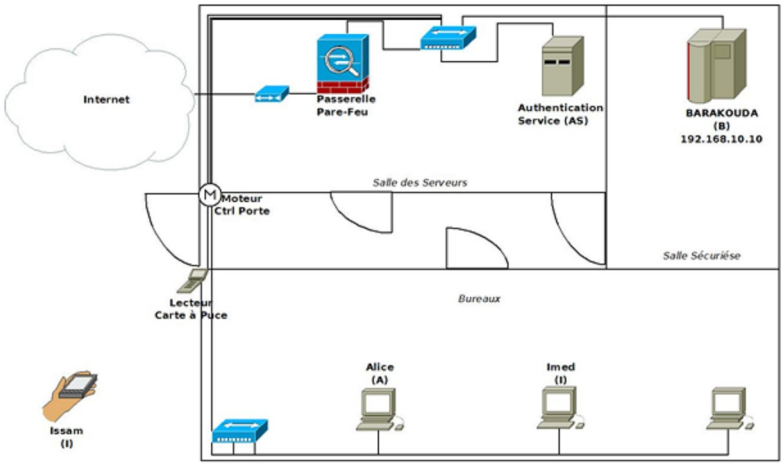
Ingénierie des Protocoles et Logiciels Sécuriés

Communications Sécurisées : Protocoles et Architectures

Version 1



08/01/2015

Table des matières

I

Communications Sécurisées : Protocoles et Architectures

- Prolifération des applications et systèmes distribués dans l'entreprise
- Applications distribuées outil principal dans le SI de l'entreprise.
- Structures décentralisées et géographiquement éloignées de l'entreprise moderne
- Nécessité de déploiement d'architectures communicationnelles robustes et sécurisées
- Ces architectures sont basées sur des protocoles cryptographiques validés et éprouvés pour éviter toute intrusion et anomalie

A. Réseaux Privés Virtuels (VPN)

Problématique

Comment assurer l'accès sécurisé à des applications distribuées sur des sites géographiquement distants. Les VPN ont été mis en place pour répondre à ce type de problématique

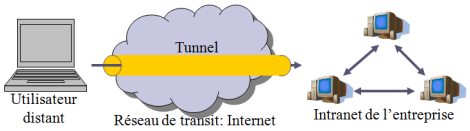
Méthode

Un VPN repose sur un protocole de « tunneling ». Ce protocole permet de transporter les données de l'entreprise chiffrées d'un bout à l'autre du tunnel. Il construit un chemin virtuel d'une source à une destination après leur identification. La source chiffre les données qui empruntent ce chemin virtuel, et la destination déchiffre. Le protocole encapsule les données dans une entête. Le tunneling est le processus d'encapsulation, transmission puis décapsulation. Les usagers auront l'impression de se connecter au réseau local de l'entreprise.

1. Types de VPN

VPN d'accès

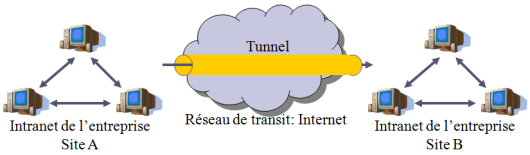
Clients itinérants accèdent au réseau local de l'entreprise.



VPN d'accès

Intranet VPN

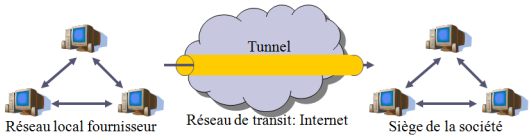
L'entreprise possède plusieurs sites distants



VPN Intranet

Extranet VPN

L'entreprise ouvre son réseau local à ses partenaire. Il est fondamental que l'administrateur du VPN puisse tracer les clients sur le réseau et gérer les droits d'accès de chacun sur le réseau.



VPN Extranet

2. Mise en oeuvre des VPN

Fondamental : Fonctions d'un VPN

Un système VPN doit pouvoir assurer les fonctionnalités suivantes:

- Authentification d'utilisateur: seuls les utilisateurs autorisés doivent pouvoir s'identifier sur le VPN. Un historique des connexions et actions effectuées doit être conservé.
- Gestion d'adresses: chaque client sur le réseau doit avoir une adresse privée confidentielle.
- Chiffrement des données: lors de leurs transports sur le réseau publique, les données doivent être protégées par un chiffrement efficace.
- Gestion de clés: les clés de chiffrement pour le client et le serveur doivent pouvoir être générées et régénérées.
- Prise en charge multiprotocole: la solution VPN doit supporter les protocoles les plus utilisés sur les réseaux publiques en particulier IP.

Remarque

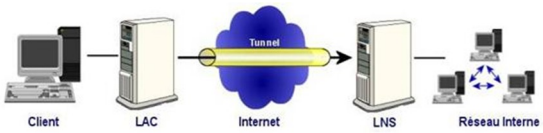
Le VPN est un principe: il ne décrit pas l'implémentation effective, c'est pourquoi il existe plusieurs produits différents dont certains sont devenus standards.

3. L2TP: VPN niveau 2

L2TP: Layer Two Tunnelling Protocol

Permet l'encapsulation de trames PPP dans des protocoles de couche 2 (ATM et

Frame Relay), et couche 3 (IP) (RFC 2661). Il peut être utilisé pour créer un tunnel sur Internet (Encapsulation de PPP dans IP). Il repose sur deux concepts: Les concentrateurs d'accès L2TP (LAC) Les serveurs réseau L2TP (LNS)



L2TP

4. IPSec, ou tunnelling niveau 3

Introduction

L'objectof de IPSec est de sécuriser l'échange de données au niveau de la couche réseau (RFC2401). Il est basé sur trois protocoles:

- AH: Authentication Header, pour l'intégrité et l'authenticité des datagrams IP
- ESP: Encapsulating Security Payload, pour l'authentification et la confidentialité des données.
- IKE: Internet Key Exchange, permet de gérer les associations de sécurité.

Fondamental : Association de Sécurité

Les protocoles AH et ESP utilisent des mécanismes cryptographiques (algorithmes de chiffrement, hachage, clés, ...), sur lesquels doivent se mettre d'accord les tiers communicants. IPSec utilise une structure de données appelée SA (Security Association) pour stocker ces paramètres cryptographiques. Une association de sécurité (SA) est unidirectionnelle. Une SA est identifiées d'une manière unique avec:

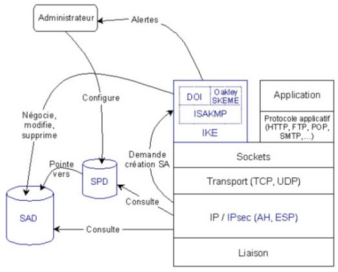
- L'adresse de destination des paquets
- L'identifiant du protocole de sécurité utilisé (AH ou ESP)
- Un SPI (Security Parameter Index): un bloc de 32 bits inscrit en clair dans l'entête de chaque paquet échangé: il est choisi par le récepteur.

Les SA sont négociées et établies suivant le protocole IKE.

Une SAD (Security Association Database) contient et permet de gérer les SA actives. Elle sera consultée pour savoir comment traiter chaque paquet reçu ou à émettre. La protection offerte par IPSec est basée sur des choix définis dans une SPD (Security Policy Database). Elle décidera pour chaque paquet s'il se verra apporté des services de sécurité, s'il sera autorisé à passer, ou rejeté.

Vue d'ensemble

La figure suivante synthétiqe le fonctionnement de IPSec et les actions à entreprendre selon le type de trafic (entrant ou sortant) :

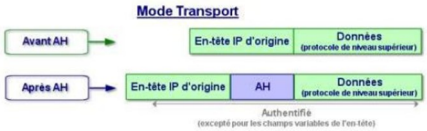


IPSecs

- Trafic sortant :
  - Consulter SPD
  - Consulter SAD,
  - récupérer SA à appliquer
  - Si SA n'existe pas, alors
    - Demande création SA à IKE
  - Appliquer SA
- Trafic entrant
  - Récupérer référence SA de l'entête
  - Récupérer SA de SAD
  - Appliquer SA pour vérifier et/ou déchiffrer le paquet
  - Consulter SPD pour voir si l'application de la SA correspond bien à la politique de sécurité requise

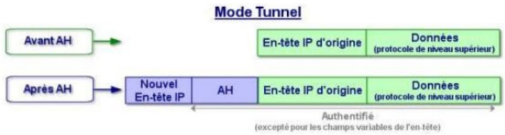
Deux modes de fonctionnement

- Mode transport : Réalise les mécanismes IPSec sur un flux de niveau transport, puis le transmet à IP. Se fait généralement en deux hôtes.
  - Avantage: facilité de mise en œuvre
  - Inconvénient: entête IP externe non protégée



Mode transport

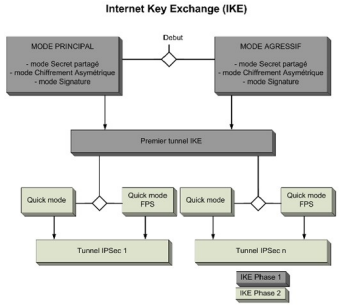
- Mode tunnel : Les données de l'application traversent la pile de protocole jusqu'à IP inclus, puis le flux est transmis à IPSec. Se fait généralement entre deux passerelles.
  - Avantage : permet le masquage d'adresses
  - Inconvénient : plus d'overhead dû à plus d'encapsulation



Mode tunnel

IKE : Internet Key Exchange

IKE se déroule en deux phases comme illustré sur la figure suivante :

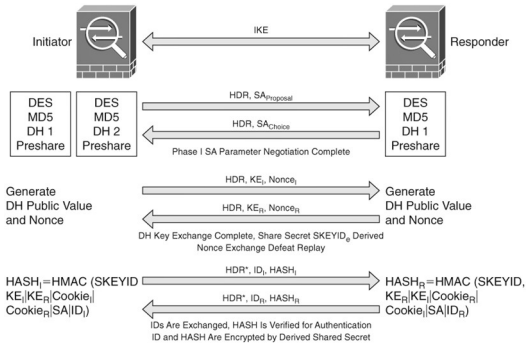


IKE

- Phase 1: authentifier les deux parties et faire un échange de clé pour protéger la phase 2

Il existe deux modes pour la phase 1 : mode principal et mode agressif

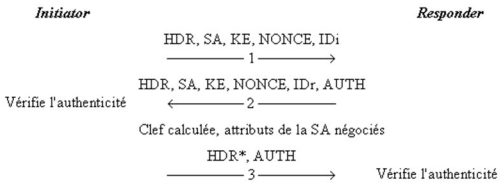
- Mode Principal (Protège les identités des pairs)



Phase 1 : mode principal

-

  - Mode agressif (ne protège pas les identités des pairs)



Mode agressif

- Phase 2: la SA de la phase 1 est utilisée pour générer une SA additionnelle pour transporter le trafic entre les entités (mode rapide).

  Il existe deux modes:

  - Sans PFS (Perfect Forward Secrecy): les clés sont dérivées des clés de la phase 1
  - Avec PFS: un nouvel échange Diffie Hellman pour générer des clés indépendantes

5. VPN-SSL ou tunnelling niveau 4

- Usage de SSL
- Souplesse et facilité de déploiement: Nécessite uniquement un navigateur du côté client
- Établissement d'un canal sécurisé entre deux applications
- Deux fonctionnalités de sécurité:
  - Authentification du serveur et du client éventuellement
  - Chiffrement des échanges

B. Pretty Good Privacy (PGP)

Objectif

Protéger l'échange de courriers électroniques

Complément : Performance

Combine systèmes symétriques et systèmes asymétriques

Fondamental : Principe de fonctionnement

PGP choisit une clef symétrique aléatoire: clef de session. Chiffre le courrier avec la clé de session. Puis, chiffre la clé de session avec la (les) clef(s) publique(s) du (des) destinataire(s). Ces derniers pouront alors déchiffrer la clé de session avec leur clé privée puis déchiffre le message avec la clé de session.

Remarque : Protection des clés privées

Les clefs privées sont chiffrées sur le disque de l'utilisateur de PGP en utilisant un algorithme de dérivation de clef à partir d'un mot de passe. Quand la clef privée est nécessaire (pour signer ou déchiffrer un message), l'utilisateur saisit le mot de passe pour déchiffrer sa clé privée

Méthode : Distribution des clés publiques

Le moyen le plus simple et efficace est de rencontrer la personne, de l'authentifier et lui demander sa clé publique. Cette rencontre physique n'est pas toujours commode. On récupère les clefs publiques des annuaires (dit serveurs) PGP. Une clef PGP obtenue sur un serveur PGP ne devrait pas être considérée de confiance sans vérification supplémentaire. Un intrus peut enregistrer une clef PGP sous un faux nom car il n y a pas de vérification. Quelqu'un peut être victime d'une usurpation de DNS et être redirigé vers un faux serveur PGP. Pour faire cette vérification, Alice récupère de l'annuaire une clé publique de Bob signée par Charlie à qui elle fait confiance (elle connaît la clef publique de Charlie).

Remarque : Graphe de Confiance

La relation entre Alice et Charlie peut être généralisée aboutissant à un graphe de confiance. Le poids des arêtes est le niveau de confiance :

- Confiance inconnue
- Aucune confiance
- Confiance partielle
- Confiance totale

Avant d'envoyer un courrier à Bob, Alice doit trouver un chemin de confiance qui la mène à Bob, calculer la confiance qu'elle a dans la personne qui a signé la clé de Bob, décider si elle considère la clef de Bob valide

Graphe de Confiance

Calcul du niveau de confiance dans le modèle PGP

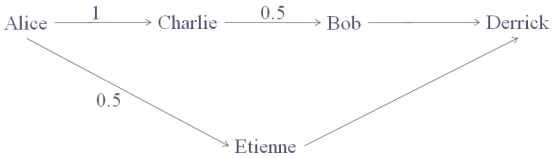
Les poids des confiances sur un même chemin se multiplient. Les poids des confiances sur des chemins disjoints se rajoutent.

On considère les poids suivants:

- Confiance totale = 1
- Confiance partielle = 0.5
- Aucune confiance = 0

Exemple

Dans le graphe de confiance suivant :



Exemple de calcul de la confiance

La confiance de Alice en Bob est de 0.5. La confiance de Alice en Etienne est de 0.5. Bob et Etienne délivrent chacun un certificat à Derrick. La confiance calculée de Alice en Derrick est de 0 .0+0.5=1.

Révocation des clés PGP

Retirer la clé déposée sur un serveur PGP ne suffit pas. Les utilisateurs ont stocké la clé sur leurs disques. De ce fait, la clé est répliquée sur d'autres serveurs.

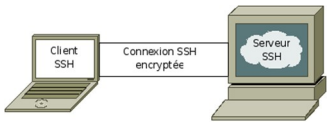
Solution:

- Générer un certificat de révocation
- Envoyer ce certificat sur le serveur PGP
- Envoyer le certificat aux correspondants réguliers

C. Secure Shell (SSH)

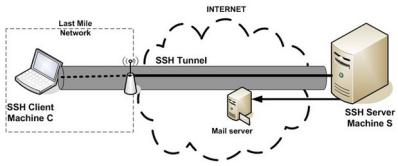
Définition : SSH

C'est un protocole qui permet de faire des connexions sécurisées (i.e. chiffrées) entre un serveur et un client SSH.



SSH

Ce tunnel peut servir pour protéger le flux de n'importe quelle application comme illsutré sur la figure suivante :



Tunnelling avec SSH

Méthode : Etablissement d'une connexion SSH

Un serveur SSH dispose d'un couple de clefs RSA stocké dans le répertoire /etc/ssh/ et généré lors de l'installation du serveur. Le fichier ssh_host_rsa_key contient la clef privée et a les permissions 600. Le fichier ssh_host_rsa_key.pub contient la clef publique et a les permissions 644. Le serveur envoie sa clef publique au client. Celui-ci vérifie qu'il s'agit bien de la clef du serveur, s'il l'a déjà reçue lors d'une connexion précédente, ou comparaison à un hash ou certificat.

Le client génère une clef secrète (symétrique) et l'envoie au serveur, en chiffrant l'échange avec la clef publique du serveur. Le serveur déchiffre cette clef secrète en utilisant sa clé privée. Pour le prouver au client, il chiffre un message standard avec la clef secrète et l'envoie au client. Si le client retrouve le message standard en

utilisant la clef secrète, il a la preuve que le serveur est bien le vrai serveur. le client et le serveur peuvent alors établir un canal sécurisé grâce à la clef secrète commune (chiffrement symétrique).

Une fois que le canal sécurisé est en place, le client va pouvoir envoyer au serveur le login et le mot de passe de l'utilisateur pour vérification.

Remarque

Au lieu de s'authentifier par mot de passe, les utilisateurs peuvent s'authentifier grâce à la cryptographie asymétrique et son couple de clefs privée/publique, comme le fait le serveur SSH auprès du client SSH. La clé privée de l'utilisateur est protégée (chiffrée) par un mot de passe, qui lui sera demandé à chaque utilisation de cette clé.

Série d'Exercices Protocoles de communication sécurisée

II

A. Déploiement de PGP

Alice, directrice d'une agence d'une société, doit faire parvenir régulièrement un compte-rendu d'activité au responsable qualité de la société. Pour cela, ce dernier préconise à tous les directeurs d'agences d'utiliser PGP afin de chiffrer et de signer les données transmises ; il déconseille en revanche d'utiliser un graphe de confiance pour valider les clefs.

Après avoir installé PGP sur son ordinateur, Alice a généré une paire de clefs asymétriques (clef publique / clef privée) pour le chiffrement et la signature des données. Elle conserve cette paire de clefs uniquement sur le disque dur de son ordinateur.

Question 1

Quel moyen permet d'éviter que n'importe qui puisse lire la clef privée d'Alice sur son disque dur ?

Question 2

Donner la démarche précise que doivent accomplir Alice et le responsable qualité avant de pouvoir s'échanger de manière sûre des informations par courrier électronique.

Question 3

On suppose maintenant que l'étape de la question précédente a été réalisée. Alice souhaite envoyer son compte-rendu d'activité. Elle chiffre le fichier mais oublie de le signer. A sa grande surprise, PGP ne lui demande aucun mot de passe, Pourquoi ?

Question 4

Etant donné que les systèmes de chiffrement asymétriques sont beaucoup plus lents que les systèmes de chiffrement symétrique, PGP n'utilise pas directement la clef publique du destinataire pour chiffrer les données proprement dites. Expliquer le procédé réellement utilisé par PGP.

Question 5

Détailler ce procédé si le responsable qualité envoie un même courrier électronique à plusieurs directeurs d'agence.

Question 6

Satisfaite, des services de PGP, Alice souhaite également l'utiliser pour chiffrer les sauvegardes de son disque dur : elle chiffre son répertoire avec PGP puis sauvegarde le fichier obtenu sur une bande magnétique. A quel risque s'expose-t-elle si son disque dur tombe en panne ?

Le responsable qualité de la société s'aperçoit qu'il est fastidieux de gérer ce procédé et préfère abandonner PGP au profit d'un service accessible via un site web en utilisant un serveur HTTPS.

Question 7

Quel est le protocole de sécurité sur lequel est fondé HTTPS ?

Question 8

Le responsable qualité a obtenu un certificat X-509 pour le site web auprès d'une autorité de certification. Quel est le but de ce certificat ?

Question 9

Outre la signature de l'autorité de certification, quelles sont les deux onformations essentielles que l'on trouve de manière générale dans un certificat ?

Question 10

Lorsque Alice se connecte sur le site web, son navigateur vérifie la validité du certificat fourni. Quelle clef sera utilisée par son navigateur ? Comment l'aura-t-il obtenue ?

B. SSH et VPN

Le protocole SSH remplace les protocoles de connexion à distance et de transfert de fichiers comme Telnet, rsh, FTP, et rcp avec un protocole authentifiant les clients et les serveurs et chiffrant toutes les données échangées. De plus, avec sa fonctionnalité de redirection de port, il permet de sécuriser d'autres protocoles.

Toute connexion vers un port local du client peut être acheminée par un tunnel chiffré vers le serveur SSH qui relaiera la connexion vers un serveur prédéfini. Il est ainsi possible d'utiliser une connexion SSH vers une machine à l'intérieur d'un réseau d'entreprise pour accéder à sa messagerie en faisant passer le protocole POP à travers un tunnel SSH. On pourrait ainsi aussi accéder à des serveurs de fichiers ou tout autre service disponible à l'intérieur du réseau d'entreprise.

Question 1

Est-ce qu'un système de tunnel SSH peut offrir toutes les fonctionnalités qu'offre un VPN classique ? Justifier la réponse.

Question 2

Quelle erreur se produit si on utilise un tunnel SSH pour atteindre un serveur HTTPS ?

Question 3

L'administrateur réseau autorise les connexions SSH depuis Internet vers la machine interne de l'utilisateur afin qu'il puisse accéder à ses fichiers. Expliquer les risques auxquels s'expose l'administrateur et discuter comment il pourrait s'en prémunir.

Question 4

Rencontre-t-on les mêmes problèmes dans le cas d'un VPN classique ?