Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE

Secrétariat général
de la défense
et de la sécurité nationale

*Agence nationale de la sécurité
des systèmes d'information*

Paris, le 3 août 2015

N° DAT-NT-003/ANSSI/SDE/NP

Nombre de pages du document
(y compris cette page) : 18

Note technique

Recommandations de sécurité relatives à IPsec [1] pour la protection des flux réseau

Public visé :

Développeur	
Administrateur	✓
RSSI	✓
DSI	✓
Utilisateur	

1. Internet Protocol Security

Informations

Avertissement

Ce document rédigé par l'ANSSI présente les **« Recommandations de sécurité relatives à IPsec [a] pour la protection des flux réseau »**. Il est téléchargeable sur le site www.ssi.gouv.fr/ipsec. Il constitue une production originale de l'ANSSI. Il est à ce titre placé sous le régime de la « Licence ouverte » publiée par la mission Etalab (www.etalab.gouv.fr). Il est par conséquent diffusable sans restriction.

Ces recommandations sont livrées en l'état et adaptées aux menaces au jour de leur publication. Au regard de la diversité des systèmes d'information, l'ANSSI ne peut garantir que ces informations puissent être reprises sans adaptation sur les systèmes d'information cibles. Dans tous les cas, la pertinence de l'implémentation des éléments proposés par l'ANSSI doit être soumise, au préalable, à la validation de l'administrateur du système et/ou des personnes en charge de la sécurité des systèmes d'information.

a. Internet Protocol Security

Personnes ayant contribué à la rédaction de ce document :

Contributeurs	Rédigé par	Approuvé par	Date
LAM, LRP, COSSI	DAT	SDE	31 août 2012
DAT	DAT	SDE	3 août 2015

Évolutions du document :

Version	Date	Nature des modifications
1.0	31 août 2012	Version initiale
1.1	3 août 2015	Corrections mineures Exemples de groupes de DH

Pour toute remarque :

Contact	Adresse	@mél	Téléphone
Bureau Communication de l'ANSSI	51 boulevard de La Tour-Maubourg 75700 Paris Cedex 07 SP	communication@ssi.gouv.fr	01 71 75 84 04

Table des matières

1 Préambule

Les systèmes d'information adoptent généralement aujourd'hui une architecture distribuée. Les différentes briques logicielles et matérielles qui les composent sont de plus en plus communicantes, non seulement entre elles mais également avec des systèmes d'information distants et à travers l'internet. La montée en puissance de l'informatique en nuage et de l'externalisation ne font qu'accélérer cette tendance.

Tout comme ces différentes briques peuvent être critiques pour un système d'information, les flux de communication entre elles peuvent l'être également. Ces flux regroupent de nombreuses informations sensibles (données d'authentification, informations métier confidentielles, commandes de pilotage d'installations industrielles, etc.). L'interception ou l'altération de ces informations par des individus potentiellement malveillants représentent des risques non négligeables dans un contexte où les cyberattaques sont de plus en plus nombreuses et sophistiquées. La protection de ces flux sensibles est alors primordiale.

Force est pourtant de constater que cette problématique n'est pas toujours bien appréhendée, et que de nombreux flux réseau sensibles ne sont pas protégés comme ils le devraient. IPsec est une suite de protocoles de communication sécurisée permettant la protection des flux réseau. Elle est éprouvée mais souvent mal maîtrisée et reste encore trop peu ou mal employée.

2 Présentation d'IPsec

IPsec permet, par encapsulation, de protéger en confidentialité, intégrité et anti-rejeu un flux au niveau de la couche réseau (couche « Internet » de la pile TCP/IP ou couche 3 « réseau » du modèle OSI). IPsec est normalisé par l'IETF, au travers notamment des RFC 4301 à 4309. Plusieurs versions se sont succédées et divers éléments additionnels ont été définis. Un inventaire en est donné dans la RFC 6071.

Un très grand nombre d'équipements réseaux, en particulier les routeurs et les pare-feux, permettent l'utilisation d'IPsec. De même, les principaux systèmes d'exploitation pour micro-ordinateurs ou ordiphones prennent en charge IPsec nativement. Le dialogue IPsec est généralement possible entre ces différents systèmes et équipements.

Dans de nombreux cas, l'utilisation d'IPsec présente un rapport "bénéfice en sécurité" sur "coût" appréciable dans la mesure où cette technologie est prise en charge nativement par la plupart des systèmes clients et des équipements réseau et ne nécessite donc généralement pas d'investissements lourds. Il s'agit par ailleurs d'un protocole arrivé à maturité et bien connu. Sa mise en œuvre peut donc se faire sans charge excessive pour les équipes d'administration.

3 Glossaire

AH *Authentication Header* : protocole faisant partie de la suite IPsec, cf 6.1.1.

ESP *Encapsulation Security Payload* : protocole faisant partie de la suite IPsec, cf 6.1.2.

IKE *Internet Key Exchange* : protocole d'échange de clés, cf 6.4.3.

VPN *Virtual Private Network* : réseau privé virtuel.

IETF *Internet Engineering Task Force* : organisme à l'origine des standards Internet.

RFC *Request for comments* : documents émanant de l'IETF, tels que les standardisations de protocoles.

NAT *Network Address Translation* : mécanisme de traduction d'adresses réseau.

TLS *Transport Layer Security* : protocole de sécurisation en couche applicative.

SSL *Secure Socket Layer* : version obsolète de TLS.

LS *Liaison spécialisée.*

MPLS *Multiprotocol Label Switching* : protocole fonctionnant par commutation de labels, utilisé notamment dans les offres de type « IP-VPN ».

RGS *Référentiel général de sécurité* : document disponible sur `www.ssi.gouv.fr/rgs`.

MTU *Maximum Transmission Unit* : taille maximale d'un paquet pouvant être émis ou reçu sur une interface réseau.

4 Différents cas d'usage d'IPsec

La technologie IPsec est la plupart du temps associée aux connexions de réseau privé virtuel (Virtual Private Network) qui, bien souvent, transitent sur un réseau public tel que l'internet. Il est toutefois important de noter que cet usage d'IPsec est loin d'être le seul possible.

4.1 Accès distants en nomadisme

Les flux réseau échangés entre un poste en situation de nomadisme et le système d'information doivent être protégés. IPsec est très souvent employé pour la connexion à distance d'un poste à un réseau privé et se prête effectivement bien à ce cas d'usage. Le VPN est habituellement monté entre un poste client (ordinateur portable ou ordiphone par exemple, via un client VPN logiciel) et un équipement réseau de sécurité (pare-feu ou boitier VPN).

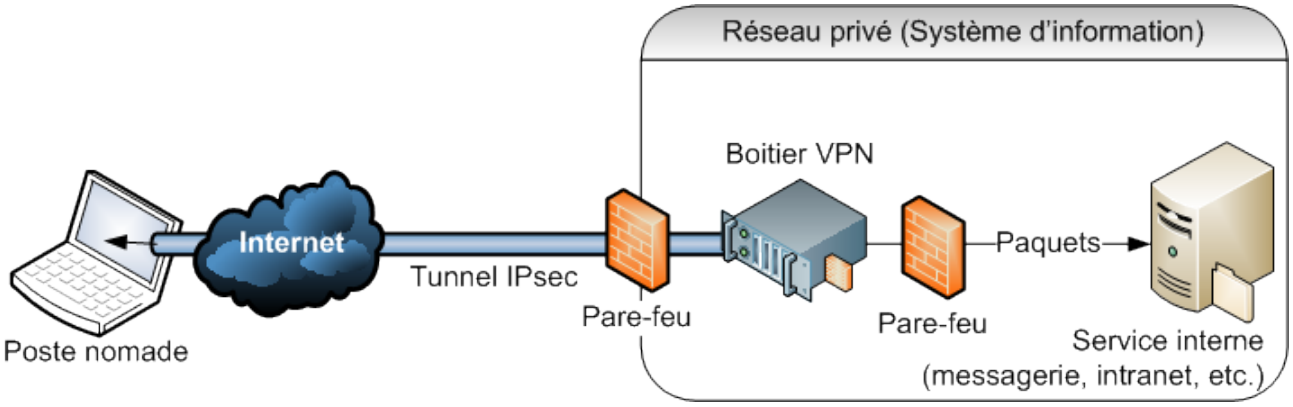

FIGURE 1 – Exemple d'emploi d'IPsec dans le cas d'un VPN.

La protection apportée est certes plus évidente pour des applications qui ne reposent pas sur des protocoles sécurisés (tels que TLS), mais il est recommandé de recourir systématiquement à IPsec y compris pour des applications bénéficiant d'une sécurisation en couche applicative. Cela s'inscrit dans une démarche de défense en profondeur et permet en outre d'adopter une politique plus simple à définir et à maintenir. IPsec apporte alors généralement la protection en intégrité et en confidentialité après une authentification préalable. L'usage d'IPsec comme technologie de protection des flux VPN est donc à privilégier et complète utilement les protocoles tels que PPTP ou L2TP.

R1 - Équipements de confiance

> Un certain nombre de logiciels ou d'équipements réseau destinés à la mise en oeuvre de VPN IPsec ont été évalués par l'ANSSI et ont obtenu une certification de sécurité ou une qualification. Il est recommandé de recourir à ces produits, en priorité à ceux qui sont qualifiés, (listés sur www.ssi.gouv.fr/fr/certification-qualification/) dès lors qu'il existe un besoin de produits de confiance.

4.2 Liaison de deux sites distants

Il est également possible d'utiliser IPsec pour relier de manière sécurisée les réseaux locaux de deux sites distants. Cela permet de se prémunir de malveillances qui consisteraient à accéder au lien entre ces deux réseaux, et à ainsi intercepter des informations sensibles ou procéder à des attaques par le milieu.

L'intérêt d'utiliser IPsec est avéré lorsque le lien considéré s'appuie sur un réseau public (tel que l'internet), mais l'est également lorsqu'un lien loué (de type LS ou VPN MPLS par exemple) est utilisé.

Dans ce contexte, le lien IPsec est généralement monté entre deux équipements dédiés ou entre deux pare-feux périmétriques au système d'information. La recommandation R1 est aussi applicable à ce cas d'usage.

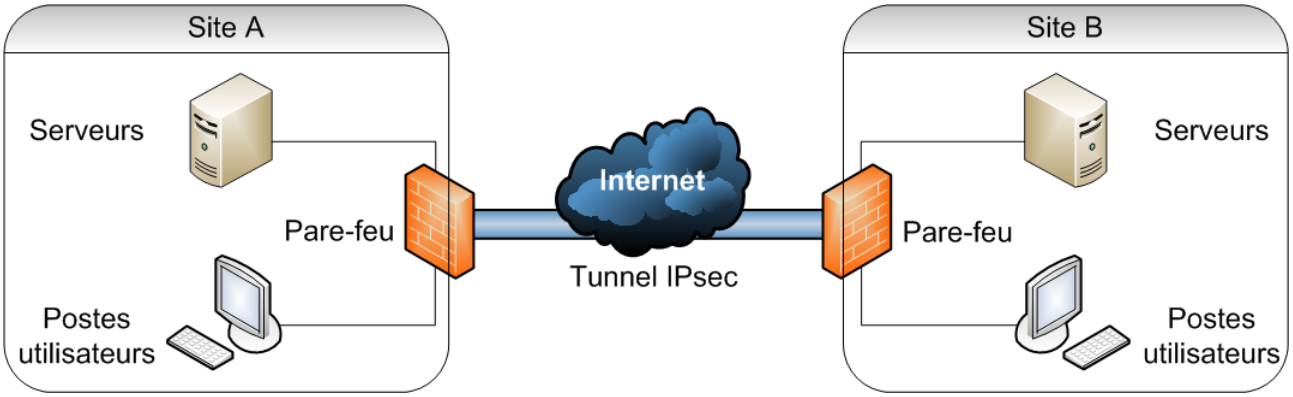

FIGURE 2 – Exemple d'emploi d'IPsec entre sites distants.

Note : Dans cet exemple, un tunnel IPsec est monté entre deux pare-feu.

4.3 Protection vis à vis d'une faiblesse protocolaire ou d'une vulnérabilité logicielle

Il arrive qu'il soit nécessaire de gérer la subsistance dans un système d'information d'équipements ou de briques logicielles dont les mécanismes de confidentialité ou d'authentification ne sont pas à l'état de l'art (voire inexistant), et dont les communications réseau ne sont donc pas protégées efficacement. Des individus malveillants qui auraient accès à ces flux (parce qu'ils transitent par des liens réseau publics ou insuffisamment sécurisés), pourraient alors les intercepter ou procéder à des attaques par le milieu. Ceci est par exemple souvent le cas :

- sur les systèmes SCADA en milieu industriel, utilisant des protocoles de communication de faible robustesse ;
- entre serveurs applicatifs et systèmes de gestion de bases de données ;
- entre briques applicatives distribuées utilisant des protocoles propriétaires, ou des bus logiciels pas ou mal sécurisés ;
- entre clients et serveurs utilisant des protocoles non sécurisés (FTP, POP3, SMTP, HTTP, RDP, VNC, etc.) ;
- etc.

Nombreux sont les cas ou les flux réseau doivent être protégés par des solutions tierces. IPsec se présente alors comme la technologie idéale pour pallier certaines faiblesses des protocoles de plus haut niveau. Son emploi est donc recommandé pour encapsuler des flux réseau véhiculant des informations jugées sensibles, et ainsi leur assurer la protection nécessaire. Lorsque les nœuds terminaux ne prennent pas en charge IPsec, il peut être nécessaire d'interposer des équipements réseau intermédiaires. La recommandation R1 s'applique alors à nouveau. On ne négligera pas, dans ce cas, le risque résiduel constitué par les tronçons d'extrémité en clair.

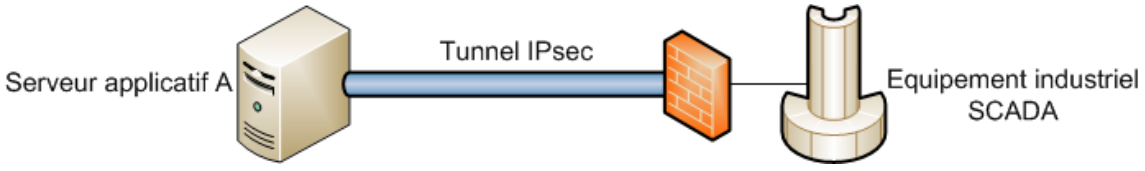

FIGURE 3 – Exemple d'emploi d'IPsec avec un équipement intermédiaire.

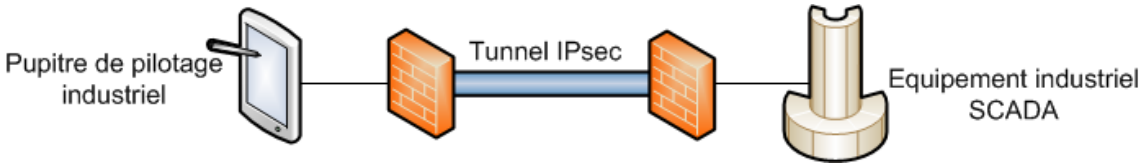

FIGURE 4 – Exemple d'emploi d'IPsec avec deux équipements intermédiaires.

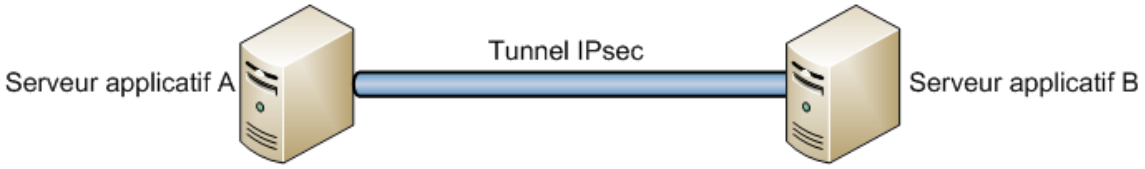

FIGURE 5 – Exemple d'emploi d'IPsec de point à point.

4.4 Défense en profondeur

Dans le cadre d'une défense en profondeur, IPsec peut être utilisé comme mesure de sécurité additionnelle pour encapsuler des protocoles qui sont déjà sécurisés par d'autres mécanismes voire un tunnel IPsec existant. Comme déjà indiqué, IPsec étant dans la plupart des cas peu couteux à mettre en place, il peut permettre de renforcer le niveau de sécurité de manière efficiente.

5 Comparaison avec TLS

Il est fréquent de voir IPsec comparé au protocole TLS [2]. Il est vrai que les deux technologies permettent de bénéficier de mécanismes de confidentialité, d'intégrité ou d'authentification. Il existe toutefois plusieurs différences importantes, qui tendent à faire préférer IPsec.

TLS agit beaucoup plus haut dans la pile réseau qu'IPsec, en se plaçant au dessus de la couche transport réalisée par TCP. TLS est souvent employé pour sécuriser d'autres protocoles : c'est ainsi que fonctionne par exemple le protocole HTTPS. C'est toutefois sur un autre usage que ce protocole entre en concurrence avec IPsec, à savoir la mise en oeuvre de « VPN-SSL ». Cette méthode consiste à encapsuler un flux réseau dans une session TLS. Certaines solutions de ce type proposent de s'appuyer sur un navigateur pour se dispenser de la nécessité de déployer un client spécifique sur les postes utilisateurs.

Le premier inconvénient de TLS est que les opérations liées à la sécurité sont effectuées en espace utilisateur, au sein du processus utilisateur. Ces opérations (et les secrets qu'elles manipulent) sont alors nettement plus exposées aux attaques que dans le cas d'IPsec où les opérations critiques se déroulent au sein du noyau ou dans des processus dédiés. Cela est d'autant plus vrai dans le cas où le client VPN s'appuie sur un navigateur, logiciel présentant une surface d'attaque considérable, y compris à distance.

En outre, sur le plan cryptographique, plusieurs éléments plaident en faveur d'IPsec. D'une part, IPsec permet plus largement l'utilisation d'algorithmes modernes recommandés par les bonnes pratiques, que ce soit en termes de prise en compte dans les standards ou d'implantations concrètes dans les logiciels disponibles sur le marché. D'autre part, dans IPsec, l'utilisation des primitives cryptographiques est légèrement meilleure au regard des bonnes pratiques. IPsec recourt, par exemple, à un fonctionnement « Encrypt-then-MAC », méthode considérée plus sûre que le « MAC-then-Encrypt » employé par TLS.

Enfin, on peut observer que le détournement de TLS de l'usage initialement prévu [3] en recourant à des « VPN SSL » n'est pas une solution idéale. L'encapsulation de paquets de la couche réseau en couche applicative conduit notamment à avoir une en-tête TCP « externe » sans aucune corrélation avec l'éventuelle en-tête TCP « interne », ce qui débouche sur un fonctionnement non optimal des mécanismes de contrôle de congestion.

R2

Pour les cas d'usage évoqués précédemment, il est recommandé d'utiliser IPsec plutôt que TLS.

Note : TLS reste bien entendu tout à fait adapté pour la sécurisation d'un protocole applicatif particulier (comme c'est la cas pour HTTPS, IMAPS, LDAPS, ...) et cet emploi est complémentaire et pleinement compatible avec la mise en oeuvre d'IPsec.

2. Le mot SSL se rapporte en toute rigueur à une version ancienne et ayant pratiquement disparu du protocole TLS, protocole quant à lui très couramment employé à l'heure actuelle. Il est toutefois très fréquent de rencontrer des documents utilisant le mot SSL pour désigner TLS, au point d'éclipser cette dernière dénomination.

3. TLS n'est en principe pas destiné à sécuriser des liens entre sites distants mais plutôt à sécuriser la communication entre un utilisateur et un service. Même si la nuance est parfois ténue, il s'agit réellement d'une approche différente.

6 Fonctionnement d'IPsec

IPsec, de par ses subtilités, est souvent partiellement compris et peu maîtrisé. Les choix de configuration, y compris ceux par défaut, ne sont pas toujours judicieux et l'emploi d'IPsec peut alors offrir un niveau de sécurité plus faible que celui attendu.

6.1 Services fournis par IPsec

Les services de sécurité fournis par IPsec reposent sur deux protocoles différents qui constituent le coeur de la technologie IPsec :

- AH : « Authentication Header » (protocole n°51) dont la version la plus récente est normalisée par la RFC 4302 ;
- ESP : « Encapsulation Security Payload » (protocole n°50) dont la version la plus récente est normalisée par la RFC 4303.

Ces deux protocoles peuvent être utilisés indépendamment ou, plus rarement, de manière combinée.

6.1.1 AH : intégrité et authentification des paquets

Le protocole AH, qui est utilisé de manière moins fréquente qu'ESP, permet d'assurer l'intégrité et, employé avec IKE (voir infra), l'authentification des paquets IP. C'est à dire qu'AH permet d'une part de s'assurer que les paquets échangés n'ont pas été altérés et d'autre part de garantir l'identité de l'expéditeur d'un paquet. Il garantit aussi une protection contre le rejeu.

On notera qu'AH ne protège pas la confidentialité des données échangées. Les données ne sont pas chiffrées et transitent en clair, ou plus exactement sous le même format que si l'on utilisait un lien IP sans IPsec (un chiffrement peut être mis en œuvre plus haut dans la couche protocolaire, par exemple en utilisant TLS).

Le contrôle d'intégrité s'effectue sur l'ensemble des paquets IP y compris les en-têtes, à l'exception des en-têtes variables par nature telles que les champs DSCP, ECN, TTL, « Flags », l'offset de fragmentation et la somme de contrôle. Cela signifie en particulier que les adresses sources et destinations font partie des données protégées. Un paquet où ces données ont été modifiées est considéré comme corrompu. Cela crée une incompatibilité avec les mécanismes de traduction d'adresses, voir 6.5.

Les RFC relatives à IPsec rendent la prise en charge d'AH par les équipements mettant en oeuvre IPsec optionnelle tandis que celle d'ESP est obligatoire. De manière générale, face à ESP, AH peut être considéré comme obsolète et d'un faible apport du point de vue de la sécurité, il n'y a généralement pas lieu de le mettre en œuvre.

R3

L'emploi d'IPsec doit se faire avec le protocole ESP. Bien qu'il ne présente pas de risque de sécurité en soi, l'emploi d'AH est déconseillé.

6.1.2 ESP : confidentialité, intégrité et authentification des paquets

Le protocole ESP permet quant à lui d'assurer la confidentialité, l'intégrité et, employé avec IKE (voir infra), l'authentification des données échangées. Il garantit aussi une protection contre le rejeu. Il est possible d'utiliser uniquement les fonctions d'intégrité et d'authentification sans chiffrement (ce qui peut satisfaire la plupart des cas d'usage d'AH et justifie donc l'abandon d'AH).

Certaines implémentations permettent à l'inverse la protection en confidentialité sans mécanisme de contrôle d'intégrité : cet usage, lui-aussi obsolescent, doit être évité. La suppression du service d'intégrité ne présente aucun avantage (le coût en performance des opérations de contrôle d'intégrité

est en général négligeable devant celui du chiffrement) et expose l'utilisateur a un certain nombre d'attaques connues et réalistes.

R4

Le service de confidentialité d'ESP ne doit jamais être employé sans activer le mécanisme de contrôle d'intégrité.

Contrairement à l'approche retenue dans le cadre d'AH, les données protégées sont ici uniquement le « payload », c'est à dire le contenu du paquet IP et non ses en-têtes. Il n'y a donc pas d'incompatibilité fondamentale avec les mécanismes de traduction d'adresses. Il est toutefois nécessaire de prendre un certain nombre de mesures pour assurer l'interopérabilité entre ESP et la traduction d'adresse, voir 6.5.

6.2 Modes transport et tunnel

Indépendamment du choix entre AH et ESP, il est possible d'utiliser IPsec dans deux modes distincts : le mode tunnel et le mode transport. Le mode tunnel rend le service attendu dans la majorité des cas.

Dans le mode transport, les données associées à AH ou à ESP viennent se greffer sur le paquet IP initial (c'est à dire celui qu'on aurait envoyé en l'absence d'IPsec). Le paquet IP résultant contient un paquet AH ou ESP qui contient lui-même le contenu du paquet initial (un segment TCP par exemple). On peut remarquer que l'en tête IP initiale doit être modifiée : son champ protocole doit indiquer 50 ou 51 pour ESP ou AH en lieux et place par exemple de 6 (TCP) ou 17 (UDP). C'est l'en tête (AH ou ESP) qui indiquera le protocole encapsulé qui était auparavant indiqué dans l'en-tête IP.

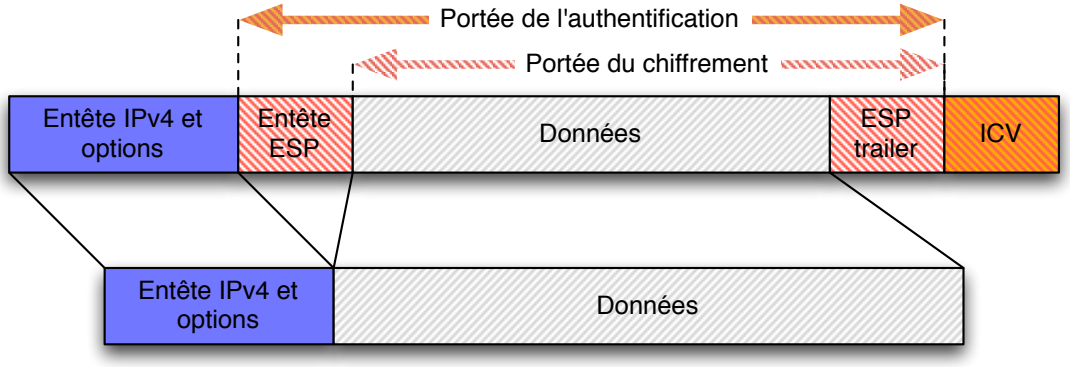

FIGURE 6 – Utilisation d'ESP en mode transport. ICV désigne l'« Integrity Check Value », valeur utilisée par le mécanisme de contrôle d'intégrité

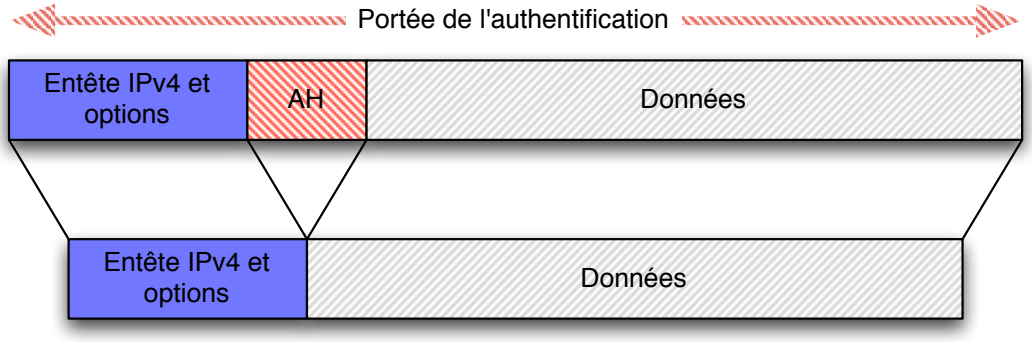

FIGURE 7 – Utilisation d'AH en mode transport

Dans le mode tunnel en revanche, un nouveau paquet IP est généré pour contenir un paquet AH ou ESP qui contient lui-même le paquet IP initial sans modification. Dans ce mode, il y a donc en définitive deux en-têtes IP. L'en-tête externe sera effectivement utilisé pour le routage dès l'émission du paquet. L'en-tête interne, qui peut être chiffrée dans le cas où l'on utilise ESP avec le service de confidentialité, ne sera traitée que par le destinataire (du paquet externe). Elle sera ignorée par les équipements réseau situés entre l'émetteur et le destinataire. On réalise ainsi un « tunnel » à travers ce réseau, de la même façon qu'on peut le faire avec des protocoles tels que IPIP (RFC 2003) ou GRE (RFC 2784).

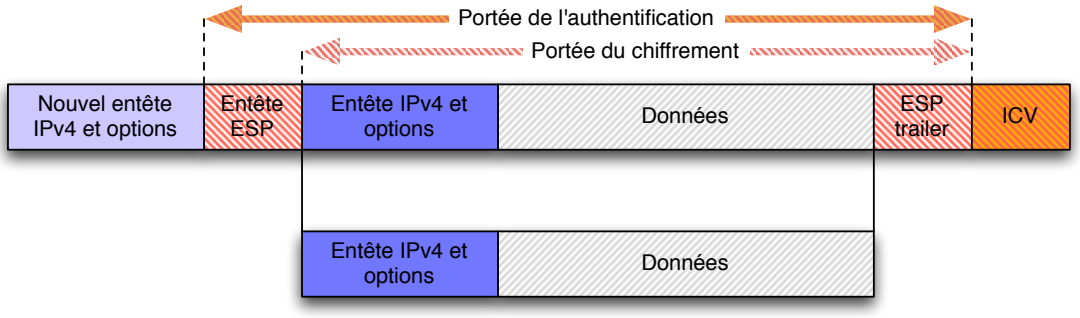

FIGURE 8 – Utilisation d'ESP en mode tunnel. ICV désigne l'« Integrity Check Value », valeur utilisée par le mécanisme de contrôle d'intégrité

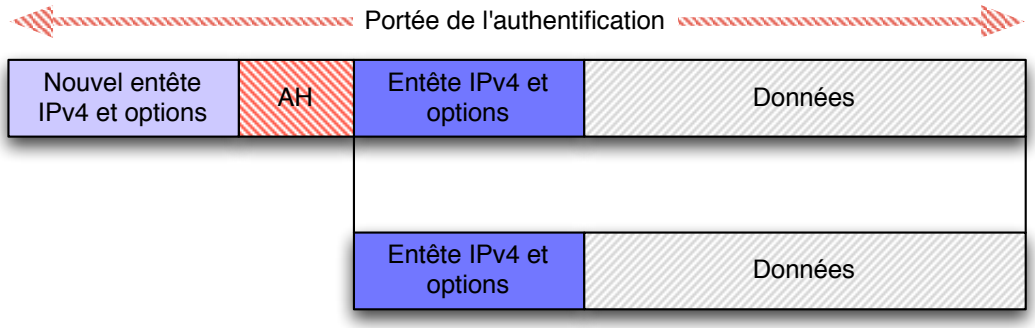

FIGURE 9 – Utilisation d'AH en mode tunnel

Le mode tunnel se prête bien à un scénario d'accès distant à un réseau privé au travers d'un réseau public. Il permet de masquer sur les tronçons publics l'adressage interne du réseau privé, fréquemment non routable sur le réseau public. IPsec est utilisé sur le réseau public entre le client et une passerelle qui extrait le paquet IP interne et l'injecte dans le réseau privé (et réciproquement pour le sens de communication inverse).

Naturellement, du fait de la duplication de l'en tête IP, l'utilisation du mode tunnel résulte en des paquets plus gros qu'en mode transport pour une même quantité de données utiles. La consommation en ressources réseau est donc plus importante. En particulier, il faudra prendre garde au fait que le MTU effectif du tunnel est le MTU du lien diminué de la taille des méta-informations ajoutées par IPsec (nouvelle en-tête IP, en-tête et trailer ESP, somme de contrôle). La taille de ces méta-données varie notamment en fonction des paramètres cryptographiques, mais il est courant que le « surcoût » en taille dû au tunnel soit de 50 à 100 octets. Dans certains cas, les mécanismes de configuration automatique du MTU gèrent mal cette situation. Il est par conséquent relativement fréquent, lors de l'utilisation d'IPsec, de devoir limiter manuellement la taille maximale des paquets IP clairs pour s'assurer qu'une fois ceux-ci encapsulés ils n'atteignent pas une taille qui nécessite de les fragmenter.

Un élément qui peut s'avérer important est le fait qu'en mode tunnel, le contrôle d'intégrité offert par le mode AH porte non seulement sur le paquet interne mais aussi sur l'en-tête IP externe, de la même façon qu'en mode transport. Cela peut avoir des effets indésirables en cas de NAT, voir 6.5. Le contrôle d'intégrité d'ESP ne porte quant à lui que sur le paquet interne et permet donc à l'en-tête externe d'évoluer.

6.3 Security Policy

Le terme « Security Policy » désigne, dans le contexte IPsec, le choix pour un lien unidirectionnel [4] donné :

- de l'utilisation obligatoire ou facultative ou de la non-utilisation d'IPsec ;
- de l'utilisation du mode tunnel ou transport ;
- de l'utilisation d'AH ou d'ESP.

L'ensemble des SP est regroupé dans une SPD : « Security Policy Database ».

À l'image des règles de flux d'un pare-feu, les SP ont pour but de spécifier les flux que l'on veut autoriser et ceux que l'on veut interdire.

R5

Les SP permettant un usage « facultatif » ou « optionnel » d'IPsec doivent être évitées car elles ne garantissent pas la sécurité (possibilité de « downgrade attack »). Pour un lien donné, on s'en tiendra donc à n'autoriser que les flux sécurisés dès lors qu'il existe un besoin de sécurité.

R6

Malgré la possibilité technique de fonctionnement asymétrique, on préfèrera lorsque c'est possible avoir une politique uniforme entre le lien aller et le lien retour.

6.4 Etablissement d'un lien IPsec

Les mécanismes cryptographiques utilisés pour la protection en intégrité ou en confidentialité sont paramétrés par une ou plusieurs clés. Ces éléments doivent être partagés par les différents hôtes

4. On distingue en effet le lien $A \to B$ et le lien $B \to A$ qui peuvent avoir deux politiques différentes.

employant IPsec. Deux approches sont possibles : mettre en place manuellement des clés sur chaque hôte ou utiliser le mécanisme d'échange de clés IKE pour que les hôtes puissent négocier ces clés.

6.4.1 Security Association

Pour chaque lien unidirectionnel (comme ci-dessus), on désigne par « Security Association » (SA) les données de contexte telles que :

- les hôtes source et destination ;
- le mode (transport/tunnel) et les protocoles (AH/ESP) employés ;
- les algorithmes cryptographiques employés ;
- les clés associées à ces algorithmes.

Chaque SA est associée à une période de validité et à un nombre entier la désignant de manière univoque et appelé SPI (Security Parameter Index). Les en-têtes AH et ESP indiquent systématiquement le SPI associé à la SA utilisée.

Les premiers éléments (hôtes aux extrémités, mode, protocole) sont conditionnés par les SP en vigueur : un système ne doit pas avoir de SA qui violent ses SP.

Les paramètres cryptographiques (algorithmes, taille de clés) peuvent être fixés manuellement ou négociés par le protocole IKE (voir plus bas). Les options possibles sont configurées par l'administrateur.

On définit, comme pour la SPD, la SAD comme étant la « Security Association Database » (base des SA).

R7

Il est préférable de fixer a priori les algorithmes et tailles de clés employés (voir infra pour le choix) et de n'utiliser IKE que pour l'échange de clés. À défaut de pouvoir les fixer, on ne permettra la négociation que sur un nombre réduit d'algorithmes.

Note : Dans ce dernier cas, la sécurité du lien est conditionnée par l'algorithme le plus faible parmi ceux acceptés ; il est donc nécessaire que toutes les options soient conformes à la politique de sécurité de l'organisme.

6.4.2 Mise à la clé manuelle

Les algorithmes et les clés peuvent être paramétrés manuellement sur chaque équipement. On parle généralement du « Manual Keying » ; il est important de ne pas confondre cette méthode avec l'authentification « Pre-Shared Key » d'IKE abordée au chapitre suivant.

La mise à la clé manuelle est fortement déconseillée. Elle exige en effet une configuration fastidieuse, la clé étant idéalement différente pour chaque couple d'hôtes. Par ailleurs, il est difficile en pratique de renouveler les clés à une fréquence suffisante pour être conforme tant aux bonnes pratiques cryptographiques (usure de la clé) que de SSI (cryptopériode) [5]. En outre, elle ne permet pas de bénéficier de la propriété de « Perfect Forward Secrecy » présentée en 6.6. Enfin, elle ne permet pas de mettre en oeuvre des mécanismes d'authentification cryptographiques.

En définitive, la mise à la clé manuelle doit être réservée à des procédures de tests ou de diagnostics ou à des système très particuliers ayant fait l'objet d'une étude de sécurité approfondie, notamment pour s'assurer que le cycle de vie des clés est bien géré et qu'il y a bien une clé différente pour chaque usage.

5. On distingue en effet l'usure de la clé, qui décrit une propriété mathématique selon laquelle le système cryptographique est fragilisé au delà d'une certaine quantité d'information chiffrée, de la cryptopériode, durée maximale d'usage de la clé basée sur des considérations organisationnelles ayant pour but de borner l'impact d'une compromission.

6.4.3 Utilisation d'IKE

La négociation dynamique des algorithmes et clés d'une SA peuvent se faire grâce au protocole IKE, actuellement en version 2 (RFC 5996).

R8

Il est recommandé d'utiliser la version 2 d'IKE.

6.4.3.1 Un protocole en deux phases

Le protocole IKE se décompose en deux phases distinctes. Dans une première phase, un canal sécurisé (chiffré et authentifié) est créé entre les deux participants. Dans une deuxième phase, ce canal est utilisé pour négocier les divers paramètres de la SA.

La première phase utilise bien entendu elle aussi des algorithmes cryptographiques, qui ne sont pas nécessairement les mêmes que ceux définis finalement dans la SA. Les paramètres du canal sécurisé négocié lors de la première phase et utilisé pour protéger la seconde phase sont parfois désignés sous le terme ISAKMP [6] SA ou encore IKE SA, par opposition aux IPSEC SA qui sont les SA négociées lors de la seconde phase et utilisées pour protéger le trafic « utile ».

La première version d'IKE permettait deux modes différents pour la phase 1, le mode principal (« main mode ») et le mode agressif (« aggressive mode »). Le deuxième a la caractéristique de nécessiter moins de messages que le premier mais de ne pas cacher l'identité des participants à un éventuel attaquant en écoute passive sur le réseau. La phase 2 utilisait quant à elle le mode rapide (« quick mode »). IKE version 2 a une première phase similaire au mode principal mais n'emploie plus cette terminologie. On trouve toutefois encore des produits désignant par « mode principal » la première phase et « mode rapide » la deuxième.

6.4.3.2 Authentification des correspondants

L'authentification des participants à la première phase peut se faire soit au moyen d'un secret partagé (PSK : « Pre-Shared Key ») soit par utilisation d'un mécanisme de cryptographie asymétrique tel que RSA. Dans ce cas, il est possible d'utiliser une Infrastructure de Gestion de Clés (IGC ou PKI) pour certifier les clés publiques des participants et ainsi ne pas devoir pré-positionner toutes les clés publiques sur l'ensemble des hôtes.

On privilégie généralement l'utilisation d'une IGC, ce qui permet de simplifier l'exploitation du système : l'ajout d'un nouvel hôte ou la révocation d'une clé compromise est aisée (il n'est pas nécessaire d'intervenir sur tous les équipements déjà en place). Il peut être délicat dans les autres modes de réagir avec la diligence nécessaire à une compromission de clé, par exemple le vol d'un équipement.

Le mode PSK doit en principe être évité pour des systèmes en production et être cantonné à des systèmes de tests ou à des opérations de diagnostic. S'il était nécessaire d'y recourir exceptionnellement, une bonne pratique générale pour les secrets partagés est de prendre garde à ce que l'entropie soit suffisante pour rendre difficile une attaque par recherche exhaustive. On se reportera à se sujet au référentiel général de sécurité publié par l'ANSSI. Une entropie inférieure à 100 bits est considérée à la date de rédaction de ce document comme un choix risqué.

6. ISAKMP est un « protocole cadre » (framework) au sein duquel le protocole IKE a été défini.

R9

Il est fortement déconseillé dans le cas général d'utiliser la mise à clé manuelle ou une clé pré-partagée (PSK) pour l'établissement d'un lien IPsec. Des mécanismes basés sur de la cryptographie asymétrique sont à privilégier. On privilégiera en particulier les mécanismes d'IGC qui permettent la révocation rapide des clés compromises, en particulier en cas de perte d'un poste. Les dérogations à ces recommandations doivent avoir fait l'objet d'une étude de sécurité rigoureuse.

6.4.3.3 Négociation des SP

IKE permet aussi de négocier les SP. Dans la plupart des cas, tous les paramètres des SP sont connus à l'avance et cette négociation ne présente que peu d'intérêt. Ce mécanisme prend toutefois tout son sens pour les situations de mobilité. Dans ce cas, en effet, l'adresse IP du client nomade n'est pas connue a priori : elle est attribuée par le réseau accueillant le poste nomade. Il est alors très utile de pouvoir adapter ce paramètre de la SP à la volée au moyen de la négociation IKE.

Dans les cas où un tel mécanisme de négociation n'est pas nécessaire, il est préférable d'employer une configuration statique (si les équipements le permettent) de manière à garder la maîtrise de la politique de sécurité. Dans le cas où une négociation des politiques de sécurité par IKE est utilisée, il est nécessaire de s'assurer par la politique de filtrage que le système ne se trouve jamais dans un état où il échange des données en clair. Concrètement, cela signifie interdire par des règles de filtrage réseau tout trafic qui n'utilise pas le protocole IKE, ESP et (le cas échéant) les protocoles qui seraient nécessaires au fonctionnement du réseau, tel qu'ICMP.

R10

On privilégiera la configuration statique des SP lorsque le cadre d'emploi le permet. À défaut, il est nécessaire de s'assurer que la politique de filtrage mise en œuvre garantit l'absence de flux en clair.

6.5 Utilisation d'IPsec avec un système de traduction d'adresses (NAT)

L'utilisation d'un système de traduction d'adresses (NAT) en conjonction avec IPsec peut poser plusieurs problèmes.

Tout d'abord, l'utilisation d'AH n'est pas possible, dans la mesure où le contrôle d'intégrité des en-têtes IP devient invalide dès lors que les adresses IP sources ou destinations sont modifiées.

Par ailleurs, certains mécanismes de NAT très courants nécessitent de pouvoir modifier les ports TCP ou UDP. Si le protocole transporté par IP est ESP, qui ne présente pas de port, un tel mécanisme ne peut fonctionner. La solution est l'emploi du « NAT-Traversal » (NAT-T) qui consistent à encapsuler le trafic IKE puis ESP dans des datagrammes UDP utilisant de manière standard le port 4500.

Enfin, il faut prendre garde à certaines extensions hors standard qui peuvent être incompatibles avec l'utilisation de NAT ou nécessiter l'utilisation de NAT-T même dans des cas où la modification de ports n'est pas nécessaire.

R11

S'il est nécessaire de recourir au NAT sur des flux IPsec, il est nécessaire d'activer le mécanisme de NAT-Traversal.

6.6 PFS : Perfect forward Secrecy

La propriété de PFS (Perfect forward Secrecy) est la caractéristique de certains protocoles cryptographiques qui garantit qu'un attaquant ayant enregistré des échanges chiffrés à un instant donné et parvenant à obtenir les secrets cryptographiques à une date ultérieure ne puisse pas pour autant déchiffrer les enregistrements effectués.

La PFS permet donc de mettre en place des fenêtres temporelles « étanches », en ce sens que l'impact d'une éventuelle attaque ne pourra pas (sous certaines hypothèses) s'étendre aux fenêtres déjà refermées. Il s'agit d'une mesure de « mitigation » du risque.

Cette propriété est obtenue (pour le cas d'IPsec) en employant un mécanisme d'échange de clé « Diffie-Hellman éphémère » ou sa variante sur courbe elliptique.

Le degré de granularité de cette protection (la fenêtre) est la session, délimitée par des échanges de clés IKE. Ainsi, à chaque échange de clés on acquiert la garantie que les échanges antérieurs à cet échange sont définitivement protégés même en cas de compromission ultérieure du secret. C'est, entre autre, pour cette raison qu'il est nécessaire de définir une plage d'utilisation des clés à la fois en temps et en volume de données.

Cette propriété n'est vérifiée que dans le cas de l'utilisation d'IKE ; elle ne l'est pas lors d'une mise à la clé manuelle. Il est possible avec certains équipements d'améliorer la granularité de cette propriété en utilisant un second échange de clé en phase 2 (plutôt que de dériver toutes les clés de celle négociée en phase 1), échange qui sera renouvelé plusieurs fois au cours de la durée de vie d'une SA. Cela a en pratique pour effet de raccourcir la « session » évoquée ci-dessus, en la renouvelant plus fréquemment. Il est généralement possible d'associer un critère temporel et un critère de quantité de données échangée : le premier quota atteint provoque un renouvellement de clés.

R12

Dès lors que cette possibilité est offerte par les équipements employés, il est recommandé de mettre en œuvre la propriété PFS en phase 2 en utilisant dans le « quick mode » l'échange de clé Diffie-Hellman éphémère classique ou sa variante sur courbes elliptiques.

R13

Dès lors que cette possibilité est offerte par les équipements employés, il est recommandé de forcer le renouvellement périodique des clés, par exemple toutes les heures et tous les 100 Go de données, afin de limiter l'impact de la compromission d'une clé sur le trafic des données.

Note : La définition exacte de la période de renouvellement (cryptopériode) relève d'un choix organisationnel et de l'analyse de risque propre à un déploiement.

6.7 Choix des paramètres

Le choix des algorithmes cryptographiques et le dimensionnement des clés est traité dans le référentiel général de sécurité (annexe B1 « Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques » disponible sur www.ssi.gouv.fr/rgs), seul document faisant foi.

R14

Il est fortement déconseillé d'employer la fonction de hachage MD5, le chiffrement DES, des clés RSA de taille inférieure à 2048 bits ou des clés ECDSA de taille inférieure à 200 bits.

R15

Il est déconseillé d'utiliser 3DES, SHA-1 ou ECDSA avec des clés de moins de 256 bits si des alternatives plus sécurisées telles qu'AES (AES-128 ou AES-256), SHA-2 (SHA-224, SHA-256, SHA-384 ou SHA-512) ou ECDSA avec des clés d'au moins 256 bits sont disponibles.

R16

On prendra garde au groupe de Diffie-Hellman employé. Les groupes 1 ou 2, très fréquemment proposés dans les configurations par défaut, ne sont plus d'une taille acceptable. On privilégiera les groupes ayant des modules de taille plus importante (comme les groupes 14 et 15) voire (si possible) les groupes construits sur des courbes elliptiques d'au moins 256 bits (comme la courbe `ecp256`, aussi nommée groupe 19 ou encore la courbe `ecp384bp`, normalisée sous l'appellation groupe 29).