Informatique

Réseaux

Sécurité : IPSEC

Bureau S3-354
Mailto:Jean.Saquet@unicaen.fr
http://saquet.users.greyc.fr/M2

IPSEC - Introduction

Pour assurer la sécurité des données :

- Les mécanismes de niveau physiques (switches, Vlans, ou ceux utilisés pour le Wi-Fi) sont utiles mais insuffisants
- Résoudre le problème au niveau application oblige à incorporer ces mécanismes dans chaque application (protocoles ssh, https, pops, ...etc).

Une bonne solution serait donc d'agir au niveau réseau-transport. C'est ce que propose IPSEC, ensemble de spécifications introduites avec IPv6 mais adaptées à IPv4.

Sécurité : fonctions(1)

Confidentialité des données :

C'est le principal souci. Il s'agit de rendre incompréhensibles les données émises dans le réseau pour ceux qui ne possèdent pas la clef de déchiffrement.

Confidentialité du flux de données :

Ne pas fournir non plus assez d'infos sur la quantité, la fréquence des données émises pour permettre une analyse et en déduire des informations.

Sécurité : fonctions(2)

Authentification des données :

Garantir que les données reçues ont bien été émises par l'interlocuteur qui se déclare.

Authentification mutuelle

Dans une communication, les partenaires doivent être sûrs de s'adresser au bon interlocuteur (par exemple client au bon serveur).

Intégrité des données

Garantir que les données n'ont pas subi d'altération entre leur émission et leur réception

Sécurité : fonctions(3)

Prévention contre le rejeu :

Garantir qu'un intrus qui aurait enregistré un dialogue ne puisse pas utiliser son enregistrement pour répéter ce dialogue comme s'il émanait de l'interlocuteur d'origine.

Non répudiation :

Fournir une preuve du fait qu'un échange de données a bien eu lieu.

==>Mécanismes de cryptographie, échanges de clefs.

Échange de clefs

Le problème est d'assurer un échange de clefs entre deux partenaires ne se connaissant pas a priori.
Protocole Diffie-Hellman (1976) :
Chaque entité a un couple (clef publique, clef privée).
Avec la clef publique de l'interlocuteur et de sa clef privée, chacun calcule un secret (également calculé par l'interlocuteur).
On obtient ainsi un secret partagé. Il ne peut pas être calculé par un tiers car il utilise une clef privée.

Utilisation de Diffie-Hellman

Le secret partagé calculé au moyen de Diffie-Hellman est ensuite utilisé pour dériver des clefs de session.

Diffie-Hellman est toutefois vulnérable à l'attaque de l'intercepteur (man-in-the-middle) : interception des clefs publiques et remplacement par la sienne. Le résultat est que les entités partagent chacune un secret avec l'intercepteur, pas avec l'interlocuteur désiré.

IPSEC : AH et ESP

IPSEC est basé sur deux extensions possibles aux datagrammes IP(v6 donc, mais aussi v4 modifié) :

AH ou Authentication Header : services d'authentification, intégrité des données, protection contre le rejeu, éventuellement non répudiation.
ESP ou Encapsulating Security Payload : services de confidentialité, intégrité, authentification, détection de rejeu et confidentialité du flux de données.
AH existe surtout pour des questions de législation.

IPSEC : positionnement

IPSEC peut être utilisé :

- Entre les deux interlocuteurs (protection "de bout en bout")
- Entre les passerelles d'accès aux réseaux des interlocuteurs (et donc pas entre passerelle et utilisateur)
- Ou bien entre l'utilisateur et la passerelle d'accès au réseau (pour protection interne)
- Ou encore entre un utilisateur et la passerelle du correspondant ...

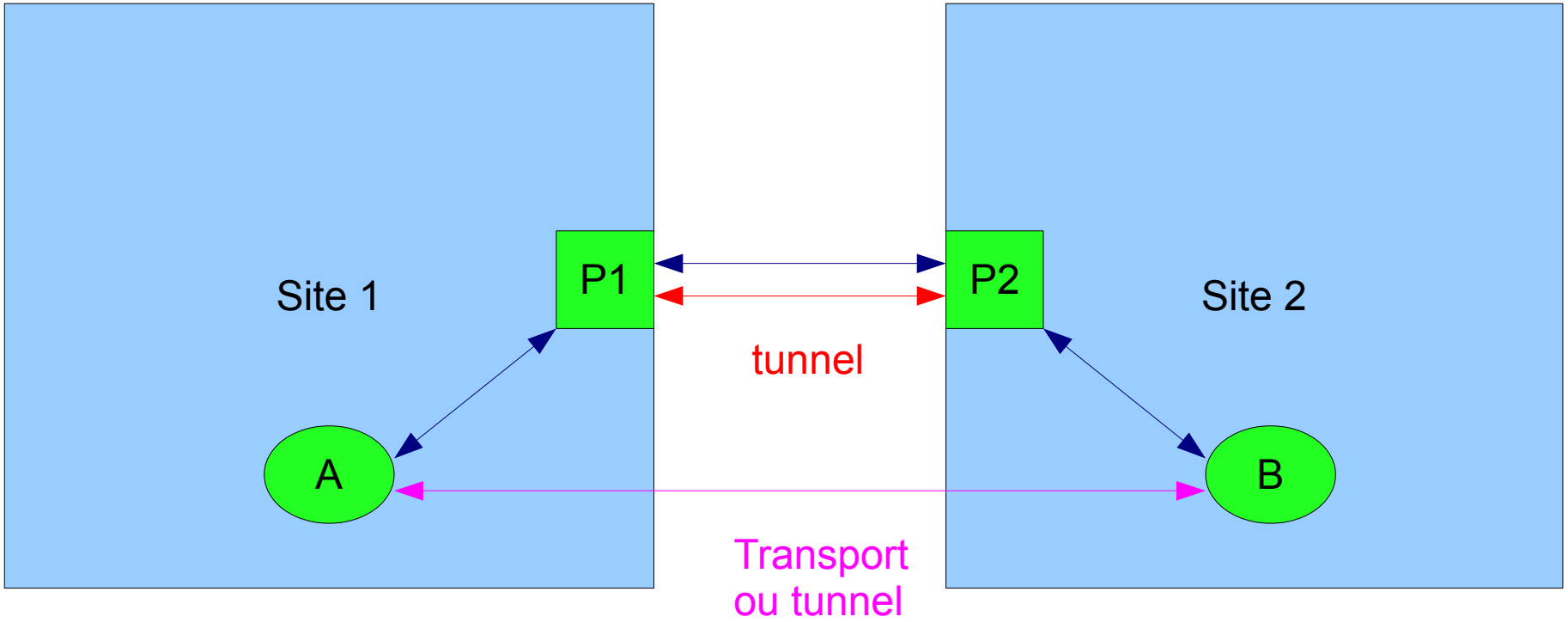
IPSEC : Modes

Du fait des différents positionnements possibles, IPSEC peut être utilisé dans deux modes différents :

- Mode transport. Les données du dg sont protégées (chiffrées et/ou authentifiées), l'en-tête principale étant inchangée. Prend en compte également la protection de certains éléments de l'en-tête.
- Mode tunnel. Le dg initial est encapsulé dans un nouveau dg (adresses différentes). Tout le dg est ainsi protégé, y compris adresses source et destination.

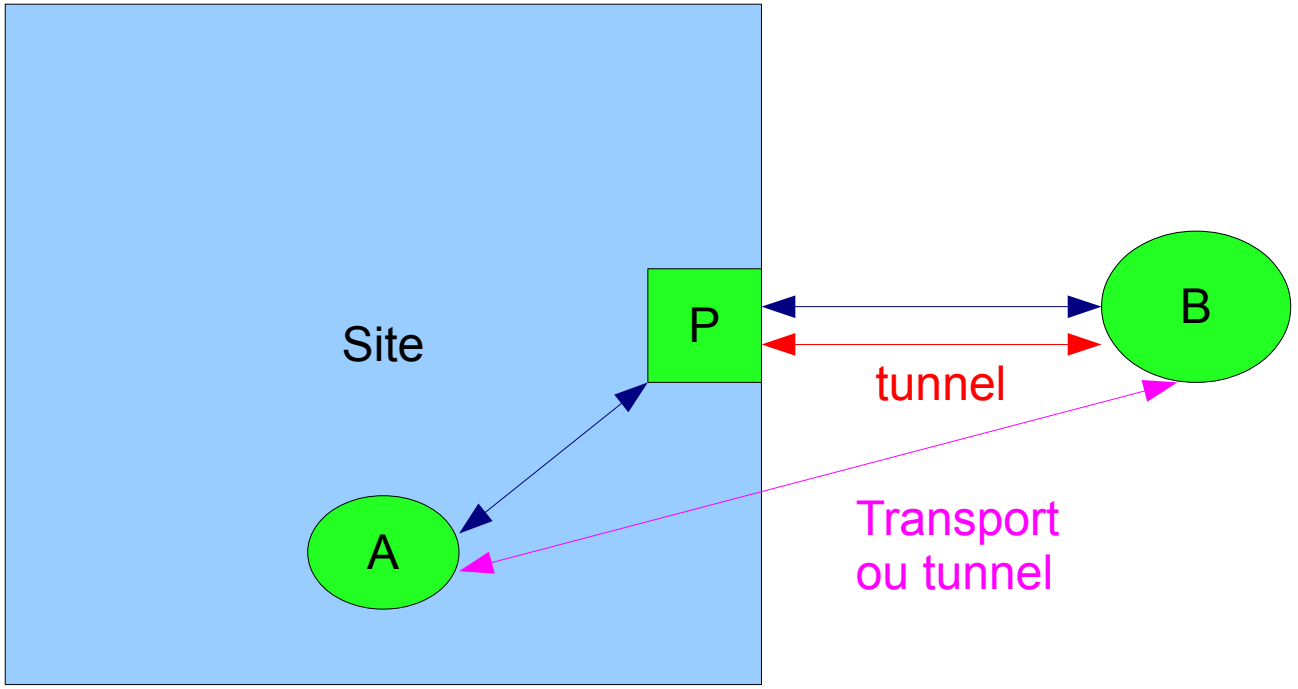
IPSEC : Utilisations

Utilisation entre deux sites d'une même entreprise



IPSEC : Utilisations

Utilisation entre un site et une machine reliée à Internet



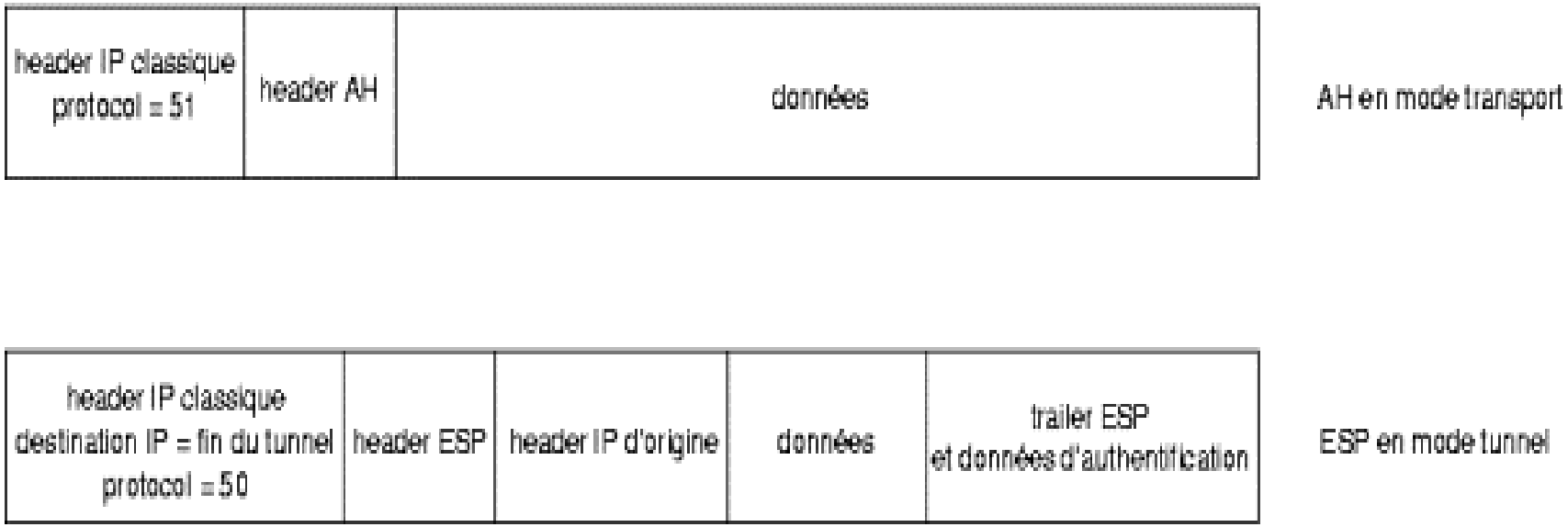
IPSEC : Utilisations

Les extensions AH et ESP ont été pensées pour IPv6 : leurs codes respectifs (51 et 50) sont annoncés par le champ "next header" de l'en-tête principal ou précédent, et leur propre champ "next header" indique la nature des données (TCP ou UDP) ou l'entête suivant.

En v4, IPSEC n'a pas été prévu à l'origine. Ce fonctionnement doit donc être géré par le module additionnel implémentant IPSEC.

IPSEC et IPv4

Les extensions AH ou ESP sont intercalées entre en-tête et données, comme en v6 :



Association de sécurité

Une SA (Security Association) définit les paramètres d'une communication en vue de protéger un échange entre deux points.
Une SA est identifiée par :

- un indice de paramètres de sécurité SPI
- l'adresse de destinataire du paquet IP
- le type de protection AH ou ESP

Elle est unidirectionnelle. (Donc 2 SA pour communication bidirectionnelle).

Contenu d'une SA

Principaux paramètres :

- algorithme d'authentification, clés de chiffrement utilisées pour l'authentification
- algorithme et clés de chiffrement
- durée de vie de la SA
- mode utilisé (tunnel ou transport)

Le SPI figure dans chaque extension de sécurité

IPSEC : implémentation(1)

Deux bases de données dans le système :
SPD (Security Policy Database)
Ensemble de règles comportant les critères de sélection et l'action à effectuer :

- rejet du paquet (discard)
- paquet autorisé, sans sécurité (bypass IPSEC)
- application de la ou des SA à appliquer, définies dans la deuxième base de données.

IPSEC : implémentation(2)

SAD (Security Association Database)
Précise pour chaque SA les services et mécanismes de sécurité à appliquer
(SPI, adresse destination, protocole AH ou ESP)

Un système peut ainsi ouvrir plusieurs SA simultanément, avec un ou des partenaires.
En V6, toute pile doit implémenter IPSEC (théorique ...)

IPSEC : AH

AH authentifie l'émetteur, assure l'intégrité du DG et peut détecter le rejeu. Les champs sont:

- l'en-tête suivante
- la longueur de l'extension
- le SPI
- le no de séquence (détecte le rejeu)
- les données d'authentification

L'authentification porte sur les données et les champs invariables du DG (mode transport).

IPSEC : ESP(1)

Chiffrement, authentification, intégrité.
Aussi détection de rejeu (si authentification utilisée) et, dans une certaine mesure, confidentialité du flux (possibilité de bourrage).
En mode transport seules les données sont protégées. De manière générale, le chiffrement s'applique aux données ou au paquet tunnelé, l'authentification inclus également l'en-tête ESP

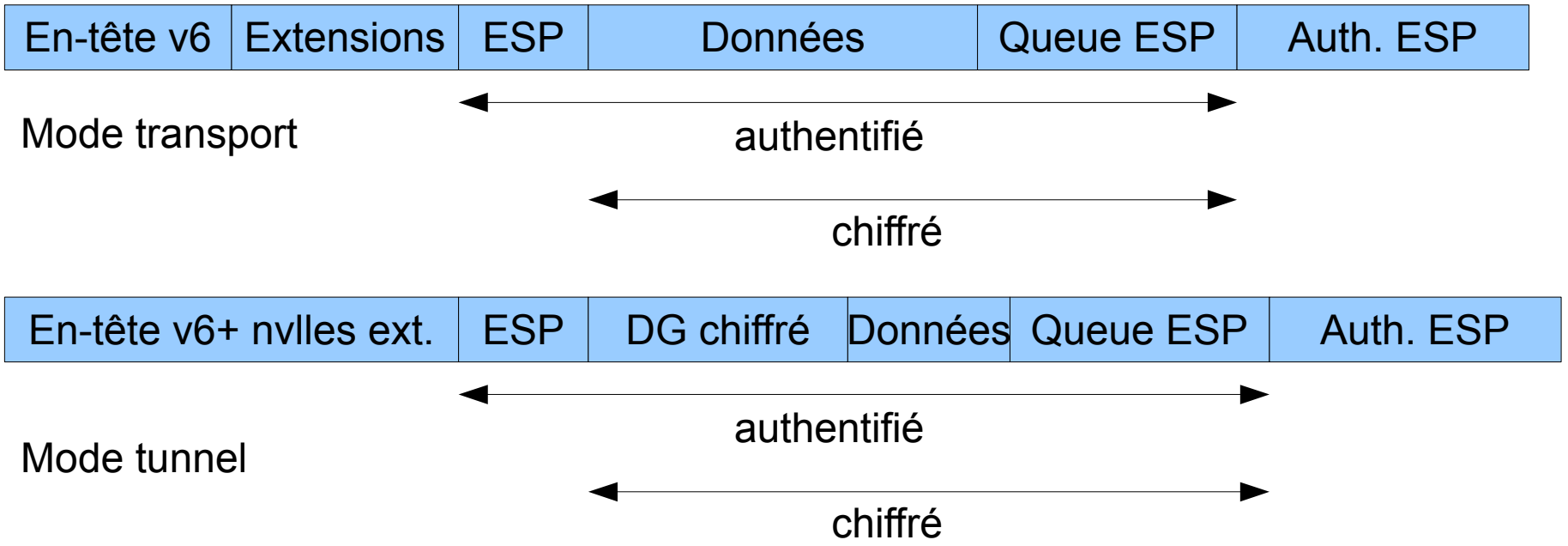
IPSEC : ESP(2)

L'en-tête ESP contient :

- l'en-tête suivante
- le SPI
- le no de séquence
- les données chiffrées, dont le champ de bourrage et sa longueur
- les données d'authentification (optionnelles)

IPSEC et IPv6

En v6, les extensions AH ou ESP sont les dernières (sauf un cas particulier d'option "destination").



Échange de clefs

Le problème de Diffie-Hellman est l'attaque possible de l'intercepteur.
Pour pallier ceci :

- soit échange de clefs "manuel" (mais clés fixes)
- soit système de certification des clefs publiques (serveurs "connus" – et authentifiés ! - certifiant les identités de personnes – ou organismes - inscrites)

ISAKMP

Internet Security Association and Key Management Protocol.
Cadre générique pour la gestion d'association de sécurité
Utilisé surtout pour IPSEC mais possibilité de négocier une liaison SSL par exemple.
Un DOI (domain of Interpretation) définit les paramètres et l'utilisation pour un cadre précis (par exemple IPSEC)

ISAKMP (2)

Deux phases :
1 : authentification des entités, génération de clefs, mise en place d'une SA bidirectionnelle pour protéger les échanges suivants
2 : négociation de SA pour divers protocoles (AH et ESP de IPSEC par exemple)
"kit de construction" pour un protocole d'échange de clefs

IKE

Instance de ISAKMP (définie pour IPSEC)
Main Mode et Agressive Mode pour la phase 1
6 échanges ou 3, le main mode offrant plus de sécurité : PFS notamment.
Quick Mode pour la phase 2 (3 échanges), peut (option) négocier les champs authentifiés.

New Group Mode pour de nouveaux échanges Diffie-Hellman après établissement SA ISAKMP.
IKE version 2 : simplification.

IKE phase 1

Négociation des attributs et génération de 3 clefs pour chiffrer, authentifier, et dériver d'autres clefs.
Main Mode nécessite 6 messages servant à :
négociation des algos, méthodes d'auth.,
secret partagé Diffie-Hellman
authentification des partenaires
Agressive Mode : 3 échanges mais pas propriété PFS (découverte des clefs de longue durée ne permet pas de casser les clefs de session générées avant)

IKE phase 2

Quick Mode pour négocier les SA IPSEC.
Génère une nouvelle clé dérivant de celle de la SA ISAKMP
Possibilité de nouvel échange Diffie-Hellman pour assurer PFS

Utilisation

Si une SA doit être utilisée pour échanger les données, alors celle-ci est établie par IKE si elle n'est pas déjà en place.
En entrée, si un paquet concerne IKE, il doit pouvoir passer pour être traité même si pas de SA active.

PKI : Public Key Infrastructure

Autorités de certification habilitées à délivrer des certificats (authentification des clefs publiques)
Organisées hierarchiquement.
Certificat : clé publique, identité, durée de validité
DNSSEC : Possibilité d'authentifier les enregistrements DNS. Un DNS peut alors jouer le rôle d'une autorité de certification.

cf. cours spécifiques

IPSEC - conclusion

Utilisé à l'heure actuelle surtout pour création de VPNs d'entreprise : liaison entre sites et/ou connexion de collaborateurs nomades au site de l'entreprise.
Encore assez lourd à mettre en œuvre.

Futur : avec Ipv6 et lorsque les piles incluront effectivement IPSEC, communications chiffrées et authentifiées entre particuliers possibles.