FAQ VPN

- FR
- EN

Cette foire aux questions a pour but de répondre à un certain nombre d'interrogations concernant l'utilisation des VPN sur le Cloud OUTSCALE.

Quelles sont les bonnes pratiques de sécurité pour la mise en place d'un tunnel IPsec ?

Pour déployer un VPN, nous recommandons de suivre scrupuleusement la documentation : Tutoriel : Mettre en place une connexion VPN.

Lors de la configuration du tunnel VPN, vous devez notamment correctement configurer les valeurs de dead peer detection (DPD). Dans certains cas, un délai d'inactivité est fixé du fait d'un faible trafic sur un tunnel VPN et la connexion peut être coupée. Nous pouvons préconiser une durée de vie de 86400 secondes pour la phase 1 et 3600 secondes pour la phase 2.

Les virtual private gateways utilisent-elles une plage d'IP spécifique ?

Oui, il y a une plage spécifique pour les virtual private gateways. Lors de la création d'une virtual private gateway, notre orchestrateur TINA OS alloue une IP publique. Il y a uniquement une IP publique par virtual private gateway.

⚠ L'IP attribuée à la virtual private gateway n'est pas une EIP : elle ne peut pas être détachée ni choisie à l'avance.

Comment autoriser l'IP de la virtual private gateway ?

Nous ne recommandons pas d'autoriser toutes les IP OUTSCALE : il est préférable d'autoriser explicitement l'IP source qui réalise les négociations d'authentification et de chiffrement pour monter le tunnel VPN.

Lorsque vous utilisez les actions API OUTSCALE CreateVpnConnection et ReadVpnConnections (ou les actions FCU CreateVpnConnection et DescribeVpnConnections), cette IP aussi appelée "tunnel outside address" de la virtual private gateway est affichée dans le résultat de l'action, au niveau de l'élément `ClientGatewayConfiguration` (ou pour FCU `customerGatewayConfiguration`).

Lorsque vous utilisez Cockpit, cette IP est affichée dans les détails de la page d'interface utilisateur des connexions VPN.

Est-ce qu'il existe une fonctionnalité VPN SSL ou son équivalent sous IPsec (VPN IPsec Mobile Client), afin d'accéder aux machines au sein du VPC sans passer par mon infrastructure entreprise ?

Notre service VPN propose uniquement un tunnel IPsec avec protocole de configuration de chiffrement IKEv1/IKEv2. Le service ne supportant pas de policy routing (policy-based VPN), vous devez obligatoirement configurer une virtual tunnel interface (VTI).

Une VTI est une interface virtuelle liée au VPN lui-même, qui fonctionne pratiquement comme une interface normale. L'avantage est de pouvoir gérer le routage en utilisant vos outils habituels (routes statiques, BGP). Pour la configuration VTI, vous devez modifier les sélecteurs de phase 2 à 0.0.0.0 /0 (réseau local) et 0.0.0.0/0 (réseau distant).

Pour en savoir plus, voir Tutoriel : Mettre en place une connexion VPN > Configurer le tunnel VPN.

Le service VPN d'OUTSCALE n'est pas générateur de coûts importants. Nous sommes sur un montant d'environ 22 euros pour une utilisation de 720 heures/mois.

Puis-je déployer mon propre service de VPN sur le IaaS OUTSCALE ?

Oui, vous pouvez monter votre propre service de VPN sur une machine virtuelle du Cloud OUTSCALE. Voici un exemple de recette de déploiement avec un serveur IPSEC/L2TP.

Quand contacter le support à propos d'un VPN et comment ?

Après configuration du VPN et de tous les éléments associés, déploiement, routage, et que vous rencontrez toujours des difficultés, vous pouvez ouvrir un ticket au support OUTSCALE. Notre équipe pourra analyser en détail les logs.

Veuillez pour cela suivre la procédure de demande de support, en indiquant également bien votre modèle de routeur ainsi que les ID de toutes les ressources que vous avez déployées pour le VPN.