Informations concernant la sécurité des **Réseaux Privés Virtuels**, proposés par Foxtrot (foxtrot.network).

Sécurité physique

Les serveurs utilisés se situent dans des centres de données ayant la certification suivante : *ISO 27001*.
« Cette certification impose à l'entreprise d'évaluer régulièrement les progrès et les performances de la sécurité de l'information. Ceci est divisé en 3 actions :
La surveillance : l'organisation doit évaluer les performances de la sécurité de l'information et l'efficacité du système de gestion de la sécurité de l'information.
L'audit interne : l'organisation doit effectuer des audits internes à intervalles planifiés pour fournir des informations indiquant si le système de gestion de la sécurité de l'information est toujours adapté à la situation.
L'examen du système : la direction doit examiner le système de gestion de la sécurité de l'information de l'organisation à intervalles planifiés pour s'assurer de son efficacité. »
Pour plus d'informations : *https://www.hetzner.com/unternehmen/zertifizierung*.

Sécurité logicielle

Nous installons et configurons nos serveurs pour être en capacité de résister aux attaques informatiques. Nous utilisons une distribution Linux (Ubuntu) ouverte.
Voici une liste de quelques logiciels et protocoles utilisés :

- SSH, pour communiquer avec nos serveurs de façon chiffrée. L'accès est stricte, et nécessite des mots de passe forts et une authentification à deux étapes (avec un code à six chiffres modifié toutes les 30 secondes).
- IPTables, en tant que pare-feu. Cela permet d'autoriser seulement le trafic légitime.
- Fail2ban, pour contrer les attaques par force brute.

De plus, nous faisons particulièrement attention à faire les mises à jour de sécurité, du système d'exploitation et des logiciels utilisés.

Technologie utilisée

Le logiciel ouvert OpenVPN est utilisé, pour héberger les réseaux privés virtuels. C'est l'un des plus utilisés, notamment pour sa sécurité et sa stabilité accrues. Vous trouverez sur Internet, de nombreux audits de sécurité.

Procédés cryptographiques

OpenVPN a été paramétré pour utiliser ces procédés cryptographiques (pour des raisons de compréhension, nous exprimerons ces paramètres en Anglais) :

- Compression : *disabled*.
- TLS Version : *1.2 (tls-crypt)*.
- Certificate : *prime256v1 (ECDSA)*.
- Data channel : *AES-128-GCM*.
- Control channel : *TLS-ECDHE-ECDSA-WITH-AES-128-GCM-SHA256*.
- Diffie-Hellman key exchange : *prime256v1 (ECDH)*.
- HMAC digest algorithm : *SHA256*.

Stockage des profils OpenVPN

Les profils OpenVPN contiennent toutes les informations nécessaires au client, pour que ce-dernier se connecte au serveur. Si ce fichier devient public, alors votre connexion ne sera plus sécurisée lorsque vous utiliserez votre réseau privé virtuel. C'est pour cette raison, que lors du téléchargement du profil, nous vérifions que vous êtes autorisé à le faire grâce à un code associé à votre compte, et à votre réseau privé virtuel. Si ce-dernier est incorrect, nous bloquons le téléchargement du fichier.

Journaux

Les journaux OpenVPN ont été désactivés avec le paramètre suivant : *verb 0*.

Pour toutes questions supplémentaires, merci d'adresser la demande à l'adresse électronique suivante : *foxtrot.n@protonmail.com*.