Master – IPSEC

Présentation

IPSEC est un ensemble de protocoles utilisant des algorithmes permettant le transport de données sécurisées sur un réseau IP.

Pour protéger les communications, deux modes d'utilisation existent :

- Le mode **transport** qui permet de protéger la charge utile du paquet et certains champs de l'en-tête
- Le mode **tunnel** qui protège tous les champs du paquet IP arrivant à l'entrée d'un tunnel et sur certains champs du nouveau paquet IP qui encapsule le paquet IP entrant.

Le mode transport est utilisable entre des équipements d'un réseau local alors que le mode tunnel peut être utilisé au travers d'Internet grâce à l'encapsulation des paquets.

Association de sécurité

Pour que 2 équipements communiquent, le protocole doit effectuer une association de sécurité avec le type d'extension et les paramètres de sécurité (algorithmes et clés de chiffrement…) à mettre en place sur la communication. Cette association doit être connue des entités chargées de la protection de la communication.

Une association est identifiée de façon unique par un triplet comprenant un indice de paramètres de sécurité SPI/SAID (*Security Parameters Index* / *Security Association IDentifier*), l'adresse du destinataire et le protocole de sécurité choisi (AH ou ESP).

Un équipement peut participer à plusieurs associations, soit pour plusieurs communications ou sur une même communication utilisant AH et ESP.

L'équipement gérera de toute façon deux associations de sécurité distinctes. Ce fonctionnement est unidirectionnel, pour des communications bidirectionnelles, il y aura également nécessité d'utiliser deux associations.

Le choix de l'association de sécurité au niveau de la station émettrice ou d'une passerelle de sécurité peut dépendre de différents sélecteurs, mais la majorité des équipements IPsec considère que les sélecteurs sont les adresses IP de destination, les numéros de protocole et numéros de port.

Mode tunnel ou mode transport

Bases de données

L'IETF conseille aux constructeurs de définir deux bases de données pour construire l'association de sécurité à appliquer ou extraire les extensions de sécurité.

Le **SPD** (Security Policy Database) qui contrôle le trafic avec 3 options :

- Le trafic est interdit, on supprime le paquet (discard)
- Le trafic est autorisé mais sans chiffrement (bypass IPsec)
- Le trafic est autorisé et chiffré (apply IPsec) auquel cas le SPD spécifie l'association de sécurité à appliquer située dans la base de données SAD.

Le **SAD** (Security Association Database) contient l'ensemble des associations de sécurité et précise les services et mécanismes de sécurité à appliquer.

Extension d'authentification AH

Cette extension (RFC 2402), permet de s'assurer que l'émetteur du message est bien celui qu'il prétend être. Elle permet également le contrôle d'intégrité pour garantir que personne n'a modifié le contenu d'un message lors de son transfert sur le réseau.

L'extension AH en mode transport permet d'assurer l'intégrité du paquet pour les champs en-tête du paquet et extensions (proche-en-proche, routage, fragmentation).

L'extension AH est composée des champs suivants :

- Le champ **longueur de l'extension**
  indique la longueur du champ authentificateur exprimée en nombre de mots de 32 bits.
- Le champ **réservé**
  valeur 0 actuellement, réservé pour une utilisation future.
- Le champ **indice des paramètres de sécurité (SPI)**
  identifie l'association de sécurité utilisée pour construire cette extension.
- Le **numéro de séquence**
  sur 32 bits permet de détecter les rejeux.
- Le champ **authentificateur**
  garantit l'intégrité du paquet ; il est calculé grâce à l'algorithme et à la clé correspondant à l'association de sécurité (SPI + adresse(s) de destination + AH).

> L'extension AH n'offre pas le service de confidentialité. Elle ne permet pas de chiffrer les données transportées dans le paquet et ne protège donc pas ces données contre d'éventuelles écoutes effectuées sur le réseau.

L'IETF impose que pour les communications point à point, les équipements de sécurité possèdent un MAC (*Message Authentication Code*) basé sur des algorithmes symétriques (AES, 3DES) et des fonctions de hachage (SHA-1, MD5).

On parle alors des algorithmes HMAC-MD5 et HMAC-SHA-1.

Extension de confidentialité ESP

ESP (*Encapsulating Security Payload* – RFC 2406) permet de chiffrer l'ensemble des paquets et de garantir leur l'authentification et leur intégrité.

Le principe consiste à chiffrer les données à protéger, de calculer un authentificateur et d'encapsuler ces informations dans l'en-tête de confidentialité.

Deux modes de protection

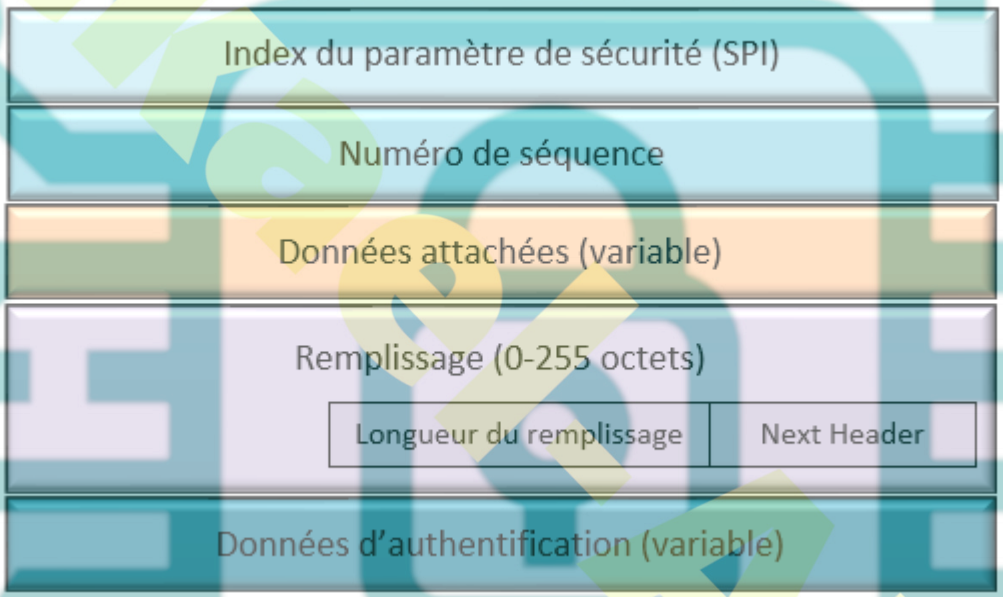
En mode transport, on protège les données de types TCP, UDP, ICMP.

- Le chiffrement porte sur les données et sur la queue ESP.

- La protection en intégrité/authentification porte sur toute l'extension ESP.
- L'extension ESP est insérée dans le paquet IP après l'en-tête IP.

En mode tunnel, on protège tout le paquet IP original en le chiffrant avant de l'encapsuler dans l'extension ESP. L'extension est ensuite placée dans le nouveau paquet IP dont les en-têtes IP sont en clair pour permettre au réseau IP de les faire circuler correctement. L'intégrité et l'authentification s'emploie sur l'extension ESP (comprenant le paquet IP original).

L'extension ESP est composée des champs suivants



- Le champ **indice de paramètres** de sécurité (SPI) + l'adresse du (des) destinataire(s), identifie l'association de sécurité utilisée pour construire cette extension.
- Le **numéro de séquence** permet de détecter les rejeux de paquet IP.
- Le champ **données attachées** peut contenir 1) un paquet IP complet (en-tête IP + extensions + données de niveau transport), 2) l'extension destination suivie de données de niveau transport, 3) des données de niveau transport.
- Le champ **remplissage** permet d'obtenir une taille de bloc compatible avec le chiffrement
- Le champ **longueur de remplissage** indique la longueur en octets du champ remplissage.
- Le champ **en-tête suivant** identifie le protocole utilisé pour le transfert.
- Le champ **authentificateur** (optionnel) est calculé à l'aide de l'algorithme et de la clé correspondant à l'association de sécurité.

Le RFC 2406 précise les algorithmes de chiffrement à proposer dans les équipements IPsec.

CHIFFREMENT

- DES dans le mode d'utilisation CBC (*Cipher Block Chaining*),
- 3DES
- AES (*Advanced Encryption Stantard*).

AUTHENTIFICATION

- HMAC- MD5
- HMAC-SHA-1

> IPsec en mode ESP ou AH pose des problèmes de compatibilité avec la translation d'adresses car le champ de contrôle est calculé en partie avec les adresses IP et toute modification d'une adresse suppose la modification de ce contrôle.

La solution proposée, consiste à n'utiliser que le protocole ESP en établissant un tunnel UDP entre les deux équipements IPsec. Grâce à cette astuce, les données encapsulées dans ce tunnel sont protégées par le protocole ESP et c'est uniquement le champ de contrôle de UDP qui est modifié et non l'en-tête ESP.

De plus, la translation de port est faite sur les numéros de port UDP accessibles car non chiffrés. Ce système est connu sous le nom de NAT-traversal (RFC 3947) (RFC 3948).

Gestion des clés – IKE

Les extensions AH et ESP utilisent les clés de chiffrement que l'on peut générer manuellement sur les équipements réseau ou automatiquement via le protocole ISAKMP (Internet Security Association and Key Management Protocol – RFC 2408)

> Dans le cadre de la standardisation IPsec, ISAKMP est associé à deux protocoles d'échanges de clés (SKEME et Oakley) pour construire le

protocole IKE (Internet Key Exchange – RFC 2409).

Le protocole IKE utilise les éléments suivants :

- Un protocole de gestion des associations de sécurité comme ISAKMP qui définit des formats de paquets permettant de créer, modifier et détruire des associations de sécurité (SA). Il assure également l'authentification entre les entités communicantes.
- Un protocole d'échange de clés de session basé sur SKEME et Oakley qui s'appuie sur une procédure Diffie-Hellman.
- Un domaine d'interprétation ou DOI (Domain of Interpretation – RFC 2407) qui définit les règles de négociation (échanges de clés, associations de sécurité…)

> Ces clés peuvent être des clés partagées ou des clés privées/publiques auto-signées ou issues d'une infrastructure PKI (Public Key Infrastructure).

Architecture

Du fait qu'ISAKMP fonctionne au-dessus d'IP (UDP port 500), les informations d'associations de sécurité et des clés sont transportées dans des paquets ISAKMP indépendamment du protocole l'utilisant.

Ainsi, il peut être utilisé avec n'importe quel protocole de sécurité comme IPsec, TLS/SSL.

ISAKMP utilise des paramètres lors des échanges

- Paramètres de sécurité à négocier (**SA** pour Security Association, **P** pour Proposal, **T** pour Transform, **D** pour Delete)
- Clés de session (**KE** pour Key Exchange)
- Identités des entités (**ID**), certificats (**CERT, CERTREQ**),
- Authentification (**HASH**, **SIG**(signature), **NONCE** qui contient un nombre aléatoire)
- Messages d'erreurs (**N** pour notification)
- Constructeur d'équipement/logiciel de sécurité (**Vendor ID**).

Echanges ISAKMP/IKEv1

ISAKMP comporte deux phases qui permettent une séparation nette de la négociation des associations de sécurité pour IPsec et de la protection du trafic propre à ISAKMP.

PHASE 1

Cette phase est utilisée pour générer une première clé qui va servir par la suite à la création de 3 autres clés. Cette clé peut être créée selon 3 modes offerts par IKE (secret partagé – Diffie-Hellman, chiffrement asymétrique, signature)
L'une des clés sera utilisée pour l'authentification, l'autre pour le chiffrement et la dernière sera utilisé lors de la phase 2 du protocole.

Ce canal, sécurisé, est ensuite utilisé pour la deuxième phase IKE.

PHASE 2

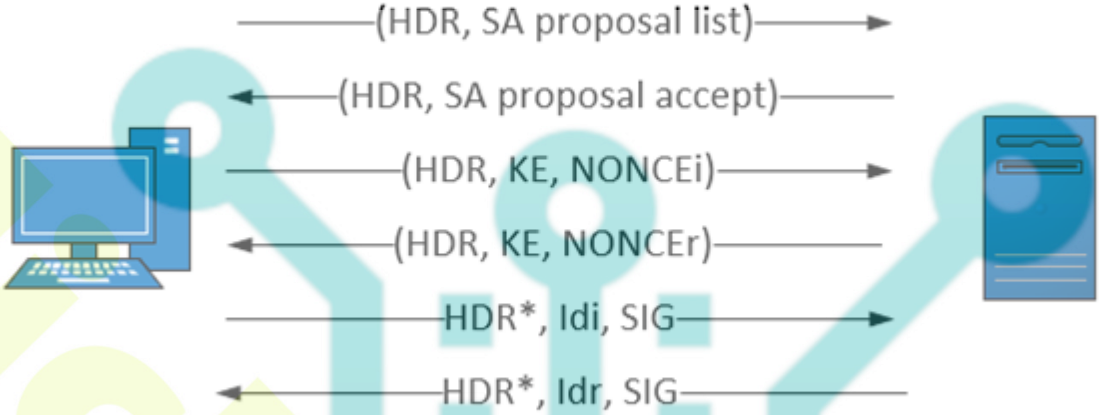
L'objectif de la deuxième phase est de créer les tunnels IPSec (SA), un pour chaque sens de communication, pour les échanges effectifs entre les hôtes. C'est lors de cette phase que chaque hôte donne ses préférences en matière d'algorithme.

IKE comprend quatre modes :

- Le mode principal (Main Mode) phase 1,
- Le mode agressif (Aggressive Mode) phase 1,
- Le mode rapide (Quick Mode) phase 2
- Le mode nouveau groupe (New Group Mode) n'est ni un échange de la phase 1, ni un échange de la phase 2, il ne s'éxécute qu'après l'établissement d'une SA ISAKMP. Il sert à convenir d'un nouveau groupe pour de futurs échanges Diffie-Hellman.

Phase 1 de IKEv1

Main Mode se compose de six messages



- Les deux premiers messages servent à négocier l'association de sécurité ISAKMP (algorithme de chiffrement, fonction de hachage, méthode d'authentification pour Diffie- Hellman.
  Les blocs ISAKMP transportés sont de type *Security Association*, *Proposal* et *Transform*.
  L'initiateur propose plusieurs combinaisons d'algorithmes, mécanismes, et méthodes, et le responder IKE en choisit un.
  Pour s'authentifier, les équipements IPsec utilisent soit un secret partagé, soit des clés publique/privée, soit un certificat.

- Les deux suivants permettent l'établissement d'un secret partagé via un échange Diffie-Hellman.
  Le secret partagé sert à dériver des clés de session, deux d'entre elles étant utilisées pour protéger la suite des échanges avec les algorithmes de chiffrement et de hachage négociés précédemment. **Les blocs ISAKMP sont de type *Key Exchange*, *Nonce* et *Certificate Request*.**

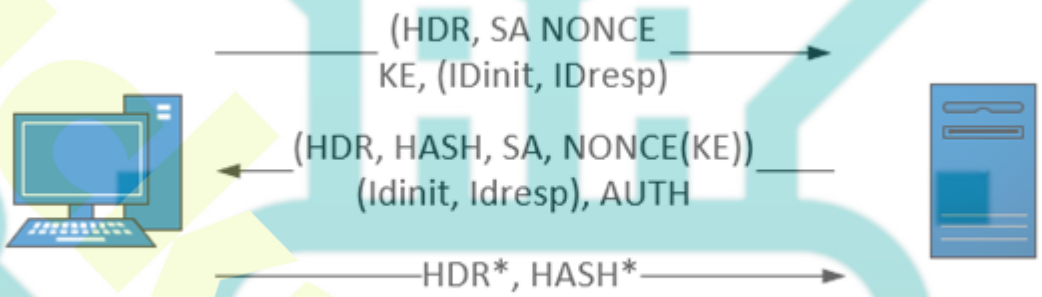
- Les deux derniers messages permettent aux tiers d'échanger leurs identités et servent à l'authentification de l'ensemble des données échangées. **Les blocs ISAKMP sont de type ID, SIG et optionnellement CERT.**

Main Mode fournit la propriété de *Perfect Forward Secrecy* (grâce à Diffie-Hellman) et assure l'anonymat des entités en présence (grâce au chiffrement des deux derniers messages).

Aggressive Mode est plus rapide car il combine les échanges du Main Mode de façon à ramener le nombre de messages à trois.

Phase 2 de IKEv1

Une fois que l'association de sécurité ISAKMP est mise en place grâce à des échanges de phase 1, Quick Mode est utilisé pour négocier des associations de sécurité IPsec. Chaque négociation aboutit à deux SA symétriques, une dans chaque sens de la communication.



On négocie tout d'abord un ensemble de paramètres IPsec, puis on échange des nombres aléatoires, utilisés pour générer une nouvelle clé dérivée de celle du SA ISAKMP.

En option, il existe la possibilité d'identifier le trafic au moyen de blocs optionnels **IDi** et **IDr**. Si l'option n'est pas active, ce sont les adresses IP de l'initiator et du responder qui sont utilisées.

> Une phase 1 peut être exécutée une fois par jour, tandis qu'une phase 2 est exécutée une fois toutes les x minutes.

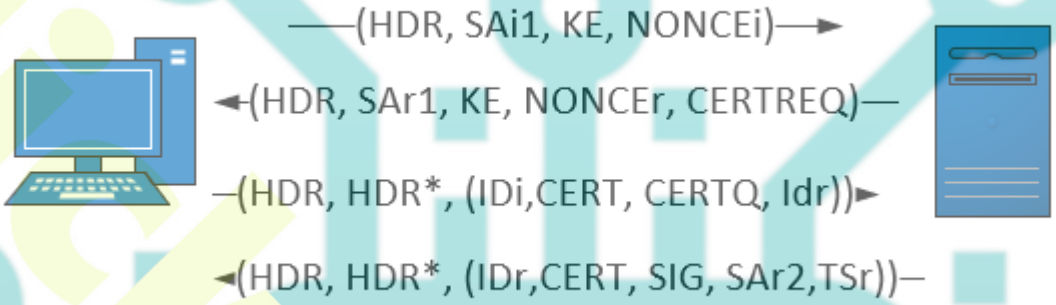
Interactions entre IKE et IPsec

Avant d'envoyer des données, la couche IPsec consulte ses bases de données SPD et SAD pour savoir comment traiter ces données et si l'association de sécurité existe déjà. Dans le cas où l'association de sécurité existe, on l'utilise pour traiter le trafic en question. Dans le cas, on refait appel à IKE pour établir une nouvelle association de sécurité.

IKE Version 2

IKEv2 a pour objectif de simplifier la version 1 en enlevant les conditions inutiles d'ISAKMP et IKEv1 et d'incorporer de nouvelles fonctionnalités dans le protocole IPsec.

La négociation des phases 1 et 2 est découpée en quatre messages ce qui rend la version 1 et 2 incompatible.



Les deux premiers messages de IKEv2 sont équivalents aux quatre premiers messages de IKEv1 en Main Mode. Les SA ISAKMP unidirectionnels apparaissent sous la notation SAi1 et SAr1.

Les deux derniers messages sont équivalents aux deux derniers messages de phase 1 en Main Mode et aux deux messages de phase 2 en Quick Mode.

Ils permettent notamment aux équipements IPsec

- d'échanger leurs identifiants respectifs,
- de s'authentifier grâce au bloc **AUTH**,
- de négocier des associations de sécurité IPsec unidirectionnelles (**SAi2** et **SAr2**) qui sont (appelées CHILD_SA)
- d'identifier le trafic protégé par ces **SA** en précisant les sélecteurs choisis dans les blocs **TSi** et **TSr** (TS pour Traffic Selector).