

Les VPN

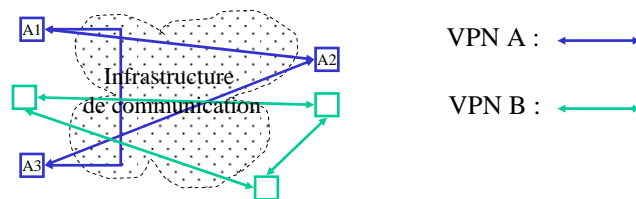
Bernard Cousin

Plan

- Présentation des VPN
- VPN de niveau 3
 - (IPsec)
- VPN de niveau 2
 - PPTP
 - GRE
 - (PPP)
- Conclusion
- VLAN

Rôle des VPN

- Un "Virtual Private Network" :
 - Réseau :
 - Un réseau numérique de télécommunication
 - Privée
 - Qui interconnecte les sites, réseaux locaux ou ordinateurs distants appartenant à un même organisme (et seulement ceux-ci)
 - Virtuel
 - Grâce à des liaisons virtuelles qui s'appuient sur une **infrastructure de communication sous-jacente**



1er décembre 2008

Virtual Private Network

3

Les services des VPN

- Les services des VPN
 - Un VPN rend un service d'interconnexion à grande distance de qualité similaire à un réseau local
 - Fiabilité, disponibilité, performance
 - Sécurité
 - Faible coût car l'infrastructure est partagée
 - Le service offert par le fournisseur de VPN à l'utilisateur du VPN est défini contractuellement

1er décembre 2008

Virtual Private Network

4

Infrastructure sous-jacente

- L'infrastructure sous-jacente peut être :
 - Un réseau international à accès publique
 - Une partie d'un réseau dédié
- Historiquement en France
 - Liaisons spécialisées
 - Réseaux téléphoniques
 - X.25
 - Frame Relay
 - Numéris (ISDN)
 - ATM (B-ISDN)
- Aujourd'hui
 - MPLS
 - Internet

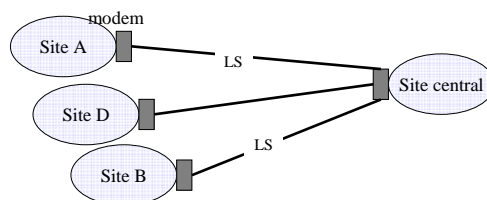
1er décembre 2008

Virtual Private Network

5

La préhistoire des VPN

- Réseaux privées
 - A base de liaisons numériques spécialisées (LS) louées à un opérateur
 - Le coût est fixe
 - Une liaison permet la transmission d'un signal quelconque
 - Le signal transmis doit être compris dans la bande de fréquence négociée mais le débit peu être important (par ex. T1 : 1,5 Mbit/s)
 - Mais l'ajout d'une liaison
 - Limitée par la couverture de l'opérateur
 - Requier un délai très important
 - L'établissement de la liaison est manuel



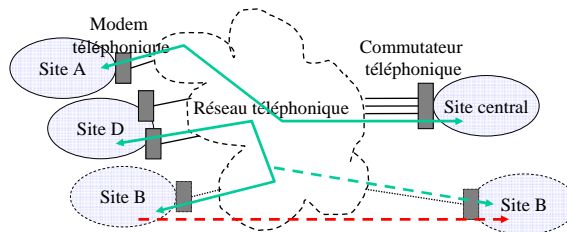
1er décembre 2008

Virtual Private Network

6

L'histoire des VPN : le téléphone

- Utilisation du réseau téléphonique
 - Couverture mondiale et très dense
 - Composition automatique de numéro
 - À partir de n'importe quel point d'accès au téléphone
 - Grande mobilité
- Mais
 - Le débit par ligne est limité (64 kbit/s)
 - La gestion de multiples lignes sur un même site est complexe
 - Le coût dépend de la durée des connexions



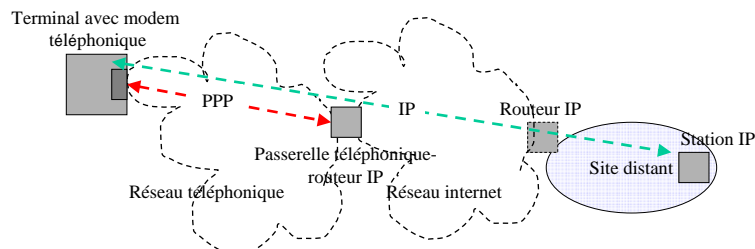
1er décembre 2008

Virtual Private Network

7

Le téléphone et IP

- L'internet utilise le réseau téléphonique
 - PPP est utilisé sur la liaison téléphonique
 - Le paquet IP est encapsulé dans la trame PPP
 - Une passerelle fait l'interface entre réseau téléphonique et IP
 - La passerelle de l'ISP est locale
 - Le coût est celui d'une communication téléphonique locale
 - La passerelle peut être localisée au sein du site du client
 - Ce principe est repris pour l'ADSL : modem ADSL/passerelle ADSL



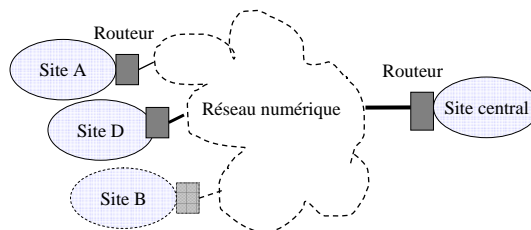
1er décembre 2008

Virtual Private Network

8

L'histoire des VPN : les réseaux numériques

- Utilisation de réseaux numériques
 - Par ex. X.25, Frame Relay, ISDN, ATM, etc.
 - Le débit peut être adapté aux besoins, les connexions sont établies automatiquement
- Mais
 - Couverture variable et peu dense
 - Équipements d'interconnexion spécialisés
 - Le coût dépend du volume des données transmises



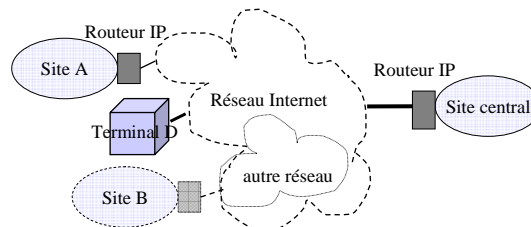
1er décembre 2008

Virtual Private Network

9

L'histoire des VPN : l'Internet

- Utilisation de l'internet
 - Le débit peut être adapté aux besoins, les connexions sont établies automatiquement, le coût est très faible
 - L'interconnexion peut être réalisé en s'appuyant sur n'importe quel autre réseau numérique (par ex. téléphonique)
 - L'interconnexion est totale
- Mais
 - La protection des données transmises n'est pas assurée
 - La protection des sites n'est pas assurée



1er décembre 2008

Virtual Private Network

10

La sécurisation des VPN de l'Internet

- Il faut déployer un système de sécurité
 - Protéger les sites
 - Protéger les communications inter-sites
 - Autoriser les accès distants aux services extranet
 - Par n'importe qui
 - Autoriser les accès licites distants aux services intranet
 - À partir de potentiellement n'importe où (terminaux mobiles)

La sécurisation des VPN

- On peut déployer un système de sécurité
 - Au niveau 2
 - Par ex. PPTP ou L2TP
 - Au niveau 3
 - Par ex. IPsec
 - Cf. chapitre correspondant
 - Au niveau 4
 - Par ex. SSL ou TLS
 - Cf. chapitre correspondant
 - Au niveau applicatif
 - Par ex. ssh

La sécurisation des VPN pour et par Internet

- La sécurisation de l'Internet
 - Transmission sûre des données
 - Par ex. IPsec
 - Cf. polycopié sur IPsec
 - Filtrage des communications
 - Firewall
 - Distribution des clefs
 - IKE, PKI
 - Cf. polycopié
 - Contrôle d'accès, authentification
 - Radius
 - Certification X.509
 - "Lightweight Directory Access Protocol"
 - Etc.

La sécurisation du niveau 2 par tunnels

- Les protocoles de "tunnelling" de niveau 2
 - Point to Point Tunneling Protocol
 - Conçu par Microsoft
 - Remplacé par L2TP
 - Layer 2 Forwarding
 - Protocole Cisco
 - Remplacé par L2TP
 - Layer 2 Tunneling Protocol
 - Transport de session PPP au-dessus de réseaux tels que l'Internet, Frame Relay, X.25 ou ATM
 - Pour l'Internet cela se passe au-dessus de IP+UDP

PPTP

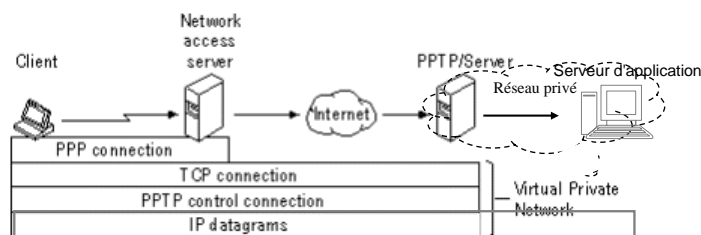
- PPTP permet d'implémenter les VPN point à point
 - PPTP est une extension de PPP
 - PPP permet d'utiliser le réseau téléphonique public comme réseau d'accès
 - PPP permet de transporter en point à point des paquets IP, IPX, NetBEUI, NetBIOS, etc.
 - PPTP permet d'encapsuler et de transmettre (c.-à-d. de "tunneller") des trames PPP sur un réseau IP
 - Utilise l'Internet comme réseau de distribution
 - Il n'offre pas service de sécurité
 - Le protocole tunnelé (par ex. PPP) doit fournir ce service
 - Compatible RFC 2637 ("not an IETF standard"), 1999
- Proposé par Microsoft (présent par défaut dans les OS Windows)

Les canaux de communication de PPTP

- Le protocole PPTP ouvre deux canaux de communication entre le client PPTP et le serveur PPTP:
 - Une connexion de contrôle du tunnel PPTP
 - Connexion TCP sur port 1723
 - Le tunnel PPTP
 - Un canal de données pour les trames PPP (pouvant être sécurisées)
 - Utilisant GRE ("Generic Routing Encapsulation") vers transiter sur IP

Scénario typique de PPTP

- Les principaux acteurs
 - Le client PPP, PPTP et d'application
 - Le serveur d'accès à l'Internet (NAS)
 - Le serveur PPTP
 - Le réseau privé
 - Le serveur d'application
- Les différentes phases
 - Établissement de la connexion PPP sur le réseau téléphonique
 - Connexion à l'Internet
 - Établissement de la connexion TCP vers le serveur PPTP
 - Établissement de la connexion de contrôle PPTP et configuration du tunnel sécurisé
 - Transport sécurisé des données sur le tunnel PPTP vers le serveur d'application



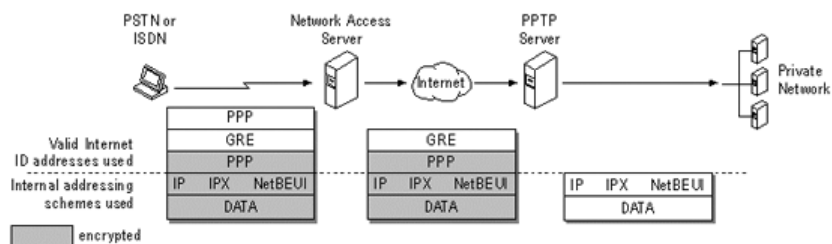
1er décembre 2008

Virtual Private Network

17

Le protocole PPP dans PPTP

- Le protocole PPP est utilisé
 1. Sur le liaison d'accès
 - S'il y a un réseau téléphonique entre le client PPTP et le RAS
 2. Comme protocole de tunnel VPN
 - Entre le client PPTP et le serveur PPTP
 - Pour transporter n'importe quel paquet protocolaire du client vers le réseau privée



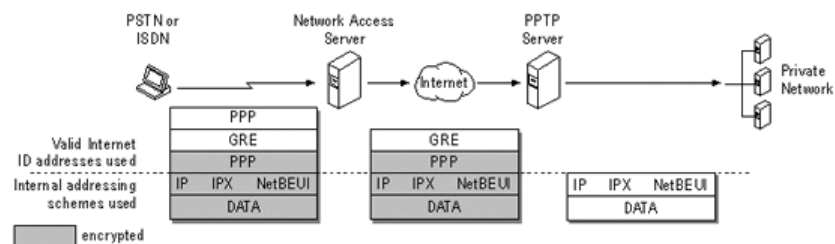
1er décembre 2008

Virtual Private Network

18

Adressage et encapsulation dans PPTP

- Un adressage non routable (adresse privée) peut être utilisé par le client et le réseau privé



1er décembre 2008

Virtual Private Network

19

Phase d'établissement de connexion PPP au-dessus du réseau téléphonique

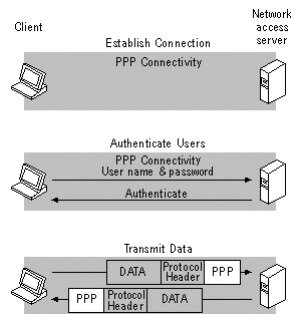
- Les sessions PPTP sont démarrées par un client appelant le serveur d'accès à l'internet d'un ISP.
- Le protocole PPP (RFC 1661)
 - est utilisé pour créer la connexion au-dessus du réseau téléphonique entre le client et le serveur d'accès à l'internet
 - Etablit et maintient des connexions PPP entre des ordinateurs distants.
 - Authentification des utilisateurs par l'ISP. Les clients PPTP sont authentifiés en utilisant le protocole PPP. Du texte en clair, crypté ou l'authentification cryptée de Microsoft peuvent être utilisés par le protocole PPP.
 - Transmission des trames PPP un client et le serveur d'accès réseau (il peut être sécurisé).

1er décembre 2008

Virtual Private Network

20

Phase d'établissement de connexion PPP au-dessus du réseau téléphonique



1er décembre 2008

Virtual Private Network

21

La connexion TCP

- Une connexion TCP est créée entre le client et le serveur PPTP
 - Pour établir une connexion de contrôle pour PPTP
 - Sur port 1723

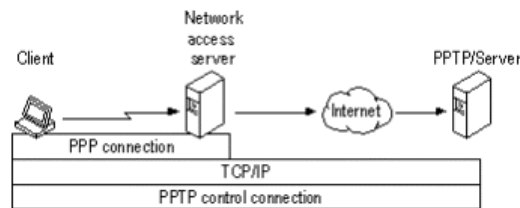
1er décembre 2008

Virtual Private Network

22

La connexion de contrôle de PPTP

- Connexion de contrôle est établie entre le client PPTP et le serveur PPTP
 - Au sein d'une connexion TCP
 - Établissement et contrôle du tunnel PPTP



- Ici le terminal est le client PPTP. Cela peut-être le NAS si le client n'est pas PPTP et si son ISP fournit un service PPTP

Les messages de contrôle de PPTP

- PPTP utilise les messages de contrôle suivants :
 - PPTP_START_SESSION_REQUEST Etablissement d'une session
 - PPTP_START_SESSION_REPLY Confirmation d'établissement d'une session
 - PPTP_ECHO_REQUEST Requête de maintien de la session
 - PPTP_ECHO_REPLY Réponse à une requête de maintien de session
 - PPTP_WAN_ERROR_NOTIFY Notifie une erreur dans la connexion PPP
 - PPTP_SET_LINK_INFO Configure la connexion
 - PPTP_STOP_SESSION_REQUEST Termine la session
 - PPTP_STOP_SESSION_REPLY Réponse à la requête de fin de session

Phase d'établissement du tunnel PPP

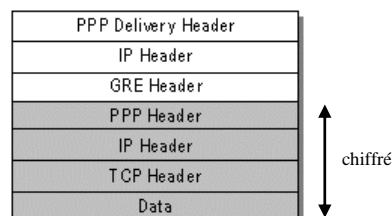
- Le protocole PPP est utilisé pour créer la connexion sécurisée entre le client et le serveur PPTP
 - Le protocole PPP établit et maintient des connexions PPP entre des ordinateurs distants.
 - Authentification des utilisateurs
Les clients PPTP sont authentifiés en utilisant le protocole PPP. Du texte en clair, crypté ou l'authentification cryptée de Microsoft peuvent être utilisés par le protocole PPP.
 - Transmettre des datagrammes PPP qui contiennent des paquets cryptés IPX, NetBEUI ou TCP/IP
Parce que les paquets sont cryptés, tout le trafic entre un client PPP et le serveur PPTP est sécurisé.

Transmission des données

- Les données sont transmises, une fois le tunnel PPTP établi
 - Les données d'application sont transmises par n'importe quel empilement protocolaire compatible avec le réseau privé,
 - Par ex. dans des segments TCP dans des datagrammes IP.
 - encapsulées dans des trames PPP
 - Qui mettent en œuvre une transmission sécurisée
 - Ces trames PPP sont placés dans des paquets IP et traversent l'internet
 - grâce à une version modifiée du protocole Generic Routing Encapsulation (GRE) (RFC 1701 et 1702).

Ou n'importe quel protocole LdD
approprié aux réseau d'accès puis
de transit

Dépend du réseau privé



Conclusion pour PPTP

- PPTP franchit difficilement les "firewalls"
 - À cause du double canal
- PPTP peut-être authentifier grâce à
 - MS-Chap2
 - Basé sur le mot de passe
 - attention aux mots de passe mal choisis
 - Peut utiliser MD4
 - EAP-TLS
 - Utilise des certificats
- PPTP peut être protéger grâce à
 - Microsoft Point-to-Point Encryption (RFC 3078)
 - PPTP ne permet pas le multipoint

1er décembre 2008

Virtual Private Network

27

GRE

- Le protocole GRE est utilisé
 - Pour encapsuler les paquets de toute sorte dans des paquets de transport
 - Ici, pour les VPN PPTP
 - Pour encapsuler des trames PPP dans des paquets IP
 - Pour leur faire traverser un tunnel point à point
 - Ici, pour traverser l'Internet au sein d'un tunnel PPTP
 - GRE offre un contrôle de flux et de congestion
 - RFC 2787, 2890, compatible avec PPTP et L2TP

```
+-----+
| En-tête IP                               |
+-----+
| En-tête GRE                               |
+-----+
| En-tête PPP                               |
+-----+
| Chargement PPP crypté                     |
+-----+
```

1er décembre 2008

Virtual Private Network

28

Paquet GRE

- Entête de paquet GRE

0				1				2				3									
0	1	2	3	4	5	6	7	8	9	0	1	2	3	4	5	6	7	8	9	0	1
C R K S s Recur A				Indicateurs				Ver				Type de protocole									
Contrôle d'erreur (facultatif)								Offset (facultatif)													
Clé (HW) Longueur du chargement				Clé (LW) ID du flux																	
								Numéro de séquence (facultatif)													
								Numéro d'accusé de réception (facultatif)													
								Routing (facultatif)													

Les champs et paramètres de GRE

C	(Bit 0) Champ de contrôle présent. Initialisée à zéro (0).
R	(Bit 1) Champ offset présent. Initialisé à zéro (0).
K	(Bit 2) Clé présente. Initialisée à un (1).
S	(Bit 3) No de séquence présent. Initialisé à 1 si un paquet de chargement (données) est présent. Initialisé à zéro (0) si un chargement n'est pas présent (le paquet GRE est en mode accusé de réception seulement).
s	(Bit 4) Routage strict par la source présent. Init. à 0.
Recur	(Bits 5-7) Nombre d'encapsulation permises. Init. à zéro.
A	(Bit 8) Numéro d'accusé de réception présent. Initialisé à un (1) pour connaître les données correctement transmises.
Checksum	Standard IP checksum
Offset	L'entrée active pour le Source Routing
Type de protocole	0x880B pour PPP, 0x800 pour IP, etc.

Les champs des paquets GRE

Clé (HW) Longueur du chargement	(2 octets) Champ Key : Taille du chargement, non compris l'en-tête de GRE.
Clé (LW) Appel ID	(2 octets bas) Champ Key: ID du flux auquel appartient ce paquet .
Numéro de séquence	Contient le numéro de séquences du paquet. Présent si le bit S (Bit 3) est un (1).
N° d'accusé de réception	Contient le numéro de l'accusé de réception du paquet le plus élevé reçu par l'homologue expéditeur pour cette session. Présent si le bit A (bit 8) est un (1).
Routing	une liste d'entrées pour le Source Routing

PPP

- Cf. Chapitre 2 de la partie "Internet et les liaisons" du polycopié "Réseaux Locaux".

Conclusion

- Le service de VPN peut être offert par le fournisseur d'accès ou bien par le client et/ou son réseau privé d'entreprise
 - Le serveur de VPN est propriété et géré
 - Soit par le fournisseur, soit par l'entreprise
 - Le terminal du client est
 - Soit muni de l'environnement nécessaire à la gestion du VPN ou bien son ISP lui offre ce service.

Bibliographie

- C. Scott, P. Wolfe, M. Erwin, "Virtual Private Networks", O'Reilly, 1999.
- Support Microsoft

VLAN

- Virtual LAN
 - Plusieurs réseaux locaux sont interconnectés via the IEEE 802.11Q
 - L'agrégation ("trunking") et la séparation du trafic
 - S'appuie sur le pontage
 - La gestion de priorités est possible
 - Cf. chap. 7 de la partie Ethernet du poly Réseaux locaux

 - D'autres techniques équivalentes
 - ATM LAN Emulation (LANE)
 - Cisco Inter-Switch Link (ISL)