.

Le module d'observation OB exécute en outre la fonction F3 précédemment décrite pour le premier mode de réalisation de l'invention.

Le module de chiffrement CH assure la sécurisation des flux de données par un chiffrement en mode tunnels. Les tunnels sont établis dynamiquement entre chaque module de chiffrement de chaque système connecté à un réseau local source ou destination. Les paquets transmis par le module d'observation OB sont chiffrés intégralement et encapsulés dans un paquet ou une trame où l'identification du flux sera au moins localement lisible, par exemple par le biais du champ DSCP du paquet encapsulant.

Le module de chiffrement CH exécute en outre la fonction F1 précédemment décrite pour le premier mode de réalisation de l'invention.

Le module d'analyse AN effectue une analyse qualitative et quantitative des flux circulant entre le réseau local S1 et les réseaux LAN distants. Cette analyse permet d'anticiper les besoins et de juger de la bonne adéquation entre besoins et moyens d'interconnexion en place. Chaque flux identifié se voit associer des contraintes d'écoulement à respecter. En fonction de catégories prédéfinies, le module d'analyse AN associe le degré de priorité du flux à un besoin minimum en bande passante. L'analyse du degré de priorité d'un flux est effectuée, par exemple, par une interprétation du protocole « session » en identifiant le champ qui porte les informations indiquant la priorité de la session qui est déterminée par des entités fonctionnelles du réseau MAN.

Le module d'analyse AN exécute en outre la fonction F4 précédemment décrite pour le premier mode de réalisation de l'invention.

Le module de décision DE établit la politique d'aiguillage des flux vers le réseau étendu WAN le plus approprié en fonction d'une part des contraintes d'écoulement à respecter de chacun des flux et du nombre de flux à servir déterminé par le module d'analyse AN, et d'autre part des disponibilités constatées des réseaux étendu WAN. Le module de décision DE détermine ainsi les services de transport qui doivent être initiés, modifiés ou annulés conformément aux règles d'aiguillages établies. A cet effet, il génère des messages adaptés permettant une communication sécurisée des

choix d'aiguillage vers le module interface IN. Les messages générés par le module de décision DE doivent garantir le cloisonnement des flux de données entre la partie noire et la partie rouge du réseau. En particulier les messages transmis entre le module de décision DE et le module interface IN ne doivent pas être corrélés aux flux de données qui transitent entre le réseau local S1 et les réseaux étendus WAN. Pour garantir le cloisonnement entre parties rouges et noires du réseau, le module de décision DE met en œuvre un ensemble de contrôles, de type machine à états. Le module de décision DE prend également en compte, dans l'affectation des flux à un réseau WAN, le surdébit ajouté par le module de chiffrement CH. Ce surdébit est notamment pris en compte pour le calcul du débit de transmission requis pour l'acheminement d'un flux en fonction de son degré de priorité.

Le module de décision DE exécute en outre les fonctions F6 et F7 précédemment décrites pour le premier mode de réalisation de l'invention.

Le module d'analyse lexicale et syntaxique ALS des messages échangés entre le module de décision DE et le module interface IN permet de réaliser un cloisonnement entre les parties rouge et noire du réseau. Les messages provenant du module interface IN ne sont acceptés par le module ALS que s'ils interviennent en réponse à une requête explicite formulée par le module de décision DE. Ces messages contiennent, notamment, les attributs d'entête de paquets chiffrés qui permettent d'identifier la liaison utilisée parmi les réseaux WANs disponibles ainsi que les caractéristiques de cette liaison. Le module d'analyse lexicale et syntaxique ALS constitue une passerelle sécurisée permettant d'une part d'informer le module interface IN des décisions d'aiguillage prises par le module de décision DE et d'autre part d'indiquer au module de décision DE l'état des liaisons établies par les réseaux étendus WANs.

La sécurisation établie par le module ALS permet de résister aux attaques en déni de service en provenance potentielle des réseaux étendus WANs. Elle garantie également l'absence de fuites d'informations.

Le module d'analyse lexicale et syntaxique ALS exécute en outre la fonction F5 précédemment décrite pour le premier mode de réalisation de l'invention.

Le module interface IN réalise l'établissement de liaisons point à point ou point-à-multipoint entre le réseau local S1 et au moins un autre réseau distant S2 à travers un ou plusieurs réseaux WAN étendus. Il s'assure que chaque liaison opère dans la plage de fonctionnement prédéterminée et sur laquelle le module de décision DE a établit sa politique d'aiguillage. Il fournit l'état de disponibilité des liaisons établies au module de décision DE, via le module ALS. L'établissement de liaisons point à point ou point-à-multipoint se fait, par exemple, à l'aide du mécanisme de transport de données MPLS (Multiprotocol Label Switching) ou par introduction de réseaux virtuels VLAN. A partir des messages transmis par le module de décision DE, le module interface IN peut appliquer la politique d'aiguillage établie, pour chaque flux chiffré, en fonction de son identification Une liaison est caractérisée d'une part par les identifiants des réseaux locaux S1, S2 qu'elle met en relation et d'autre part par les paramètres de transfert des données sur cette liaison. Ces paramètres sont notamment le délai de transfert, le taux moyen de pertes paquets, le niveau de sécurité, le niveau de criticité, le débit continu maximal, le temps maximum d'interruption de service. Une liaison est identifiée par une combinaison d'attributs d'entêtes de paquets chiffrés, dont notamment le champ DSCP et les adresses source et destination du flux. Une liaison est maintenue conformément à ses caractéristiques prédéterminées. Par exemple, en cas de dysfonctionnement d'un réseau WAN, la liaison peut être maintenue en utilisant d'autres moyens de transmission, par exemple des moyens de transmission par satellite.

Le module interface IN met également en œuvre un protocole de routage à état de lien IGP ayant la capacité à établir une topologie de liens incluant des métriques de disponibilité de bande passante et de bande occupée. Par exemple, un protocole de routage adapté à cet effet est le protocole OSPF-TE. Associé à ce protocole, une fonction de calcul du plus court chemin est exécutée. Elle tient compte desdites métriques afin de définir les meilleures routes pour joindre le réseau destinataire.

Le module interface IN exécute en outre les fonctions F2,F4 et F7 précédemment décrites pour le premier mode de réalisation de l'invention.

Le système 100 selon l'invention et les modules dont il est composé sont implémentés sur une base matérielle et/ou logicielle commune.

5

REVENDICATIONS

1. Système (100) de gestion de flux sécurisés transmis entre un premier réseau local (S1) et au moins un second réseau local (S2) interconnectés par l'intermédiaire d'une pluralité de réseaux étendus WAN (WAN M, WAN C), caractérisé en ce que le dit système (100) comporte au moins :
   - un module d'observation (OB) recevant les flux de données émis depuis ledit premier réseau local (S1) et à destination d'au moins un desdits second réseau local (S2), ledit module d'observation (OB) étant adapté à associer à chaque paquet dudit flux un tatouage permettant d'identifier les flux de données de manière unique,
   - un module de chiffrement (CH) desdits paquets tatoués par ledit module d'observation (OB), l'opération de chiffrement excluant l'information tatouée,
   - un module d'analyse (AN) qualitative et quantitative des flux de données émis depuis ledit premier réseau local (S1) permettant de classer les flux selon leur degré de priorité et/ou de sécurisation, ce degré étant déterminé au moins à partir de la source, de la destination ou du type d'utilisateur du flux,
   - un module interface (IN) réalisant d'une part l'établissement et le maintien de liaisons de données point à point ou point à multipoint entre ledit premier réseau local (S1) et au moins un desdits réseau local (S2) distant, chaque liaison de données utilisant les moyens de transmission fournis par un ou plusieurs desdits réseaux étendus WAN et fournissant des caractéristiques de communications dans une plage de fonctionnement prédéterminées, et d'autre part l'aiguillage des flux sécurisés sur ces liaisons en fonction de règles cohérentes avec les opérations de tatouage dudit module d'observation (OB) et de chiffrement dudit module de chiffrement (CH),
   - un module de décision (DE) associant à chaque flux de données, en fonction de leur degré de priorité et/ou de sécurisation déterminé par le module d'analyse (AN), une liaison de données prédéterminée parmi les liaisons de données établies par ledit module interface (IN) et en fonction de la probabilité

d'acheminement correct d'un flux empruntant chaque liaison de données établie par ledit module interface (IN),

- un module d'analyse lexicale et syntaxique (ALS) des messages transmis entre ledit module de décision (DE) et ledit module interface (IN) de façon à assurer un cloisonnement des échanges entre ledit premier réseau local (S1) et lesdits réseaux étendus (WAN).

2. Système (100) de gestion de flux sécurisés selon la revendication 1 caractérisé en ce que ledit module d'observation (OB) réalise le tatouage des flux en modifiant la valeur du champ DSCP des paquets IP contenus dans lesdits flux.

3. Système (100) de gestion de flux sécurisés selon l'une des revendications précédentes caractérisé en ce que ledit module de chiffrement (CH) met en œuvre le protocole IPSec en mode tunnel.

4. Système (100) de gestion de flux sécurisés selon l'une des revendications précédentes caractérisé en ce que lesdits flux sont associés à une liaison de données utilisant un réseau étendu privé (WAN_M) ou un réseau étendu public (WAN_M) en fonction de la nature de leur source.

5. Système (100) de gestion de flux sécurisés selon l'une des revendications précédentes caractérisé en ce que les flux dont le degré de priorité est le plus élevé sont associés aux liaisons de données bénéficiant du débit disponible le plus élevé.

6. Méthode de gestion de flux sécurisés transmis entre un premier réseau local (S1) et au moins un second réseau local (S2) interconnectés par l'intermédiaire d'une pluralité de réseaux étendus WAN (RW1,WAN M,WAN C), lesdits réseaux locaux (S1, S2) comportant au moins une interface I1 d'entrée/sortie, lesdits réseaux étendus WAN comportant au moins une interface I2,I3 d'entrée/sortie, ladite méthode étant

caractérisée en ce qu'elle comporte au moins les étapes suivantes pour chaque réseau local (S1, S2) :

- définir une pluralité de fonctions F1 à F9 aptes à être intégrées sur une plateforme matérielle et/ou logicielle unique connectée auxdites interfaces I1, I2, I3 desdits réseaux locaux et étendus,
- la fonction F1 assure la protection IPsec des flux en provenance des interfaces I1 et à destination des interfaces I2 et I3., la fonction F1 étant décomposée en sous fonctions F1.1 à F1.n, n représentant le nombre de réseaux étendus WAN,
- la fonction F2 assure l'établissement d'une pluralité de liaisons point à point entre lesdites plateformes matérielles connectées aux interfaces d'entrée/sortie de chaque réseau local (S1, S2),
- la fonction F3 assure l'aiguillage, selon leurs caractéristiques des flux en provenance et à destination de l'interface I1 dudit réseau local (S1) en séparant les flux en mode session des autres flux,
- la fonction F4 assure le traitement des flux en mode session,
- la fonction F5 assure le traitement des échanges entre la fonction F1 et la fonction F4, notamment en indiquant à la fonction F1, les débuts, fins et numéros de sessions compris dans lesdits flux,
- la fonction F6 assure le traitement des congestions,
- la fonction F7 assure l'interfonctionnement avec les réseaux étendus WAN, en récupérant les informations d'ingénierie de trafic (TE), en les synthétisant et en les communiquant à la fonction F1,
- les fonctions F2, F3, F4 et F5 sont des fonctions réseau dont l'administration est assurée par la fonction F8,
- la fonction F9 assure l'administration des fonctions de sécurité telle que la fonction F1.