Complément d'architecture de réseau BUS-SOL

DANG Xuan Thong

eRISCS

Marseille, 02/03/2017

PREFACE

L’utilisation du VPN dans le réseau de communication entre les bus et les serveurs SOL est indispensable. Ce dernier permet une communication transparent au niveau transport/application pour tous les noeuds du réseau, peu import où ils sont.

1. Le choix du type de VPN

Il y a deux types du VPN, chacun est basé sur un protocole différent: IPSec et TLS. Le choix de type de VPN dépend donc de mode d'utilisation en considérant les caractéristiques de ces deux protocoles.

La table ci-dessous nous montre une comparaison générale de ces protocoles:

	IPSec tunneling	TLS
Couche	Réseaux (3)	Transport (4)
Connexion	Sans connexion	UDP/TCP
Authentification	Authentication Header (AH)	Public Key Infrastructure (PKI)
Chiffrement	ESP (optionnel)	SSL (optionnel)
Connectivité	Network-to-network, Host-to-network, Host-to-host	Host-to-host

Pour pouvoir déterminer quel type de VPN sera utilisé, on se rappelle les exigences dans ce type de communication BUS-SOL:

	IPSec tunneling	TLS
Mode sans connexion	✅	✅ en utilisant UDP
Confidentialité de bout en bout	✅ (optionnel)	✅ (optionnel)
Reprise rapide de connexion	✅ IKE-v2 resumption	✅ TLS resumption

Les deux types de VPN satisfont parfaitement à nos exigences. Les applications aux couches au-dessus ne sont pas affectées par ce choix de type de VPN.

Néanmoins, il y a encore quelques contraintes économiques à prendre en considération:

	IPSec tunneling	TLS
Installation	❌ dispositif compatible nécessaire	✅ niveau application
Coût de setup et bande passante	❌ chère	✅ pas chère
Maintenance	✅ rarement	❌ gestion de PKI

2. Mise en place du VPN sur architecture BUS-SOL

Le choix du type de VPN reste à la décision de la RTM. Dans la section suivante, on va montrer la mise en place du VPN/TLS sur l'architecture actuelle et quelques améliorations d'utilisation.

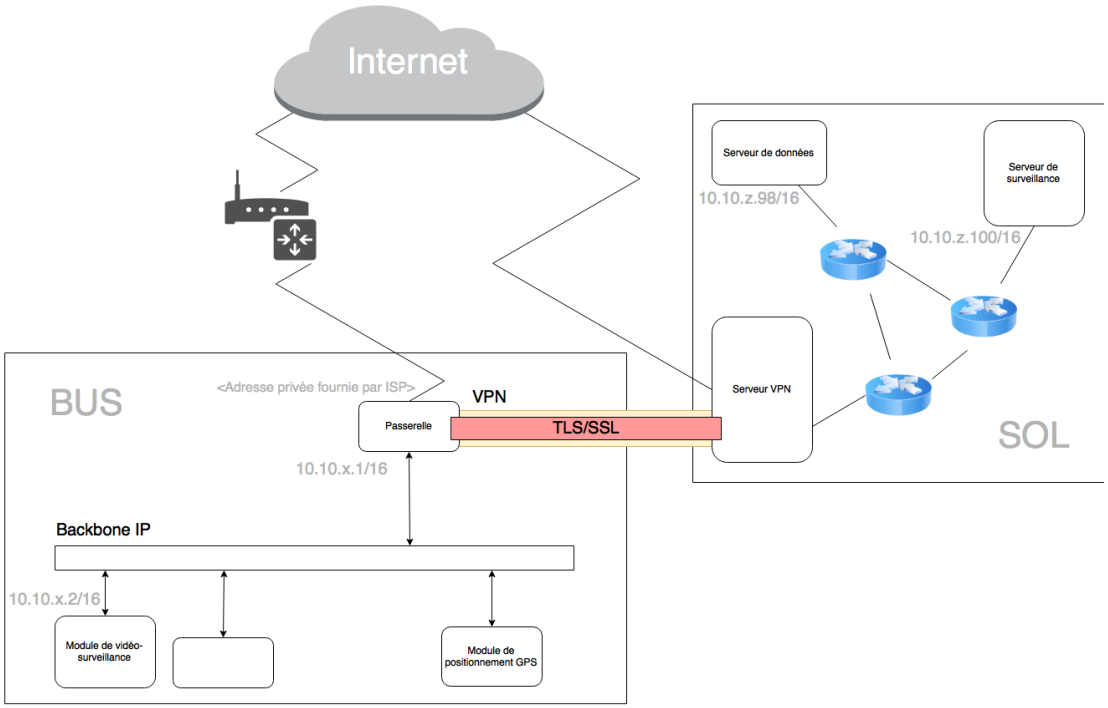

Figure 2.1 - La mise en place du VPN/TLS

Un example de la mise en place du VPN/TLS est trouvé sur Figure 2.1. Dans ce mode d'utilisation, le VPN est utilisé en mode tunnel pour faire passer les paquets entre deux réseaux locaux.
Cependant, ce mode ne protège les données seulement quand elles sont sur Internet. Dès leur entrée au serveur VPN, les données sont déchiffrées et circuler à l'état quand elle sortaient depuis expéditeurs.

Un problème de sécurité apparaît quand un attaquant a l'accès à un des dispositif, il peut facilement écouter ensemble du réseau et propager éventuellement des vers, malgré la configuration du pare-feu.

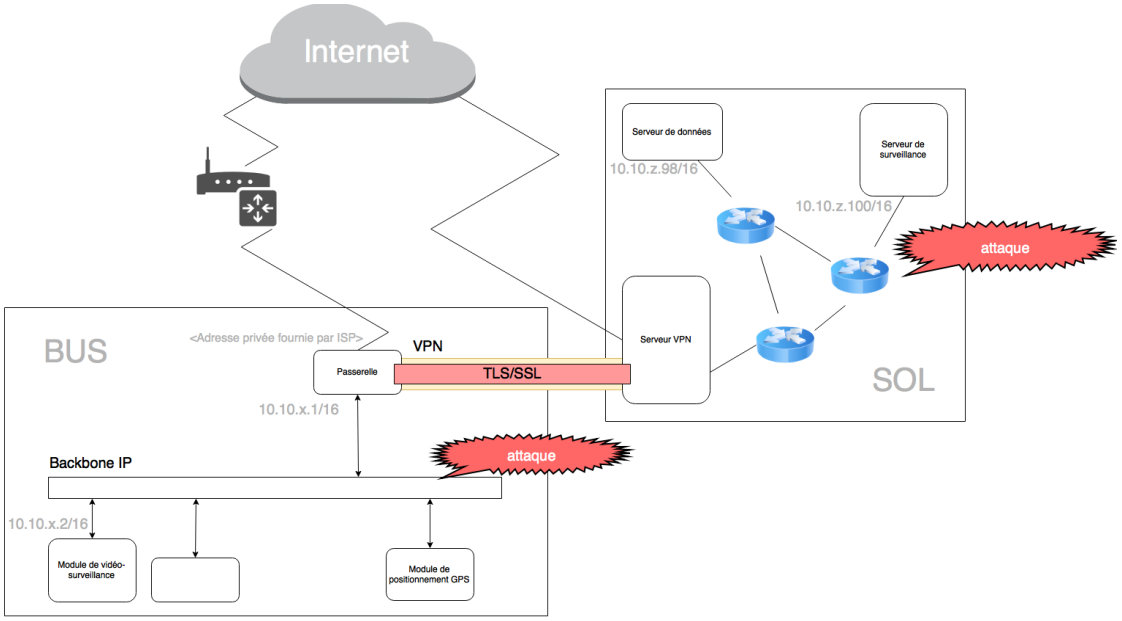

Figure 2.2 - Des vecteurs d'attaque possible dans une configuration par défaut

Une solution pour ce problème est de chiffrer encore les données envoyées depuis l'expéditeur, en utilisant au-dessus de VPN une connexion sécurisée (TLS par example). Comme ça les données seront protégées même si elles sont capturées dans le réseau locale. Pourtant, cette approche double l'effort de chiffrement, gaspiller des ressources. D'ailleurs, les protocoles supplémentaires utilisés dans ce cas-là ne supportent pas multicast.

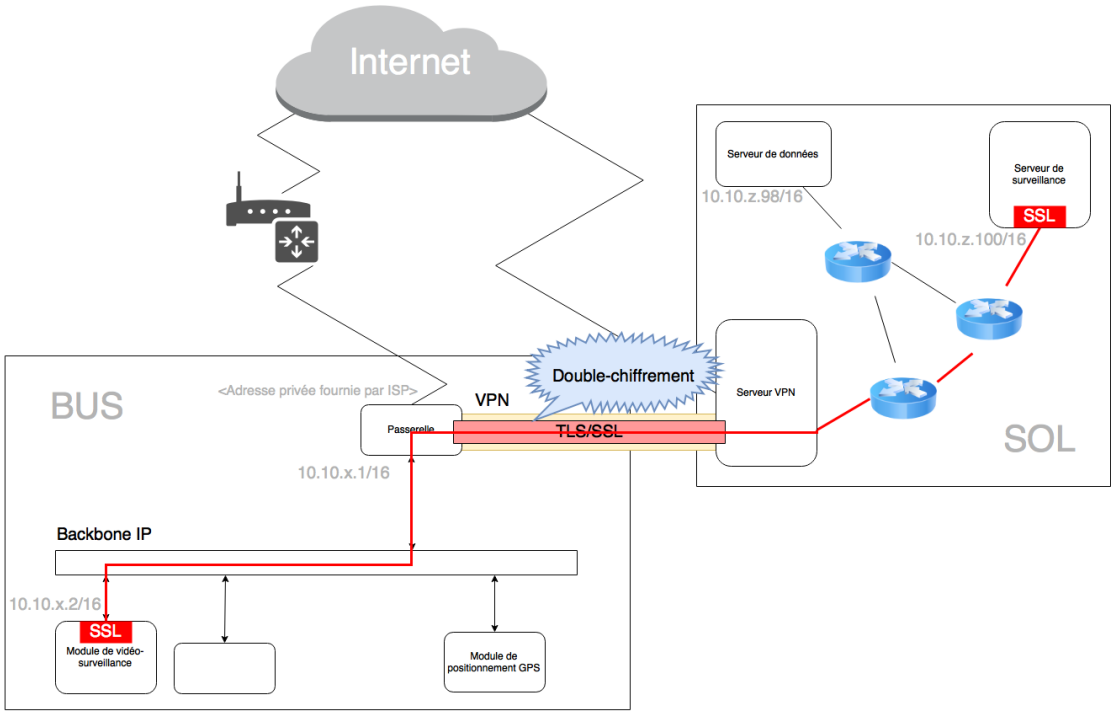

Figure 2.3 Utilisation d'une connexion SSL double l'effort de chiffrement

Notre proposition est d'enlever le chiffrement VPN, garantir seulement l'intégrité et l'authenticité. Cette configuration peut être obtenue en définissant "cipher --none" dans le fichier de configuration du OpenVPN. Pour pouvoir assurer la confidentialité, on utilise SVC au-dessus de ce VPN. SVC fonctionne sans connexion, permet le multicast et offrir une interface de chiffrement ouverte. Dans cette configuration, le double-chiffrement est éliminé, la confidentialité est assurée de bout en bout.

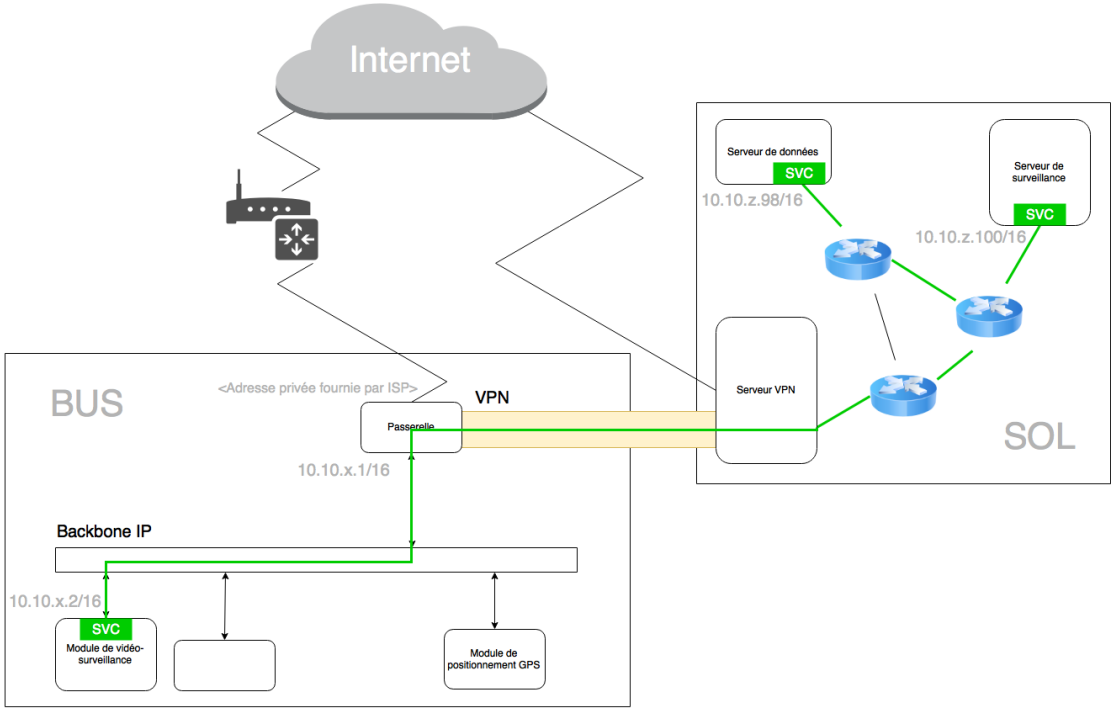

Figure 2.4 - Utilisation du SVC au-dessus de VPN