Jean Saquet – Université de Caen

Master e-secure

Sécurité réseaux

VPNs

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

VPNs - Principes

But : établir une liaison entre deux sites, ou une machine et un site, avec des possibilités identiques à celles qui seraient activées si tout était dans le même site, alors qu'en fait les échanges traversent un autre réseau, le plus souvent public.

Diverses solutions :

- PPTP, L2TP
- IPSEC (cf. cours spécifique)
- OpenVPN
- ...

PPTP

Solution « Microsoft »
- Lien client/serveur établi par une connexion TCP de commande (port 1723)
- échanges de données par encapsulation de trames PPP, elles mêmes transportant les paquets IP originaux

Authentification et encryption utilisent les mécanismes standards de PPP, ou une version plus évoluée.

Protocole « standard » de Windows, il existe des clients/ serveurs pour Linux et un client pour Mac

L2TP

Protocole d'origine CISCO
Encapsule également une trame PPP dans sa version d'origine,
Puis toute trame de niveau 2 dans la version 3
L'objectif est d'encapsuler une liaison de niveau 2 dans un réseau à commutation de paquets (IP ou autres).
Le protocole distingue les messages de contrôle et les messages de données.
L2TP peut être utilisé directement au dessus de IP ou sur UDP.
L'échange de données peut être sécurisé par IPSEC

OpenVPN - présentation

Solution open-source très répandue, s'utilise au dessus de UDP ou TCP.
Modèle client/serveur, compatible avec les Nats.
Utilise SSL pour crypter les échanges.
Disponible sous de nombreux systèmes.
Authentification possible par clé partagée, logins et mots de passe, ou certificats.
Port par défaut 1194, mais peut utiliser tout autre port, utile pour passer les firewalls (ex : port 443 de https).

OpenVPN – principes (1)

OpenVPN établit une connexion UDP ou TCP entre client et serveur. Les datagrammes ou segments transporteront des données chiffrées pour éviter l'interception par des tiers.

OpenVPN permet d'établir un réseau virtuel comprenant le client et un réseau, ou 2 réseaux, au dessus du réseau public.

Ce réseau virtuel sera de niveau 2 ou 3, voir ci-dessous

OpenVPN – principes (2)

OpenVPN peut définir le réseau virtuel à deux niveaux :

- niveau 3 (IP) en utilisant une liaison point-à-point entre client et serveur (interface de type « tun »).
- niveau 2 en établissant un pont « Ethernet » entre client et serveur (interface de type « tap »).

Dans le premier cas, la mise en place d'un routage IP approprié permettra l'utilisation. Dans le second cas, client et serveur feront partie du même réseau virtuel physique.

OpenVPN – certificats

OpenVPN peut s'utiliser avec un secret partagé, mais le mieux est d'utiliser les certificats.

Il faut donc générer un certificat pour le serveur, et un pour chaque client.

Pour que chacun vérifie la validité de ces certificats, on utilise en général un certificat de l'autorité (ca.crt)

Les certificats des clients peuvent être générés au niveau du serveur et distribués , ou bien au niveau de chaque client et signés par le serveur.

OpenVPN – paramètres

Outre le mode tun ou le mode tap, et les certificats, OpenVPN va utiliser :

- TCP ou UDP
- le port du serveur
- l'IP ou le FQDN du serveur
- les paramètres pour Diffie-Helmann (taille des nbs premiers notamment)
- la compression utilisée.

OpenVPN – mise en œuvre(1)

Sur le serveur :
- création d'une autorité de certification
- génération du certificat du serveur
- création des paramètres Diffie-Hellman
- édition du fichier de configuration

- génération du ou des certificats clients

OU

- signature des certificats générés par les clients

OpenVPN – mise en œuvre(2)

Sur le client :
- récupération du certificat de l'autorité
récupération du certificat du client :
- généré par le serveur
OU
- généré par le client et signé par le serveur

- édition du fichier de configuration

OpenVPN – mise en œuvre(3)

Il reste éventuellement à :

- configurer les adresses IP ou au moins l'adresse réseau et son masque
- forcer des routes
- utiliser dhcp et indiquer l'adresse du DNS

Ces derniers points sont importants pour permettre à la fois la connexion en VPN à l'entreprise mais garder la route par défaut pour le reste.

OpenVPN – mise en œuvre(4)

L' adresse IP du client peut être distribuée par un DHCP incorporé au serveur OpenVPN. Il suffit de spécifier adresse réseau et masque.

Une option permet également de distribuer une adresse de DNS interne à l'entreprise, indispensable pour obtenir les adresses des machines privées.

Le serveur peut également «pousser des routes » pour la table de routage du client.

cf. exemples ci-dessous.

OpenVPN – exemple 1

VPN du département pour les enseignants
Vpn.info.unicaen.fr-TCP-443

Explication du routage et du DNS

Démo

Et V6 ?

OpenVPN – exemple 2

Réseau de TP

cf. texte du TP

OpenVPN – exercice

Connexion de deux réseaux :

On ne désire plus connecter seulement une machine, mais un réseau voire un inter-réseau privé à un autre réseau d'entreprise .
Utilité : relier 2 sites d'une même entreprise, fusion de deux entreprises.
Comment faire ? (avec OpenVPN et outils classiques)

VPNs – Conclusion

Plusieurs Solutions

OpenVPN facile à mettre en œuvre, passe les Nats, donc très utile pour Ipv4.

IPSEC plus difficile, mais plus adapté à IPv6, agit uniquement sur la couche 3 donc ne perturbe pas le modèle en couches.

PPTP, L2TP solutions plus propriétaires ou plus adaptées à certaines configurations.