Étude de cas

Sécurisation des accès tiers

Reemo Containers

Comment sécuriser l'accès de ses sous-traitants avec Reemo

Reemo

Étude de cas

Sécurisation des accès tiers

Reemo Containers

Sécuriser l'accès de ses sous-traitants avec Reemo

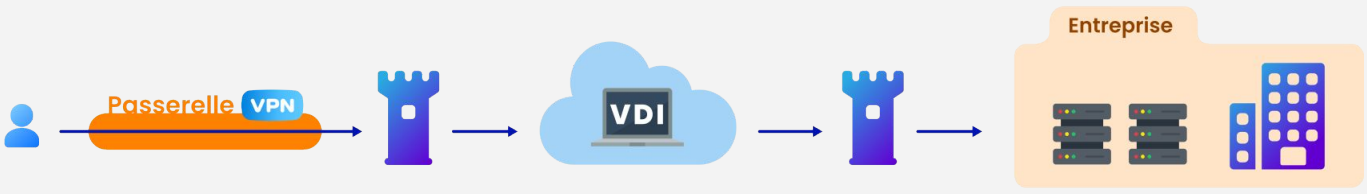
Grâce à Reemo Containers, donnez accès à des tiers de manière sécurisée, via un simple navigateur

Challenges

La problématique courante pour les grandes organisations : comment permettre aux sous-traitants d'accéder en toute sécurité à certaines applications métiers et aux ressources nécessaires pour exécuter leurs tâches, tout en garantissant la protection de l'infrastructure interne ?

Les solutions VPN ou VDI existantes ne sont plus adaptées : imposer l'installation de logiciels trop lents ou complexes aux sous-traitants pour accéder aux serveurs internes n'est plus réaliste à l'heure de la sécurité Zero Trust.

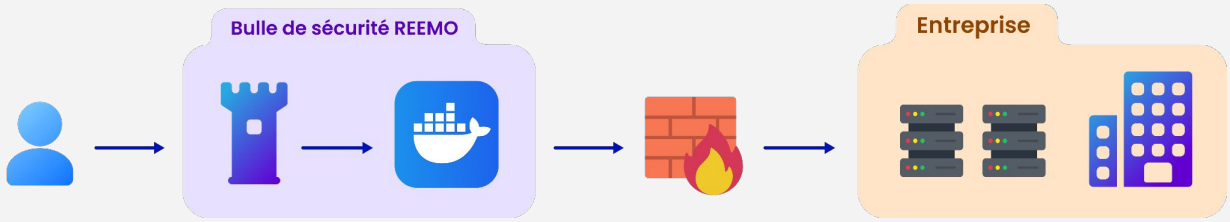
Le défi : Permettre aux sous-traitants un accès fluide et sécurisé, uniquement aux applications nécessaires, sans compromettre l'infrastructure.



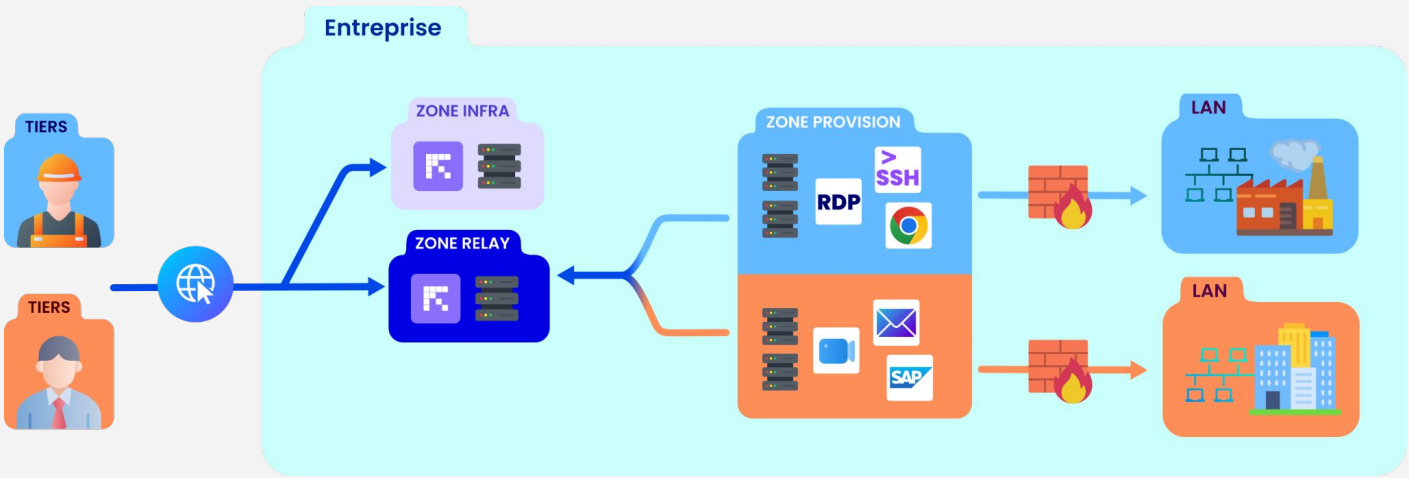
Aujourd'hui, les accès tiers reposent souvent sur une architecture classique combinant **VPN**, **bastions** et **postes virtualisés**. Un modèle **coûteux**, **complexe** à maintenir et **difficile à sécuriser** face aux exigences actuelles de performance et de conformité.

Solutions

Pour répondre à ces exigences, Reemo propose une infrastructure simplifiée, sécurisée, tout en un. Adaptée aux enjeux de tous types d'organisations.



Exemple n° 1 Sécurisation des tiers par isolation dans la zone provision



ÉTAPES CLÉS

Étape 1 : Depuis leur poste, les prestataires se connectent à Internet puis accèdent à une plateforme Reemo centralisée pour s'authentifier.

Étape 2 : Une fois authentifiés, ils sont dirigés vers une zone Relay mutualisée, qui joue le rôle de sas sécurisé. Un conteneur de relais est créé et dédié à la connexion de l'utilisateur pendant toute la durée de sa session.

Étape 3 : Le conteneur applicatif est créé dans la zone provision correspondant au profil utilisateur du tiers.

Étape 4 : L'utilisateur et le conteneur se rencontrent dans la zone relais pour établir la connexion.

A SAVOIR

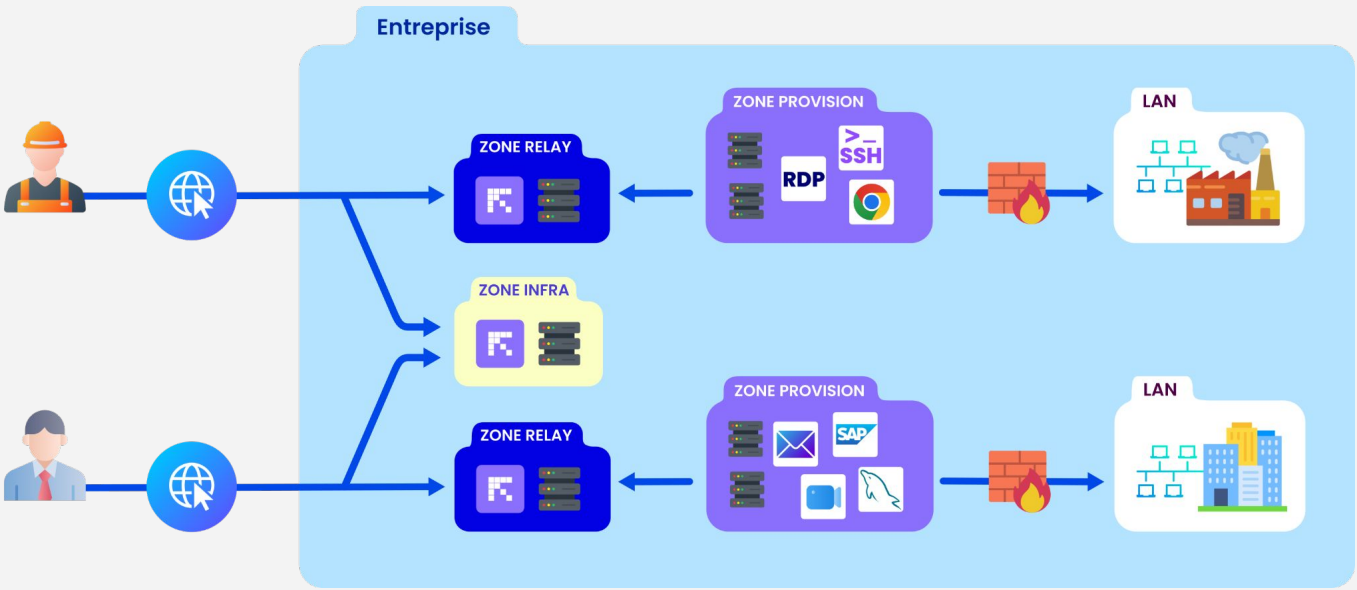
Grâce aux conteneurs, vous avez le contrôle :

- Filtrage des périphériques
- Permissions de copier-coller
- Permissions de téléchargement

Solutions

Chaque tier dispose ici de **sa propre zone Relay** et de **sa propre zone de provision**, garantissant une **isolation complète** des accès et des flux. Chaque zone de provision est reliée à son LAN dédié **via un pare-feu**, assurant un **cloisonnement strict**, une **traçabilité** fine et une **maîtrise totale des permissions**. Ce modèle est idéal pour les environnements multi-partenaires à **haut niveau d'exigence**.

Exemple n° 2 Architecture On Prem dédiée par tiers



Modularité & scalabilité : une architecture entièrement modulable

- Possibilité de créer des portails d'accès dédiés.
- Possibilité d'unifier ou de séparer les zones de provision.
- Déploiement on-premise ou cloud hybride selon les besoins.

Résultats

Sécurité accrue

Grâce à l'isolement des sessions dans des conteneurs et à l'application stricte des principes de ZTNA, **les tiers n'ont accès qu'aux ressources strictement nécessaires**, éliminant ainsi tout risque d'accès non autorisé.

Accès simplifié

L'accès à distance via le navigateur permet de **réduire la complexité d'intégration pour les sous-traitants**, ne nécessitant aucune configuration particulière ou mises à jour sur leurs machines locales.

Performance optimale

Les sous-traitants peuvent accéder aux applications critiques avec **une latence additionnelle quasi nulle**, leur permettant de **travailler efficacement même à distance**.