

Mise en place du VPN Mesh ZeroTier

ZeroTier est une solution VPN mesh qui permet de connecter plusieurs machines de manière sécurisée via un réseau virtuel. Ce projet vise à établir une infrastructure VPN permettant l'accès distant sécurisé via RDP à partir de différents appareils (serveur Windows, poste distant et téléphone administrateur).

Création du Compte ZeroTier

Un compte a été créé sur ZeroTier Central.

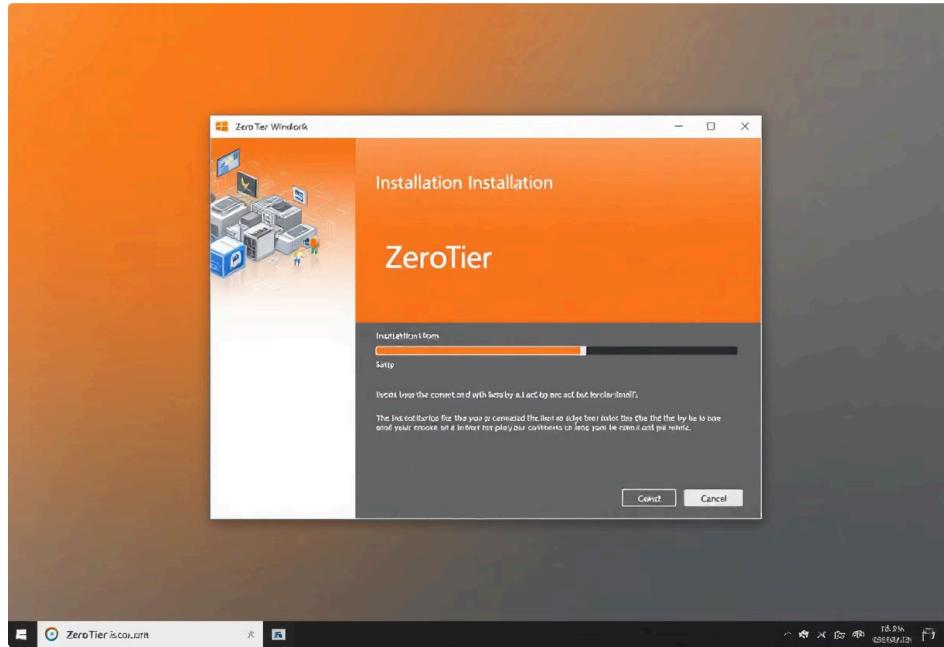
Une fois connecté, il est nécessaire de créer un réseau, ici nommé "IT-JSTD Network".

L'ID de réseau a été récupéré pour permettre l'intégration des machines.



Installation de ZeroTier sur les Appareils

Il suffit de lancer l'exécutable et installé :



ZeroTier a été installé sur :

- Windows Server (serveur principal)
- Un poste distant
- Un téléphone administrateur (mobile)

Chaque machine a rejoint le réseau en utilisant l'ID fourni lors de la création.

Effectuer un clic droit sur l'icône de l'application ZeroTier en arrière-plan.

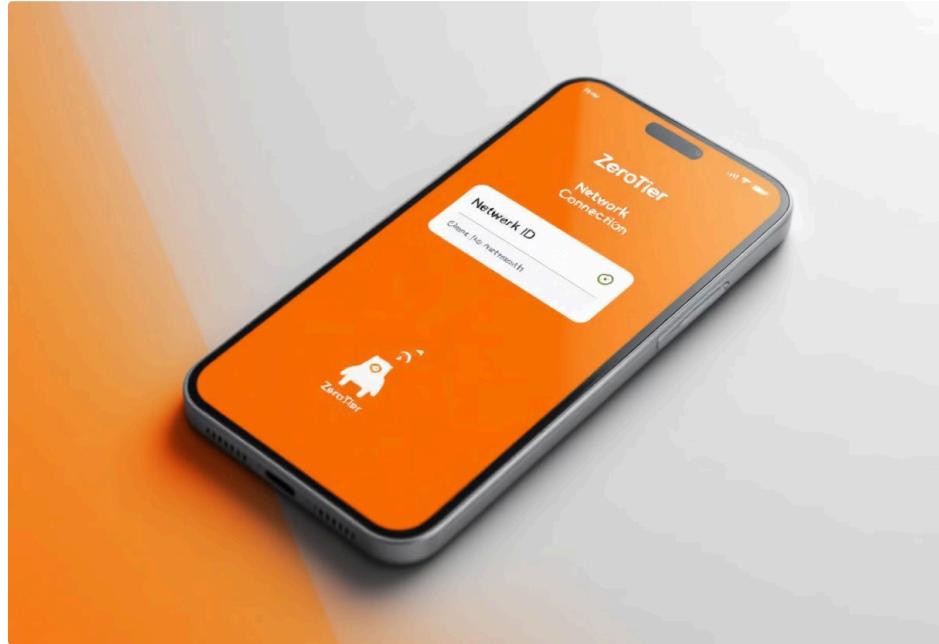
Sélectionner "Join New Network", puis saisir l'ID du réseau affiché sur la console d'administration web.

Interface ZeroTier sur Windows Server

L'installation sur le serveur Windows est une étape cruciale car il s'agit du serveur principal qui sera accessible à distance via RDP.

Une fois installé, le client ZeroTier fonctionne en arrière-plan et permet la connexion au réseau virtuel sécurisé.

ZeroTier sur Mobile



L'application mobile ZeroTier permet d'intégrer le téléphone administrateur au réseau VPN mesh.

Le processus d'installation sur mobile est similaire à celui sur desktop :

1. Télécharger l'application depuis le store
2. L'ouvrir et saisir l'ID du réseau
3. Attendre l'autorisation depuis la console d'administration

Connexion des Machines au Réseau VPN

Sur chaque appareil, le client ZeroTier a été activé et configuré pour rejoindre le réseau "IT-JSTD Network".

L'état des machines a été vérifié via la console web de ZeroTier pour s'assurer qu'elles sont bien connectées.

La console d'administration permet de voir l'ensemble des appareils connectés au réseau et de gérer leurs autorisations.

Test d'Accès à Distance

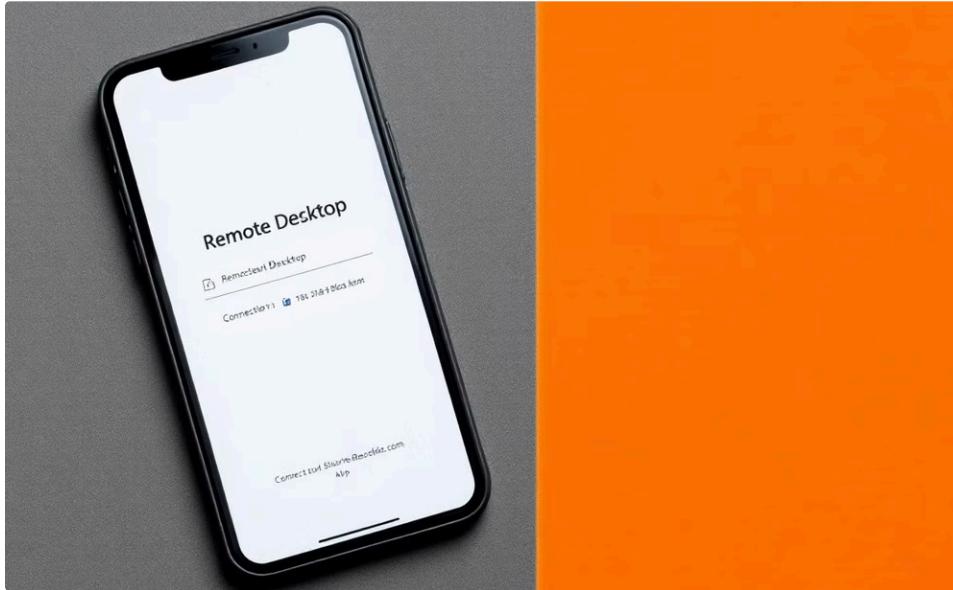
Une connexion RDP a été initiée à partir du poste distant vers le Windows Server.

Une prise en main a été effectuée depuis le téléphone administrateur à l'aide de l'application client RDP mobile de Microsoft.



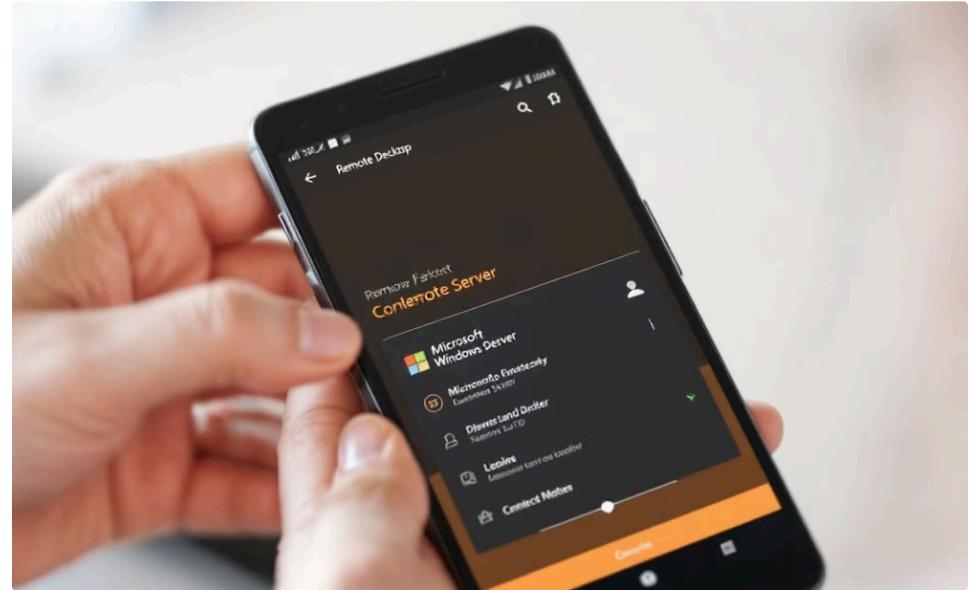
Les tests de connexion RDP ont permis de valider le bon fonctionnement du réseau VPN mesh et la possibilité d'accéder aux ressources à distance de manière sécurisée.

Application RDP Mobile



Écran de connexion

L'application Microsoft Remote Desktop permet de se connecter au serveur Windows via le réseau ZeroTier.



Session RDP active

Une fois connecté, l'administrateur peut contrôler le serveur à distance depuis son téléphone.

Résultat et Sécurisation

Le VPN mesh est fonctionnel : toutes les machines sont connectées et accessibles.



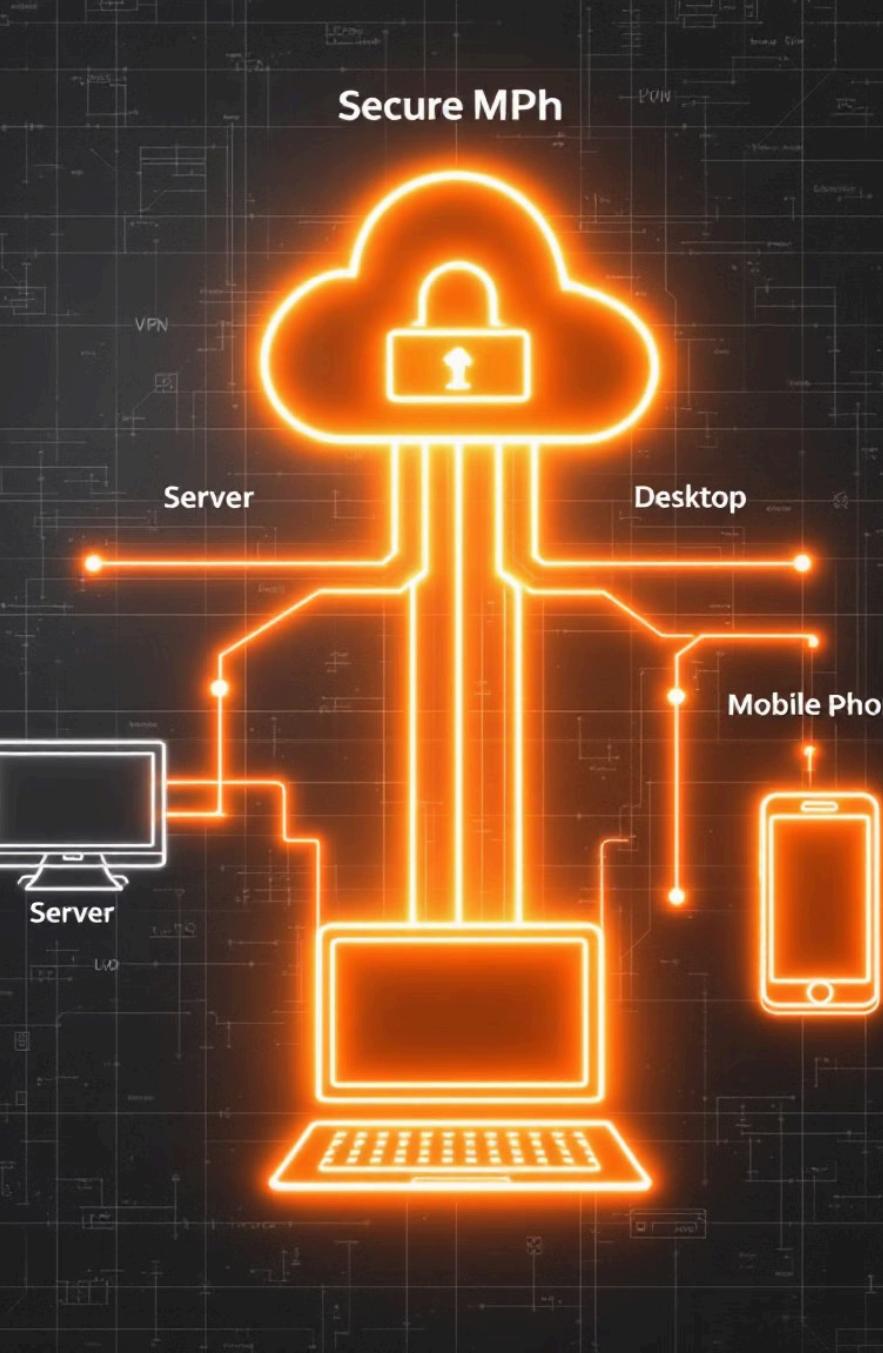
Sécurisation du réseau
Seuls les appareils autorisés peuvent rejoindre le réseau (gestion via la console ZeroTier).



Protection des communications
Chiffrement natif ZeroTier activé pour protéger les communications.



Contrôle d'accès
Utilisation de règles ZeroTier pour restreindre les accès.



Conclusion

La mise en place de ZeroTier permet un accès sécurisé et efficace aux machines distantes sans avoir besoin d'une configuration complexe comme avec un VPN traditionnel. Grâce à son architecture mesh, les appareils se connectent directement entre eux, garantissant une faible latence et une sécurité optimale.



Connexion simplifiée

Installation facile sur tous les appareils

Sécurité renforcée

Communications chiffrées

Accès distant

RDP sécurisé sur tous les appareils