

Configuration de la liaison VPN

Sommaire

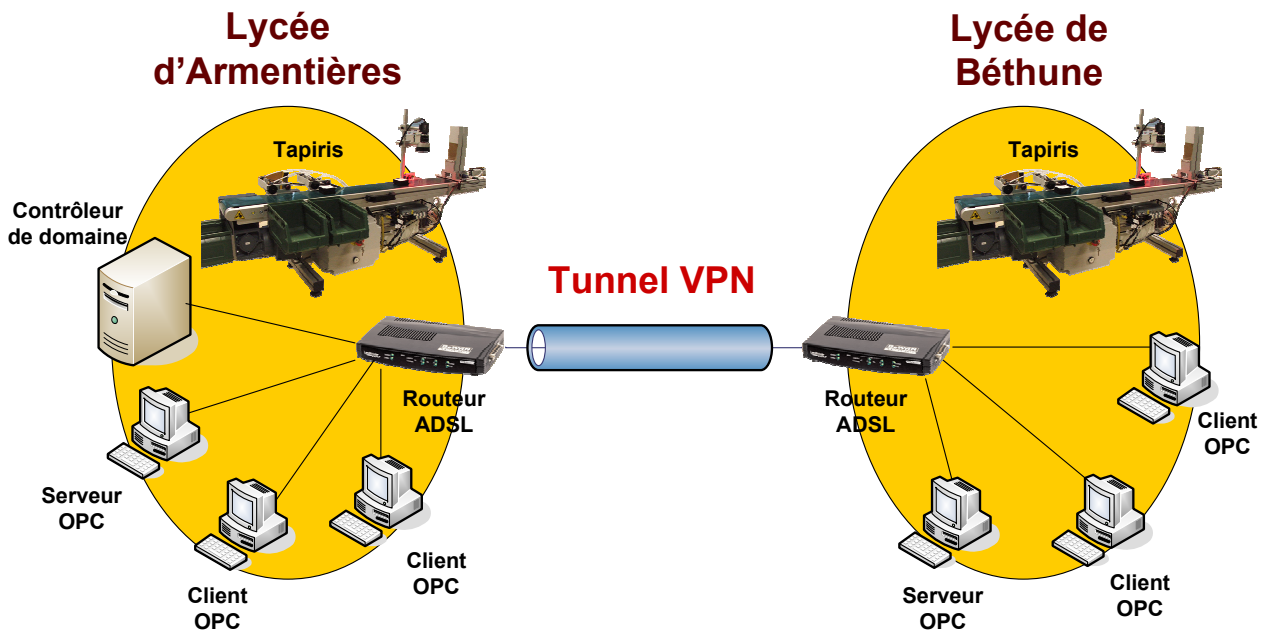
1.	Présentation du besoin	2
2.	Présentation du VPN	2
3.	Interconnexion des réseaux d'Armentières et Béthune : « Mode Tunnel »	3
3.1.	Méthode et matériels utilisés.....	3
3.2.	Paramétrage du routeur BEWAN d'Armentières.....	3
3.2.1.	Paramétrage de la clé IKE / IPSec	3
3.2.2.	Paramétrage de l'interconnexion des réseaux	4
3.3.	Paramétrage du routeur BEWAN de Béthune	5
3.3.1.	Paramétrage de la clé IKE / IPSec	5
3.3.2.	Paramétrage de l'interconnexion des réseaux	6
4.	Validation de l'interconnexion de réseau.....	6
4.1.	Visualisation de l'état de la connexion VPN.....	6
4.2.	Tests de validation	7
5.	Evolutions envisagées	7

1. Présentation du besoin

Dans le cadre du projet de BTS iris entre les sections de Béthune et d'Armentières, nous avons configuré l'interconnexion de nos deux réseaux via internet.

Pour sécuriser cette interconnexion, nous avons mis en œuvre une liaison VPN entre les deux sites. Cette liaison est réalisée par deux routeurs ADSL Bewan LanBooster 2104P.

D'autre part, l'utilisation des applications OPC demande d'avoir une base utilisateurs commune. Nous avons choisi de gérer les utilisateurs de manière unique sur un contrôleur de domaine Windows 2003 Server d'Armentières.



2. Présentation du VPN

Le VPN (Virtual Private Network) est une liaison sécurisée entre 2 sites d'une organisation via un réseau public, en général Internet. Il vous permet d'envoyer et de partager des données ou des ressources entre des sites distants.

Les réseaux privés virtuels (VPN) permettent à l'utilisateur de créer un chemin virtuel sécurisé entre une source et une destination. Grâce à un principe de tunnel (tunnelling) dont chaque extrémité est identifiée, les données transitent après avoir été chiffrées. C'est la méthode utilisée pour faire transiter des informations privées sur un réseau public. Cette technique assure donc l'authentification des 2 parties, l'intégrité des données et le chiffrement de celles-ci.

Pour communiquer au travers du VPN, plusieurs protocoles peuvent être utilisés : le PPTP (Point to Point Tunneling Protocol), le protocole L2TP (Layer 2 Tunneling Protocol) et enfin le protocole IPSec.

Il existe deux modes de VPN distincts :

- **le Mode Tunnel** : il crée des tunnels en encapsulant chaque trame dans une enveloppe qui protège tous les champs de la trame. Il est utilisé entre 2 équipements gérant l'interconnexion (exemple : la connexion VPN entre deux routeurs ou passerelles). Les données peuvent être chiffrées (mode ESP) ou non (mode AH).
- **le Mode Transport** : il protège le contenu d'une trame IP en ignorant l'en-tête. Ce mode est généralement utilisé entre deux équipements dont au moins un de type terminal (exemple : la connexion VPN d'un utilisateur isolé 'SOHO' vers une passerelle ou un routeur).

En fonction du mode VPN choisi et du protocole de connexion sélectionné, différentes configurations sont possibles. Tout d'abord, en préalable pour que la connexion VPN puisse s'établir, il est nécessaire que les administrateurs des 2 sites distants s'échangent leurs paramètres de connexion (nom d'utilisateur, mot de passe, numéro à composer ou nom d'hôte ou adresse IP du serveur, voire clé IPSec...).

3. Interconnexion des réseaux d'Armentières et Béthune : « Mode Tunnel »

3.1. Méthode et matériels utilisés

Pour interconnecter les deux réseaux nous utilisons le « Mode Tunnel » entre les deux routeurs BEWAN LanBooster 2104P et nous avons créé un tunnel VPN IPSec.

Pour ces routeurs, le routage nécessaire pour l'interconnexion des deux réseaux est activé en même temps que la configuration du tunnel VPN. Evidemment, il faut configurer les passerelles par défaut de toutes les machines pour qu'elles pointent vers l'adresse IP locale du routeur.

	Routeur Armentières	Routeur Béthune
Nom du domaine	ARMBET	ARMBET
Adresse IP locale du routeur	192.168.33.1	192.168.22.1
Adresse réseau du LAN	192.168.33.0	192.168.22.0
Adresse IP publique	193.152.XX.YY	83.192.WW.ZZ
Clé IKE sortante	CleA	CleB
Clé IKE entrante	CleB	CleA

3.2. Paramétrage du routeur BEWAN d'Armentières

3.2.1. Paramétrage de la clé IKE / IPSec

Dans l'interface web d'administration du routeur, choisissez :

Menu principal > Paramétrage des accès distants et RPV (VPN) > Paramétrage IKE / IPSec

BeWAN systems Configurateur Web du LanBooster 2104 P

> Installation Avancée > Paramétrage des accès distants et RPV (VPN) << Menu principal

Configuration de l'appel entrant << Page précédente

Méthode d'authentification IKE

Clé de partage: CleB

Confirmation de la clé de partage:

Méthode de sécurité IPSec

Moyenne (AH)
Les données sont authentiques, mais peuvent ne pas être cryptées.

Haute (ESP) DES

Annuler OK

Dans un premier temps, vous pouvez choisir une méthode de sécurité moyenne (AH) et après validation du fonctionnement du tunnel, il est conseillé d'augmenter la sécurité (ESP)

3.2.2. Paramétrage de l'interconnexion des réseaux

Dans l'interface web d'administration du routeur, choisissez :
Menu principal > Paramétrage des accès distants et RPV (VPN) > Paramétrage d'interconnexion de réseaux

BeWAN systems Configurateur Web du LanBooster 2104 P
 > Installation Avancée > Paramétrage des accès distants et RPV (VPN) << Menu principal

Profils d'interconnexion de réseaux << Page précédente | Effacer tous les profils |

Numéro	Nom	Etat	Numéro	Nom	Etat
1.	???	x	9.	???	x
2.	???	x	10.	???	x
3.	???	x	11.	???	x
4.	vpn_ipsec	v	12.	???	x
5.	???	x			
6.	???	x			
7.	???	x			
8.	???	x	16.	???	x

v : Activé x : Désactivé

Création d'un nouveau profil d'interconnexion en cliquant sur un numéro de libre

BeWAN systems Configurateur Web du LanBooster 2104 P
 > Installation Avancée > Paramétrage des accès distants et RPV (VPN) << Menu principal

Profil n° 4 << Page précédente | Effacer |

1. Configuration actuelle

1 Activer ce profil
 Nom du profil:

Sens de l'appel: Entrant/Sortant Entrant Sortant
 Rendre la connexion permanente
 Déconnexion si inactif depuis: seconde(s) 2
 Activer le ping pour garder la connexion active
 Effectuer un ping sur l'IP:

2. Paramètres d'appel sortant

3 Type de serveur appelé:
 PPTP
 Tunnel IPSec
 L2TP avec règle IPSec (aucune)

Nom d'utilisateur:
 Mot de passe:
 Authentification: PAP ou CHAP
 Compression VJ: Activée Désactivée

4 Nom d'hôte ou Adresse IP du router VPN distant:
 (ex : monrouteur.dyndns.org ou 212.23.161.89)

5 - CleA
 Méthode de sécurité IPSec
 Clé de partage IKE:
 Moyenne (AH) Haute (ESP) DES avec authentification

Plages horaires (1-15): : : :

3. Paramètres d'appel entrant

Type d'appel entrant permis

- PPTP
- Tunnel IPSec
- L2TP avec règle IPSec (aucune)

Activer l'authentification

Adresse IP du serveur : 83.192.wv.zz

Nom d'utilisateur : ???

Mot de passe : []

Authentification PPP : PAP ou CHAP

Compression VJ : Activée Désactivée

Méthode de sécurité IPSec

Clé de partage IKE : []

Moyenne (AH)

Haute (ESP) : DES

4. Paramètres TCP/IP de l'interconnexion de réseaux

Mon adresse IP WAN : 193.152.xx.yy

Adresse IP de la passerelle distante : 83.192.wv.zz

Adresse IP du réseau distant : 192.168.22.0

Masque de sous-réseau du réseau distant : 255.255.255.0

Direction du RIP : TX/RX

Version du RIP : Ver. 2

NAT : IP publique

Routage : IP privée

Redéfinir ce tunnel comme route par défaut

OK

Callouts: 6 points to Tunnel IPSec; 7 points to server IP; 8-CleB points to IKE key; 9 points to remote network IP; 10 points to routing type.

3.3. Paramétrage du routeur BEWAN de Béthune

3.3.1. Paramétrage de la clé IKE / IPSec

Dans l'interface web d'administration du routeur, choisissez :

Menu principal > Paramétrage des accès distants et RPV (VPN) > Paramétrage IKE / IPSec

BeWAN systems Configurateur Web du LanBooster 2104 P

> Installation Avancée > Paramétrage des accès distants et RPV (VPN) << Menu principal

Configuration de l'appel entrant << Page précédente

Méthode d'authentification IKE

Clé de partage : []

Confirmation de la clé de partage : []

Méthode de sécurité IPSec

Moyenne (AH)
Les données sont authentiques, mais peuvent ne pas être cryptées.

Haute (ESP) : DES

Annuler OK

CleA

Dans un premier temps, vous pouvez choisir une méthode de sécurité moyenne (AH) et après validation du fonctionnement du tunnel, il est conseillé d'augmenter la sécurité (ESP)

3.3.2. Paramétrage de l'interconnexion des réseaux

Dans l'interface web d'administration du routeur, choisissez :

Menu principal > Paramétrage des accès distants et RPV (VPN) > Paramétrage d'interconnexion de réseaux

Créez un nouveau profil d'interconnexion en cliquant sur un numéro de libre

Remplissez les champs en respectant l'ordre du paragraphe précédent :

1. Activez le profil et donnez lui un nom
2. Appel Entrant / sortant, sans déconnexion
3. Validez le tunnel IPSec
4. Adresse routeur distant = 193.152.xx.yy
5. Clé IKE = CleB ; Sécurité = moyenne
6. Validez le tunnel IPSec
7. Adresse du serveur = 193.152.xx.yy
8. Clé IKE = CleA ; Sécurité = moyenne
9. IP WAN = 83.192.ww.zz ; passerelle distante = 193.152.xx.yy ; réseau distant = 192.168.33.0 /24
10. Adresse IP privée

4. Validation de l'interconnexion de réseau

4.1. Visualisation de l'état de la connexion VPN

Dans l'interface web d'administration d'un des routeurs, choisissez :

Menu principal > Etat de la connexion RPV (VPN)

Exemple pour le routeur d'Armentières :

BeWAN systems Configurateur Web du LanBooster 2104 P

> Administration Système > Etat de la connexion RPV (VPN) << [Menu principal](#)

Choisissez le profil d'interconnexion créé précédemment et cliquez sur Appeler << [Page précédente](#) | [Rafraichir](#) |

Outil de connexion distante Intervalle de rafraîchissement : 10 secondes

(vpn_ipsec) 83.192.ww.zz Appeler

Etat de la connexion RPV (VPN) 1ère page 2nde page

RPV	Type	Adresse IP distante	Réseau virtuel	Paquets TX	Vitesse TX	Paquets RX	Vitesse RX	Connecté depuis	
1 (vpn_ipsec)	Tunnel IPSec AH-Auth MD5	83.192.242.111	192.168.22.0/24	38	9	62	14	0 : 11 : 50	Arrêter

Vérifiez que le Tunnel est actif xxxxxxxx : Données cryptées.
xxxxxxx : Données non cryptées.

Copyright © 2001-2002, BeWAN systems. Tous droits réservés.

4.2. Tests de validation

- Une fois le tunnel activé, vous pouvez vérifier que le routage IP est bien activé aussi en effectuant un PING sur une machine du réseau distant.
- Intégration des machines de Béthune dans le domaine géré par le contrôleur de domaine d'Armentières
- Ouverture de session sur une machine de Béthune avec un login du contrôleur de domaine d'Armentières.
- Accès aux fichiers distants à l'aide de l'explorateur de fichiers
- Test des applications clientes OPC sur le serveur OPC distant (nécessité d'avoir une configuration DCOM identique)

5. Evolutions envisagées

Installation d'un contrôleur de domaine secondaire à Béthune pour pallier aux problèmes de déconnexion internet. Cette solution nous offrirait une plus grande souplesse pour réaliser les TP locaux.