Licence Professionnelle SEICOM
Module M3-7
« Les technologies VPN »

Pierrick Tasse – Damien VERON
IUT Nantes, GEII

Présentation technique

Sommaire

- La cryptographie
  - Terminologie
  - Algorithme de chiffrement…
  - Fonctions de hachage, signature, scellement
  - Authentification mutuelle et échange de clefs de session
  - Certificat
- La base des VPNs
- Les topologies de VPNs IPsec
- Exemples et exercices

La Cryptographie

- **La cryptographie**
  - **Terminologie**
  - **Algorithme de chiffrement…**
  - **Fonctions de hachage, signature, scellement**
  - **Authentification mutuelle et échange de clefs de session**
  - **Certificat**
- La base desVPNs
- Les topologies deVPNsIPsec
- Exemples et exercices

Terminologie

- Définition : méthodes permettant de transmettre des données de manière confidentielle.
- On applique aux données une transformation qui les rend incompréhensibles :
  - Etape 1 : chiffrement qui donne un texte chiffré ou cryptogramme
  - Etape 2 : déchiffrement

  - Les transformations : des fonctions mathématiques appelés algorithmes cryptographiques dépendant d'un paramètre appelé clef.

Terminologie

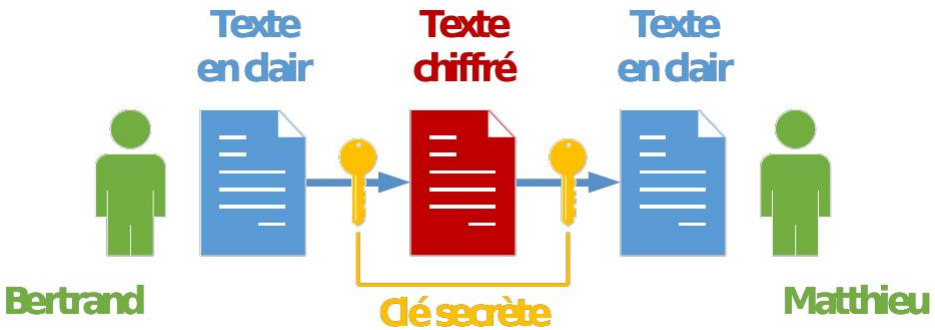
- But :
  - Confidentialité
  - Intégrité
  - Authentification de l'origine des données ou d'un tiers
  - Non-répudiation
  - …
- Moyens
  - Chiffrement
  - Scellement et signature
  - Protocoles d'authentification mutuelle avec échange de clefs
  - …

Algorithme de chiffrement

- On utilise 2 types algorithmes cryptographiques. L'algorithme est en général public, et le secret du chiffre dépend d'un paramètre appelé clé.
  - Algorithmes symétriques ou à clé privé
  - Algorithmes asymétriques ou à clef publique
    - Échange de clefs publiques
    - Signature

Algorithme de chiffrement ou à clé privée

- Clef de chiffrement = clé de déchiffrement, elle doit rester secrète. (exemple : Che Guevarra)



Algorithme de chiffrement ou à clé publique

- Clefs de chiffrement et de déchiffrement distinctes
  - Connaître la clé publique ne permet pas de retrouver la clef privé correspondante
  - Algorithmes lents pour une utilisation intensive (chiffrements des données), souvent utilisés pour l'échange de clef, la signature.

Algorithme de chiffrement ou à clé publique

- Chiffrement
  - Clé publique utilisée pour le chiffrement, seul le détenteur de la clé privée peut déchiffrer.
    (Exemple : Cadenas ouvert)

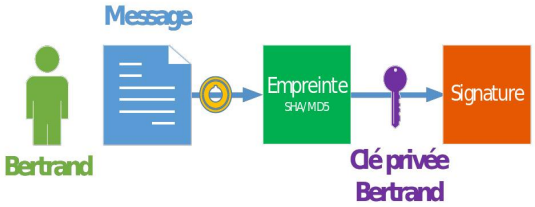
- Signature
  - Clé privée utilisée pour le chiffrement, seul son détenteur peut chiffrer, mais tout le monde peut déchiffrer (et donc vérifier la signature).

Fonction de Hachage, Signature et Scellement

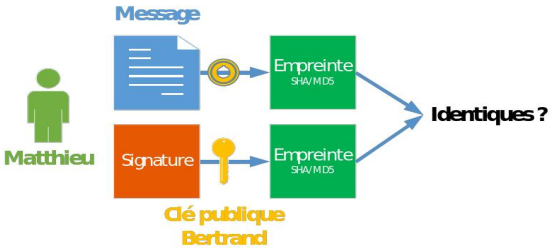
- Hachage, Signature, Scellement : mécanisme fournissant les services d'intégrité, d'authentification de l'origine des données et la non-répudiation de la source.
  - Hachage : fonction qui permet de convertir une donnée quelconque en une chaîne de taille inférieure et fixe = empreinte numérique d'un fichier (SHA ou MD5).

Fonction de Hachage, Signature et Scellement

- Signature

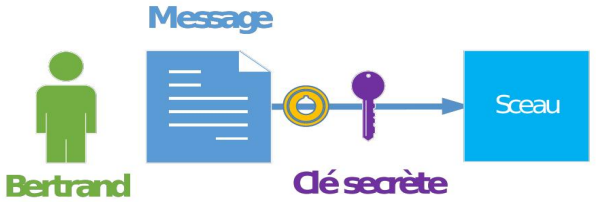


- Verification

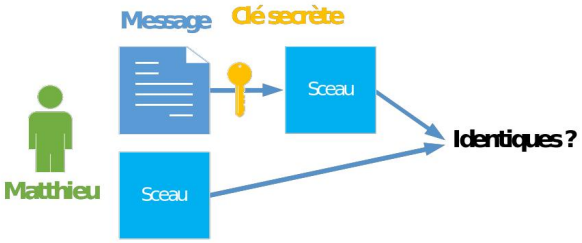


Fonction de Hachage, Signature et Scellement

- Scellement



- Verification



Authentification mutuelle et échange de clefs de session

- L'échange de clefs doit être authentifié pour éviter les attaques.
- Une clef de session permet d'étendre l'authentification à l'ensemble de la communication
- Protocole d'authentification mutuelle avec échange de clefs
  - Fournit authentification mutuelle et un échange de clefs authentifié tout-en-un

- Types d'échange de clefs
  - Transport (ex : RSA)
  - Génération (ex : Diffie Hellman)

Authentification mutuelle et échange de clefs de session

Transport de clef

Authentification mutuelle et échange de clefs de session

- Génération de clef
  - DH permet à deux tiers de générer un secret partagé sans informations préalables l'un sur l'autre

    1 - Matthieu génère une valeur publique à partir d'une valeur privée.

    2 - Bertrand fait de même.

    3 - Ils s'échangent leurs valeurs publiques mutuellement.

    4 - Un secret partagé est généré à partir de ces échanges

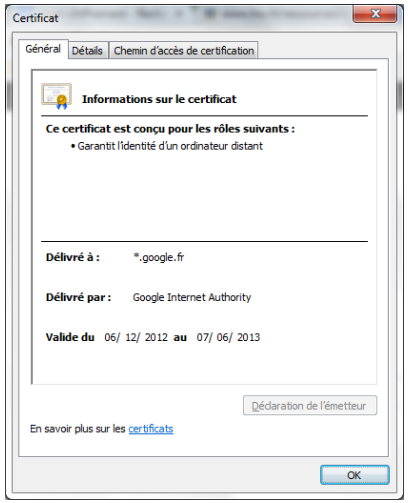
  - Un espion ne peut reconstituer le secret partagé à partir des valeurs publiques

Certificat

- Certificat = structure de données
  - Permet de lier une clef publique à différents éléments au moyen de la signature d'une autorité de confiance :
    - Propriétaire
    - Date de validité
    - Type d'utilisation
  - Emis par une autorité de certification (CA)
    - Garantit l'exactitude des données
  - Listes de révocation (CRL) permettant de révoquer un certificat avec l'expiration.
  - Vulnérabilité possible : les gestionnaires du système
    (Exemple de Virus Stuxnet contre le programme nucléaire Iranien)

Certificat

- Exemples d'utilisation :
  - Sites internet (SSL/TLS)
  - Messagerie
  - VPN Ipsec
  - Documents électroniques
  - Etc.



La base des VPNs

- La cryptographie
  - Terminologie
  - Algorithme de chiffrement…
  - Fonctions de hachage, signature, scellement
  - Authentification mutuelle et échange de clefs de session
  - Certificat
- **La base des VPNs**
- Les topologies de VPNs IPsec
- Exemples et exercices

La problématique

- Réseaux ont été créés pour partager librement des informations
- Nativement les réseaux permettent de transférer tout type de données rapidement mais de façon non sécurisée
- Les réseaux ATM, ISDN, MPLS offrent des solutions fiables et sécurisés mais coûteuses et dépendantes de fournisseurs de services qui ne garantissent pas la sécurité des données.
- Les liaisons Point-To-Point peuvent être interceptées. Par exemple, les lignes téléphoniques sont raccordés au commutateur d'un opérateur dont les locaux ne sont pas toujours sécurisés.

Définition

- VPN (Virtual Private Network) : canal virtuel et privé (RPV) de communication entre réseaux ou équipements à travers un réseau tiers ou publique tel qu'Internet
- Les réseaux privés virtuels ou VPN se définissent comme des réseaux physiquement ou logiquement séparés que l'on interconnecte par des liens de communication virtuels. Le terme virtuel est employé car le lien n'existe pas en tant que tel (physique).
- Réseau le plus souvent utilisé : Internet ➔ Faible cout
- Le chiffrement de l'information offre une totale sécurité des communications.
- Objectif de communication et ouverture du Système d'Information

Définition

- Utilisation d'un protocole de tunneling : circulation des informations de façon cryptée d'un bout à l'autre du tunnel.
  - Exemple : encapsuler un flux P2P dans une connexion TCP/IP (https)
- Le principe de tunneling consiste à construire un chemin virtuel après avoir identifié l'émetteur et le destinataire. Par la suite, la source chiffre les données et les achemine en empruntant ce chemin virtuel.
- Un tunnel IP s'effectue entre 2 machines, qui jouent le rôle de passerelles pour les autres machines de leur réseau respectif.
- Le tunneling peut rendre des services de différents ordres :
  - chiffrement et déchiffrement des données transmises.
  - compression et décompression des données envoyées dans le tunnel.
  - offrir l'impression à l'utilisateur de travailler en réseau local
  - la protection face
    - Aux pertes, destructions et expositions de données (confidentielles ou non)
    - Aux attaques, à l'espionnage

Définition

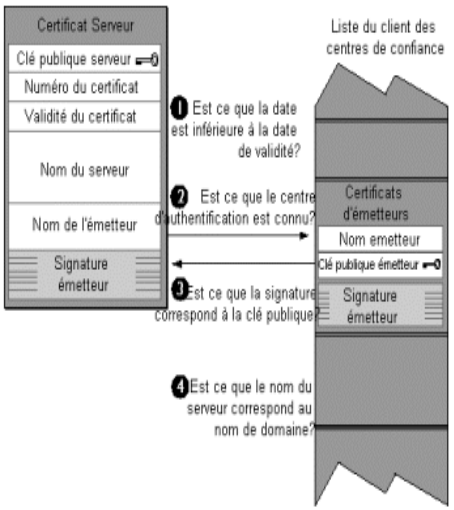
- Un serveur VPN doit pouvoir mettre en œuvre les fonctionnalités suivantes :
  - Authentification d'utilisateur
  - Gestion d'adresses privées
  - Cryptage des données
  - Gestion de clés de chiffrement
  - Confidentialité de l'information

Protocoles de tunnelisation couramment utilisés

- **PPTP** (Point-to-Point tunneling Protocol) est un protocole de niveau 2 développé par Microsoft, 3Com, Ascend, US Robotics et ECI Telematics.
- **L2TP** (Layer Two Tunneling Protocol) est l'aboutissement des travaux de l'IETF (RFC 3931 [archive]) pour faire converger les fonctionnalités de PPTP et **L2F** (Cisco). Il s'agit ainsi d'un protocole de niveau 2 s'appuyant sur PPP.
- **SSL/TLS** offre une très bonne solution de tunnelisation. L'avantage de cette solution est de permettre l'utilisation d'un navigateur Web comme client VPN.
- **SSH** permet, entre autres, d'envoyer des paquets depuis un ordinateur auquel on est connecté
- **IPsec** est un protocole de niveau 3, issu des travaux de l'IETF, permettant de transporter des données chiffrées pour les réseaux IP.

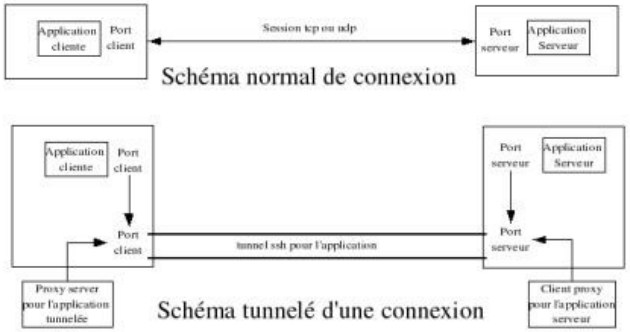
Protocoles de tunnelisation couramment utilisés

- Secure Sockets Layer / Transport Layer Security (SSL/TLS) : permet de sécuriser des connexions via un certificat.
  - Se situe entre la couche application et transport
  - Garantie l'authentification, l'intégrité et la confidentialité
  - Largement utilisé pour la sécurisation des sites www (https)
  - Mais également pour du chiffrement :
    - des processus d'authentification (LDAPs)
    - des courriels (SMTPs)
    - du transfert de données (sFTP)



Protocoles de tunnelisation couramment utilisés

- Secure Shell (SSH) est une application utilisée pour se connecter à un équipement au travers d'un réseau et d'y exécuter des commandes. Elle assure une authentification forte et sécurise les communications.



Protocoles de tunnelisation couramment utilisés

- **Internet Protocol SECurity (IPSec)** intègrent des protocoles de cryptage, d'authentification et de gestion des clés. Développés par l'IETF (Internet Engineering Task Force).
  - Spécifications
    - Authentification, confidentialité et intégrité (protection contre l'usurpation d'IP ou de session tcp)
    - Confidentialité (session chiffrée pour se protéger du sniffing)
    - Sécurisation au niveau de la couche transport (protection L3)
    - Algorithmes utilisés
      - Authentification par signature DSA ou RSA
      - Intégrité par fonction de condensation (HMAC-MD5 ou HMAC-SHA1)
      - Confidentialité par chiffrement DES, AES, etc/
  - Ipsec utilise 2 protocoles pour implémenter la sécurité sur un réseau IP :
    - Entête d'authentification (AH) permet d'assurer l'authentification des messages
    - Protocole de sécurité encapsulant (ESP) permettant d'authentifier et de crypter les messages

Protocoles de tunnelisation couramment utilisés

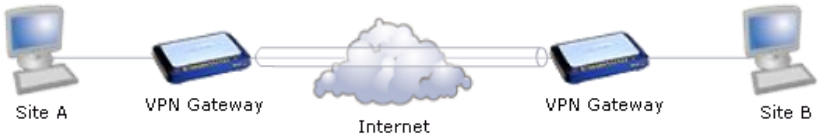
- Ipsec (suite)
  - Les VPN Ipsec peuvent être utilisés pour différents types d'accès :
    - Personnel nomade (télétravailleurs, nomades, expatriés)
    - Des sites distants
    - Des partenaires (fournisseurs, clients, prestataires)
  - Afin d'établir un tunnel, les 2 équipements doivent s'accorder sur les algorithmes et les protocoles.
    - Utilisation d'une SA (Security Association)
    - Une SA comprend :
      - Un algorithme de chiffrement (DES, 3DES, AES-256)
      - Une clé de session via IKE
      - Un algorithme d'authentification (SHA1-MD5)

Les topologies de VPNs IPsec

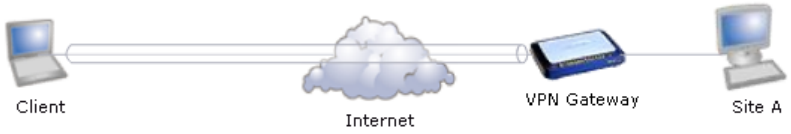
- La cryptographie
  - Terminologie
  - Algorithme de chiffrement…
  - Fonctions de hachage, signature, scellement
  - Authentification mutuelle et échange de clefs de session
  - Certificat
- La base des VPNs
- **Les topologies de VPNs IPsec**
- Exemples et exercices

Topologie des VPNs IPsec

- Site-To-Site

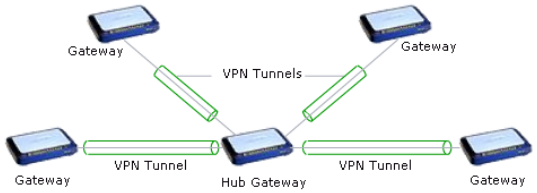


- Client-To-Site

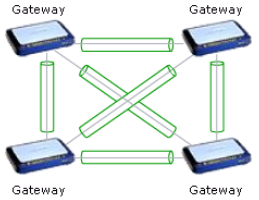


Topologie des VPNs IPsec

- Hub and Spoke (Transport / Expédition)



- Mesh (Maillé)

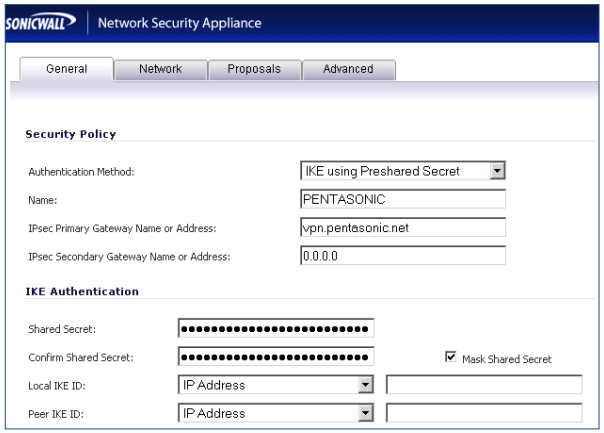


Exemples et exercices

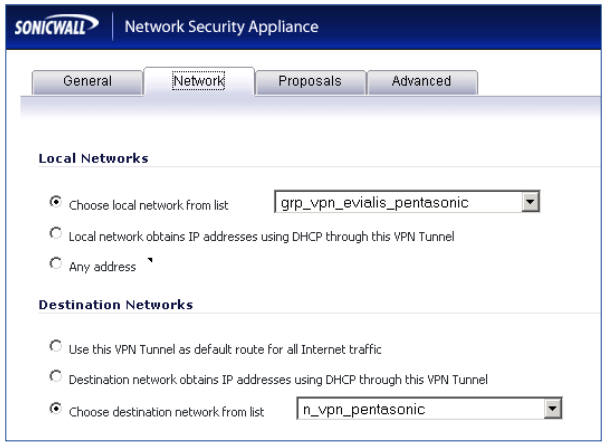
- La cryptographie
  - Terminologie
  - Algorithme de chiffrement…
  - Fonctions de hachage, signature, scellement
  - Authentification mutuelle et échange de clefs de session
  - Certificat
- La base des VPNs
- Les topologies de VPNs IPsec
- **Exemples et exercices**

VPN site-to-site

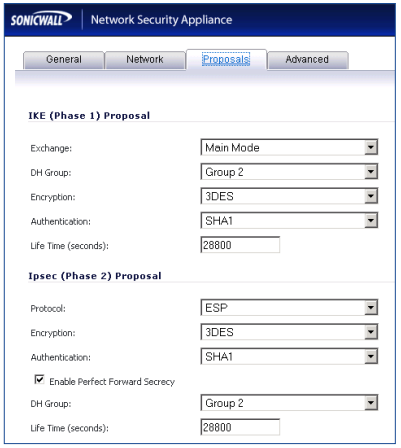
- Exemple de mise en œuvre (Dell Sonicwall)



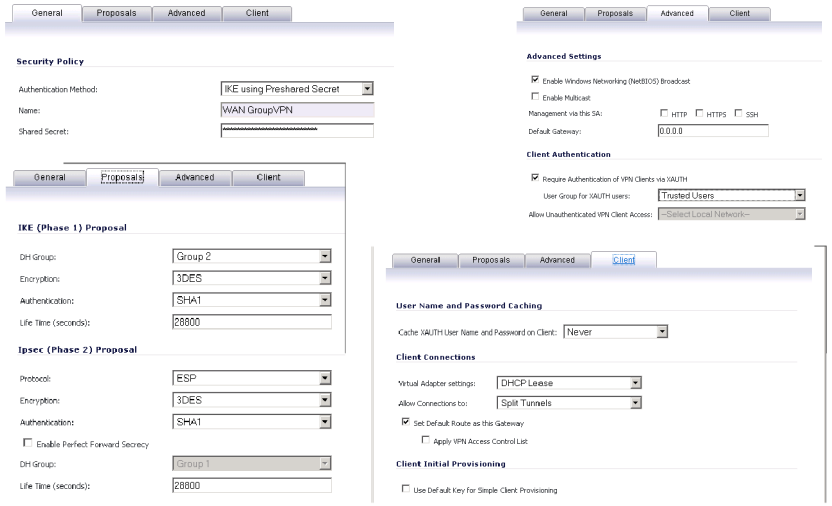
- Exemple de mise en œuvre (Dell Sonicwall)

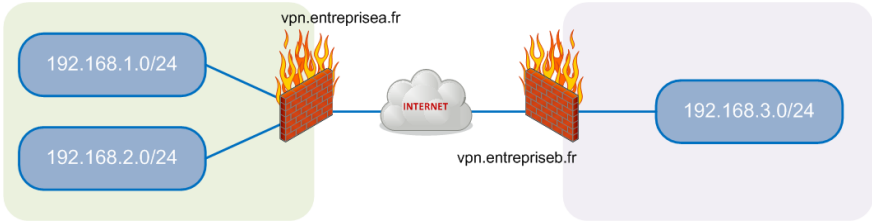


- Exemple de mise en œuvre (Dell Sonicwall)



VPN client-to-site (exemple of dell Sonicwall)





- Entreprise A :
  - Passerelle d'extrémité du tunnel VPN : .....
  - Domaine d'encryption distant : .....
- Entreprise B :
  - Passerelle d'extrémité du tunnel VPN : .....
  - Domaine d'encryption distant : .....

Exercice

- Règles de filtrage
  - Entreprise A :

Source	Destination	Port source	Port destination	Action	Commentaire
*	*	*	*	DENY	Bloque tout

  - Entreprise B :

Source	Destination	Port source	Port destination	Action	Commentaire
*	*	*	*	DENY	Bloque tout