

### Situation 7 : Mise en place de tunnels VPN

#### Fiche Stormshield associée :

- Fiche 10 – Utilisateurs et authentification
- Fiche 11 – Infrastructures à clés publiques
- **Fiche 12 – VPN**

Le DSI souhaite, dans un premier temps, permettre l'accès au réseau local de l'agence à des employés lorsqu'ils sont en déplacement. La mise en place d'un VPN SSL est envisagé. Dans un second temps, votre responsable souhaite tester la possibilité d'interconnecter deux agences à l'aide d'un tunnel VPN connecté à travers le réseau WAN public.

## I Généralités

1. Définir ce qu'est un VPN (Virtual Private Network) et ce qu'il garantit. Pourquoi est-il recommandé de mettre en place une solution de ce type lorsque l'on souhaite offrir un accès distant à un réseau interne d'entreprise ?
2. Pourquoi le VPN est-il un élément critique en matière de sécurité informatique ?
3. Après le visionnage de la conférence de l'ANSSI à propos de l'attaque de l'entreprise TV5 Monde, expliquer comment l'attaquant a pu utiliser ce service pour atteindre ses objectifs.
4. Proposer des bonnes pratiques quant à l'usage de ce service.
5. Quelles sont les différences entre un VPN SSL et un VPN IPSec ? Pourquoi le VPN IPSec est-il davantage recommandé ?

## II Création d'un accès VPN SSL/TLS pour les clients nomades

Chaque utilisateur souhaitant utiliser le VPN SSL doit disposer d'un compte d'annuaire (soit Active Directory, soit interne au pare-feu).

- Les membres du groupe informatique auront accès à l'ensemble du réseau local.
- Les membres du groupe production auront uniquement accès au sous-réseau production ainsi qu'un accès Internet par le biais du VPN.

Une fois le service correctement configuré, les utilisateurs concernés pourront récupérer après authentification leur fichier de configuration sur le portail captif du pare-feu actif sur l'interface externe. Le client VPN SSL utilisé peut être celui fourni par Stormshield ou par OpenVPN. Pour cela :

6. Configurer le service VPN SSL sur le pare-feu. *Ne pas oublier d'ajouter les règles nécessaires pour respecter les contraintes.*



Les réseaux assignés aux clients UDP et TCP seront respectivement du type (où X est votre numéro de plateforme) :

- 10.60.X0.0/24 pour le protocole UDP
- 10.61.X0.0/24 pour le protocole TCP

7. Configurer un client openVPN sur Windows et/ou sur Linux (client Stormshield ou client libre) et tester la solution.

### III Création d'un accès VPN IPSec site à site

8. Réaliser, à l'aide de la documentation technique, un VPN IPSec site à site où chaque pare-feu (extrémité du tunnel) sera authentifié à l'aide d'un certificat X509.



Pour cela, si cela n'est pas déjà fait, une PKI devra être créée sur l'un des pare-feux. Cette dernière sera en charge de générer l'ensemble des certificats nécessaire. Seuls les sous-réseaux de production seront autorisés à s'échanger des requêtes par l'intermédiaire de ce tunnel.

9. Pourquoi l'authentification par certificat X509 est-elle privilégiée au détriment d'une authentification par clé pré-partagée ?