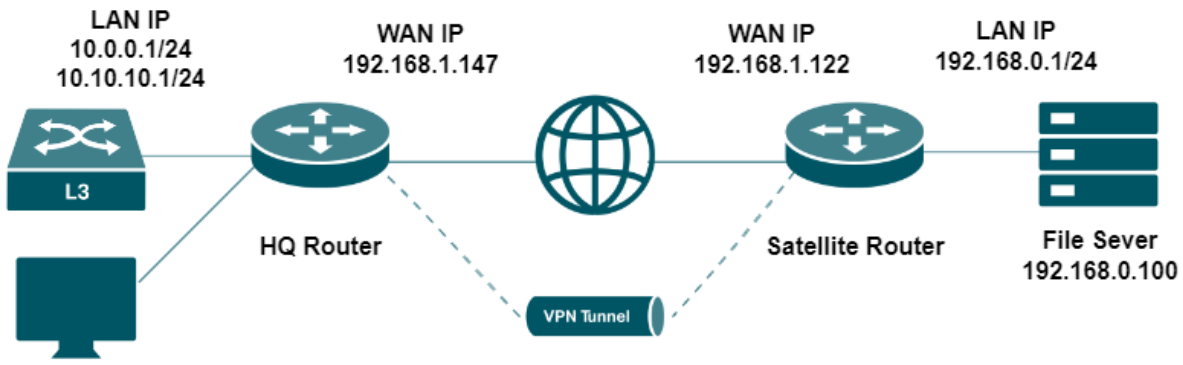
Wireguard Site to Site VPN Omada

Voici un tutoriel en français enrichi de captures d'écran détaillées pour configurer un VPN **site-à-site WireGuard** via le contrôleur **Omada SDN**, basé sur le guide TP-Link (TP-Link).

🔧 Pré-requis

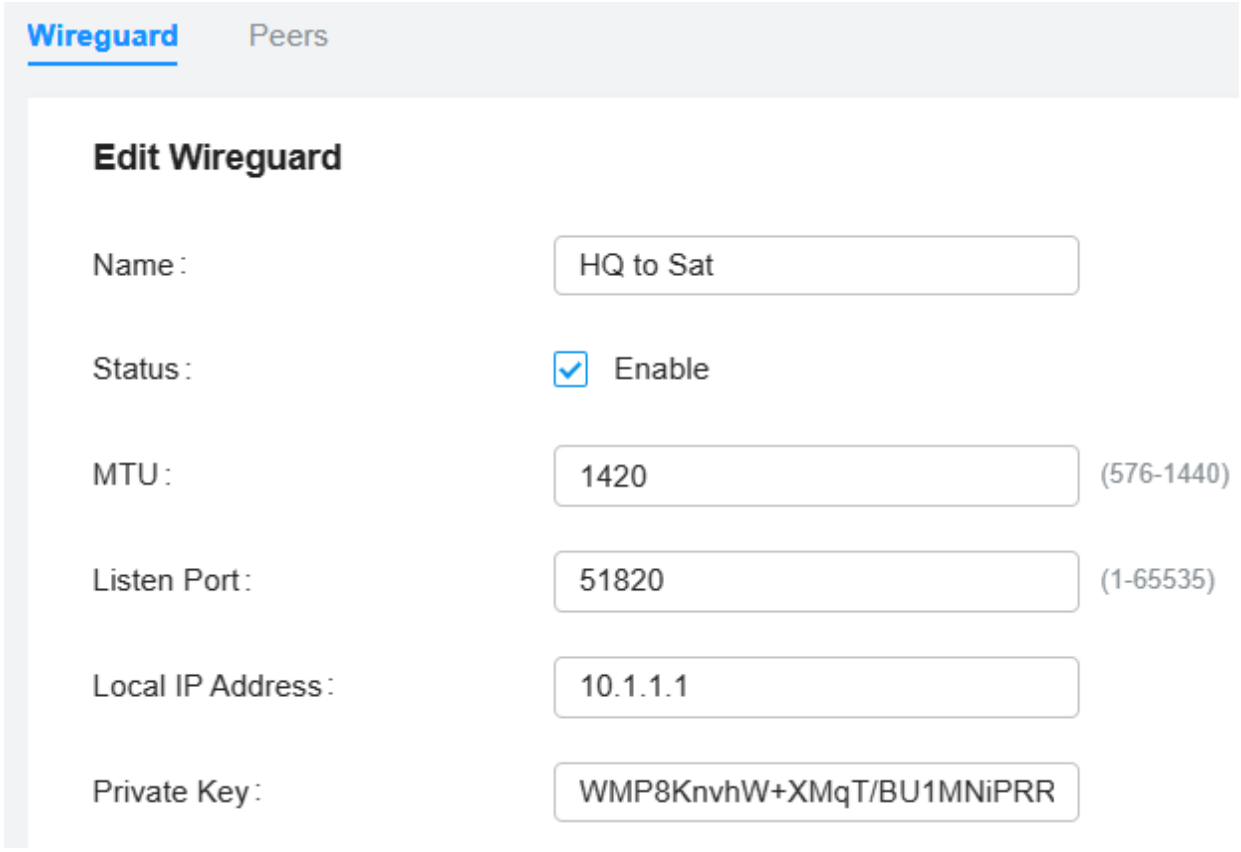
- Routeurs compatibles : ER605 V2, ER7206, ER8406, G36W-4G, ER707-M2, etc. (TP-Link)
- Contrôleur Omada SDN (sur PC ou appareil dédié)
- Accès administrateur aux deux sites (HQ & satellite)
- Firmware à jour



Étape 1 : Créer l'interface WireGuard sur le site HQ 🏢

1. Dans le contrôleur Omada, sélectionnez le site HQ → accédez à **Settings > VPN > WireGuard** (TP-Link)
2. Cliquez sur **Create New WireGuard**

3. Remplissez les champs :
a. **Name** : exemple “VPN-HQ”
b. **Status** : activé
c. **MTU** : 1420 (par défaut)
d. **Listen Port** : 51820 (par défaut)
e. **Local IP Address** : adresse VPN dédiée (non utilisée dans vos LAN)
f. **Private Key** : générée automatiquement (modifiable)



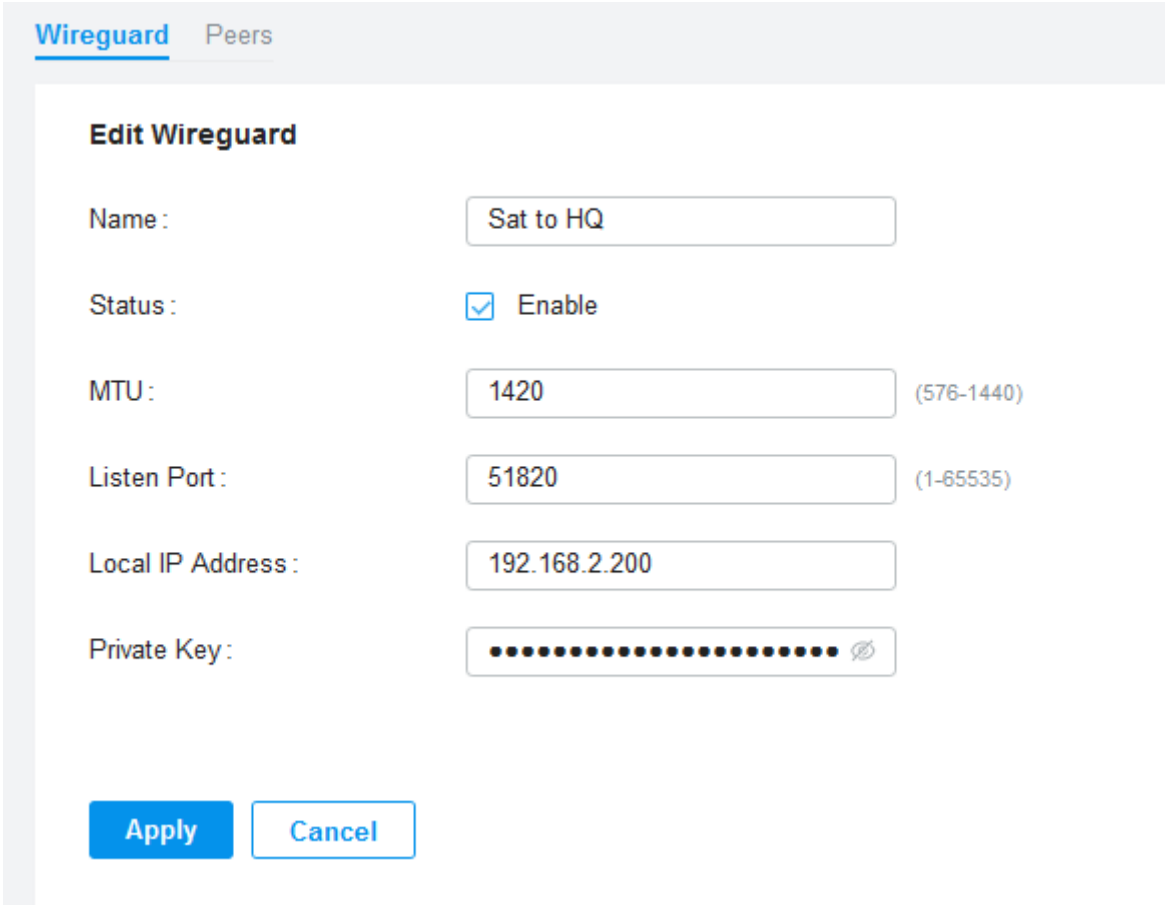
Nom: Spécifier le nom qui identifie l'interface WireGuard. (Cela n'affecte pas le tunnel ou le comportement du VPN.)
État: Préciser s'il convient d'activer l'interface WireGuard. (Impossible ou désactivez votre tunnel VPN.)
MTU: Préciser la valeur MTU de l'interface WireGuard. La valeur par défaut de 1420 est recommandée. (Il n'est généralement pas nécessaire qu'il soit réglé, et qu'il soit généralement déterminé automatiquement par le

système.)
Écoutez Port: Précisez le numéro de port que l'interface WireGuard écoute. La valeur par défaut est 51820. (Habituellement, le client n'a pas besoin de cela pour être configuré. Dans cet example, notre routeur est le serveur. Vous pouvez changer cela si vous en avez besoin et que vous savez ce que vous faites.)
Adresse IP locale: Préciser l'adresse IP de l'interface WireGuard. (Définissez l'adresse IP de l'interface WireGuard, qui devrait être une adresse IP non occupée. Il est normal de configurer en dehors de votre gamme de LAN existante.)
Clé privée: Spécifier la clé privée de l'interface WireGuard. La valeur sera automatiquement générée sur l'appareil, et vous pouvez également la modifier manuellement (Définit la clé privée de ce tunnel VPN spécifique. Il doit être réglé et ne peut être partagé avec d'autres tunnels.)

Étape 2 : Configurer l’interface WireGuard sur le site satellite 🌐

Répétez les mêmes étapes dans le site satellite :

- Accédez à **Settings > VPN > WireGuard**
- Cliquez sur **Create New WireGuard**
- Utilisez des valeurs propres au site (nom différent, IP locale unique, etc.)



Nom: Spécifier le nom qui identifie l'interface WireGuard. (Cela n'affecte pas le tunnel ou le comportement du VPN.)
État: Préciser s'il convient d'activer l'interface WireGuard. (Impossible ou désactivez votre tunnel VPN.)
MTU: Préciser la valeur MTU de l'interface WireGuard. La valeur par défaut de 1420 est recommandée. (Il n'est généralement pas nécessaire qu'il soit réglé, et qu'il soit généralement déterminé automatiquement par le système.)
Port: Précisez le numéro de port que l'interface WireGuard écoute. La valeur par défaut est 51820. (Habituellement, le client n'a pas besoin de cela pour être configuré. Dans cet example, notre routeur est le serveur. Vous pouvez changer cela si vous en avez besoin et que vous savez ce que vous faites.)
Adresse IP locale: Préciser l'adresse IP de l'interface WireGuard. (Définissez

l'adresse IP de l'interface WireGuard, qui devrait être une adresse IP non occupée. Il est normal de configurer en dehors de votre gamme de LAN existante.)

Clé privée: Spécifier la clé privée de l'interface WireGuard. La valeur sera automatiquement générée sur l'appareil, et vous pouvez également la modifier manuellement (Définit la clé privée de ce tunnel VPN spécifique. Il doit être réglé et ne peut être partagé avec d'autres tunnels.)

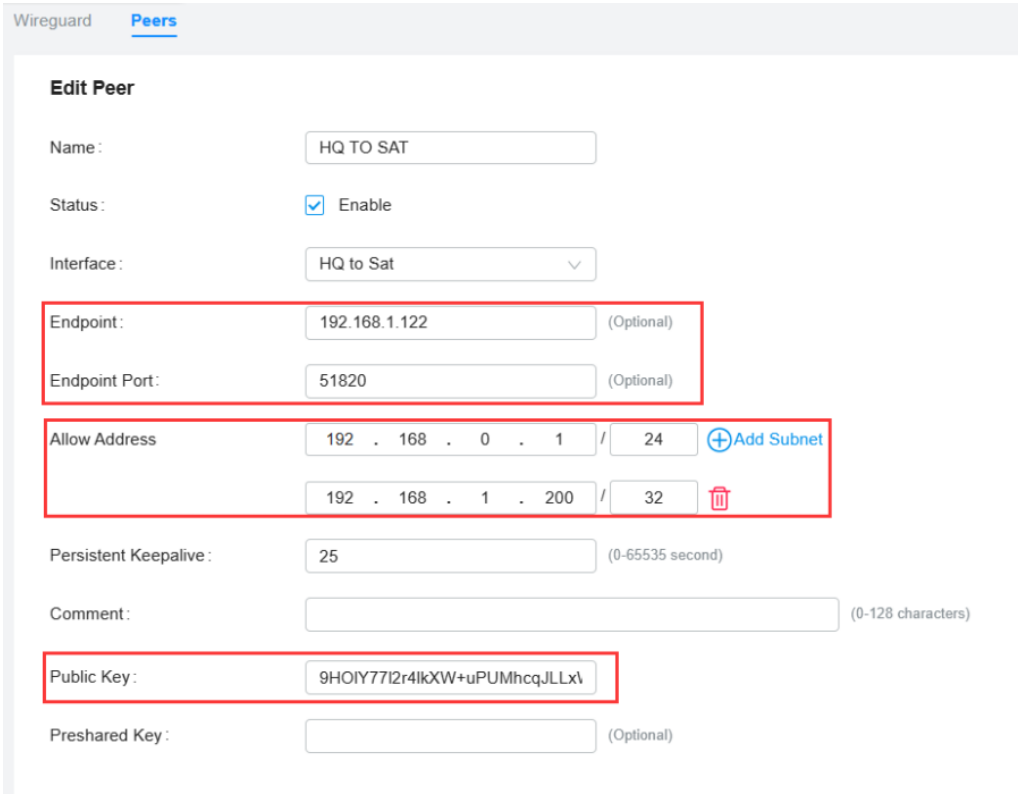
Étape 3 : Ajouter un peer (tunnel) entre HQ et satellite 🔗

Sur le site HQ

1. Allez dans **WireGuard > Peers**
2. Cliquez sur **Create New Peer**
3. Paramétrez :

a. **Name** : nom du tunnel (ex. “Tunnel-HQ-to-Sat”)
b. **Status** : activé
c. **Interface** : l’interface HQ créée à l’étape précédente
d. **Public Key** : clé publique du site satellite
e. **Endpoint** (si HQ initie) : adresse IP publique du site satellite
f. **Endpoint Port** : 51820

g. **Allowed Address** : sous-réseau LAN du site satellite (ex. 192.168.2.0/24)
h. **Persistent Keepalive**, **Preshared Key** (facultatif)
4. Cliquez **Apply** — l'entrée apparaitra dans la liste des peers (cf image 3) (TP-Link)



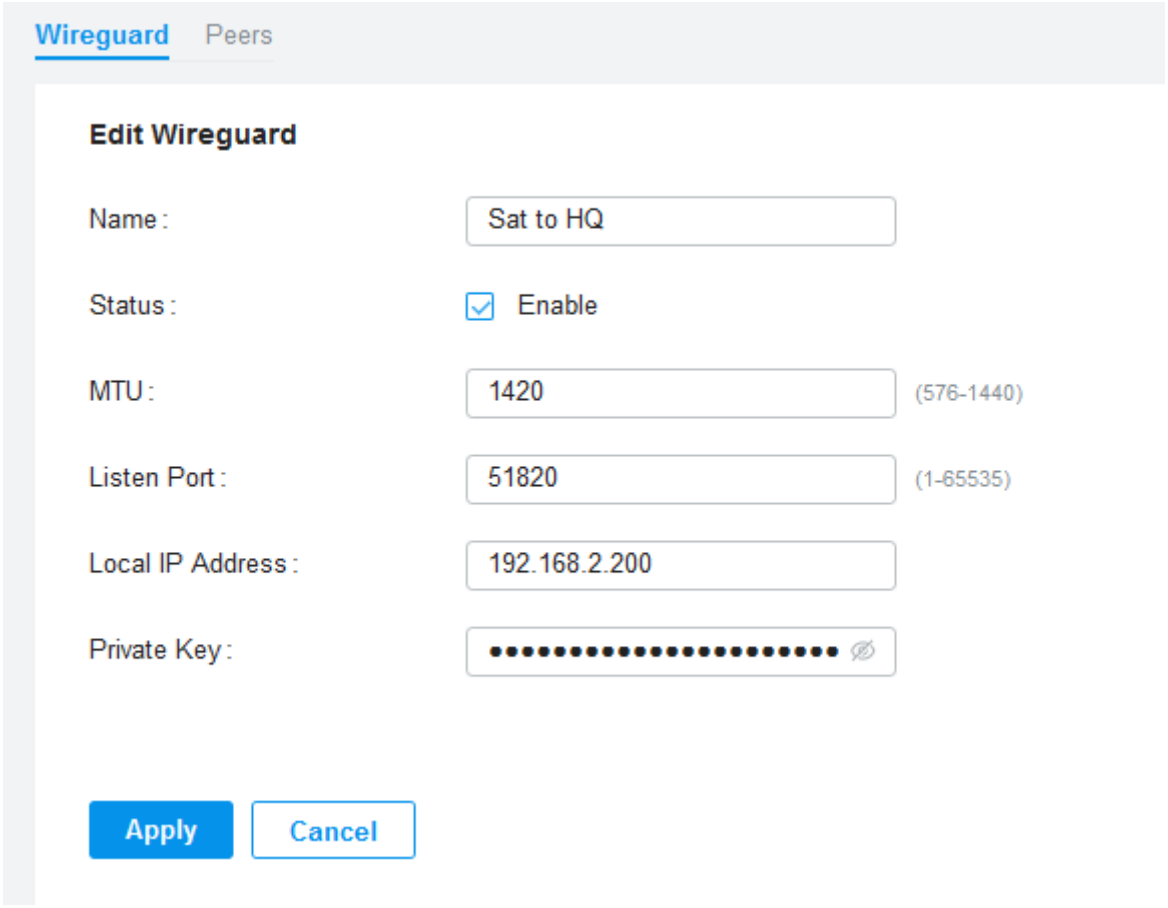
Nom: Préciser le nom qui identifie le tunnel WireGuard.
État: Préciser s'il est possible d'activer le paramétrage par pair.
Interface: Choisissez l'interface WireGuard à laquelle le pair appartient.
Point d'extrémité: Préciser l'adresse IP du pair. Ce paramètre est nécessaire lorsque le routeur Omada se connecte activement à d'autres pairs de WireGuard. (Si vous avez besoin de spécifier le serveur pair, vous pouvez mettre l'adresse IP publique du serveur pair. Si le QG a initié la connexion, cela peut être facultatif, ce qui est le cas dans ce guide. Si vous ne spécifiez pas le point d'extrémité sur les deux sites, alors la connexion ne peut pas être faite.)
Port d'arrivée: Préciser le numéro de port du pair. Ce paramètre est nécessaire lorsque le routeur Omada se connecte activement à d'autres pairs de WireGuard.
Adresse autorisée: Préciser le segment d'adresse qui permet le passage du

traffic. (Ici, vous devez spécifier le sous-réseau du réseau local pair. Cela définit ce que vous êtes autorisé à accéder sur le site homologue. Si vous n'incluez pas le sous-réseau, alors vous n'y avez pas accès.)
Maintien persistant : Préciser l'intervalle de paquets de maintien du tunnel. (Cela définit l'intervalle du paquet keepalive envoyé à l'adresse autorisée.)
Commentaire : Saisir la description du pair.
Clé publique: Remplir la clé publique du site satellite des pairs.
Clé pré-partagée: Spécifier une clé partagée si nécessaire.

Sur le site satellite

Même chose dans **WireGuard > Peers** :

- Nommez le tunnel (ex. “Tunnel-Sat-to-HQ”)
- Utilisez la clé publique du HQ
- Endpoint = IP publique du HQ (si le satellite initie)
- Allowed Address = sous-réseau LAN du HQ (ex. 192.168.1.0/24)



Nom: Préciser le nom qui identifie le tunnel WireGuard.
État: Préciser s'il est possible d'activer le paramétrage par pair.
Interface: Choisissez l'interface WireGuard à laquelle le pair appartient.
Point d'extrémité: Préciser l'adresse IP du pair. Ce paramètre est nécessaire lorsque le routeur Omada se connecte activement à d'autres pairs de WireGuard. (Si vous avez besoin de spécifier le serveur pair, vous pouvez mettre l'adresse IP publique du serveur pair. Si le QG a initié la connexion, cela peut être facultatif, ce qui est le cas dans ce guide. Si vous ne spécifiez pas le point d'extrémité sur les deux sites, alors la connexion ne peut pas être faite.)

Port d'arrivée: Préciser le numéro de port du pair. Ce paramètre est nécessaire lorsque le routeur Omada se connecte activement à d'autres pairs de WireGuard.
Adresse autorisée: Préciser le segment d'adresse qui permet le passage du traffic. (Ici, vous devez spécifier le sous-réseau du réseau local pair. Cela définit ce que vous êtes autorisé à accéder sur le site homologue. Si vous n'incluez pas le sous-réseau, alors vous n'y avez pas accès.)
Maintien persistant : Préciser l'intervalle de paquets de maintien du tunnel. (Cela définit l'intervalle du paquet keepalive envoyé à l'adresse autorisée.)
Commentaire : Saisir la description du pair.
Clé publique: Remplir la clé publique du site de la Génération du siège.
Clé pré-partagée: Spécifier une clé partagée si nécessaire.

Étape 4 : Vérifier le statut du VPN ☑

- Dans Insight > VPN Status > WireGuard VPN, vérifiez que chaque tunnel affiche **Last Handshake**, **TX/RX Bytes**, etc. (TP-Link)
- Testez la connexion depuis le HQ vers le LAN du satellite (ping ou partage de fichiers)
- Testez depuis le satellite vers le LAN du HQ
  Si les échanges fonctionnent, le tunnel est bien établi (cf image 0) (TP-Link)

📝 Récapitulatif

Étape	Action
1	Créer l’interface WireGuard sur le site HQ
2	Idem sur le site satellite
3	Configurer les peers (tunnels) sur chaque site
4	Vérifier le bon établissement du tunnel via ping & status

🔍 À retenir

- Ne jamais **dupliquer l’adresse IP locale VPN** sur les deux sites
- Le **Allowed Address** doit correspondre aux sous-réseaux distants souhaités
- Si un site est **derrière un NAT**, c’est lui qui doit initier la connexion
- Par défaut, utilisez **port 51820** et **MTU 1420**
- Pour tester un tunnel actif : vérifiez le **Last Handshake**