Sessions BGP

1. Introduction : Pourquoi utiliser BGP ?

1.1. À quoi sert une session BGP sur Tunnel-IP.com ?

Le protocole **BGP (Border Gateway Protocol)** est le protocole de routage utilisé sur Internet pour échanger des préfixes IP entre systèmes autonomes (AS). Sur Tunnel-IP.com, les sessions BGP vous permettent d'**annoncer vos propres préfixes IP** à travers notre infrastructure, offrant un contrôle total sur votre routage.

Cas d'usage :

- Vous possédez votre propre bloc d'IPs (PI/PA) et votre ASN.
- Vous souhaitez annoncer vos préfixes via l'infrastructure Tunnel-IP.com.
- Vous avez besoin d'un contrôle dynamique de vos routes (failover, multihoming, etc.).

1.2. Les deux types de sessions

Tunnel-IP.com propose **deux types** de sessions BGP :

	Session normale	Session autogérée
Principe	Session BGP classique à travers un tunnel L3. Vous configurez BGP sur votre routeur et échangez des préfixes avec la plateforme.	Routeur virtuel entièrement géré par Tunnel-IP.com. Nous annonçons vos préfixes avec votre ASN (ou le nôtre) et routons le trafic vers votre tunnel.
Configuration côté client	Oui — vous devez configurer un démon BGP sur votre routeur.	Non — aucune configuration BGP nécessaire de votre côté.

	Session normale	Session autogérée
Tunnel requis	Oui — un tunnel L3 (GRE, IPIP, Wireguard, etc.) doit être configuré. La session BGP passe à travers le tunnel.	Non obligatoire pour le BGP lui-même — les subnets sont assignés directement à la session autogérée via le panel, puis routés statiquement vers le tunnel de votre choix.
ASN requis	Oui — votre propre ASN, enregistré sur le panel.	Optionnel — vous pouvez utiliser votre ASN ou celui de Tunnel-IP.com.
Contrôle	Total — vous choisissez quels préfixes annoncer et pouvez gérer le routage dynamiquement.	Limité — nous gérons l'annonce, vous gérez l'attribution des subnets via le panel.
Idéal pour	Utilisateurs avancés, multihoming, failover BGP.	Utilisateurs qui veulent simplement annoncer leurs IPs sans gérer BGP.

2. Prérequis

2.1. Pour les deux types de sessions

- Un **service Tunnel-IP.com** actif.
- Vos **préfixes IP** correctement enregistrés auprès d'un RIR (RIPE, ARIN, etc.).
- Un **route object** correctement configuré dans la base IRR correspondante (RIPE DB, RADB, etc.) autorisant l'annonce de vos préfixes par votre ASN (ou celui de Tunnel-IP.com pour les sessions autogérées).
- Une **LOA (Letter of Authorization)** si les préfixes ne vous appartiennent pas directement.

2.2. Spécifique à la session normale

- Un **tunnel L3 configuré et fonctionnel** (GRE, IPIP, Wireguard, OpenVPN, IPsec).
- Votre **ASN** enregistré sur panel.tunnel-ip.com/asn/ avec votre **AS-SET**.
- Un **routeur capable de faire du BGP** (Linux avec BIRD/FRR, MikroTik, Cisco, Juniper, etc.).

2.3. Spécifique à la session autogérée

- Si vous souhaitez utiliser **votre propre ASN** : l'enregistrer sur panel.tunnel-ip.com/asn/.
- Si vous souhaitez utiliser **l'ASN de Tunnel-IP.com** : aucun ASN à enregistrer.
- Une **demande de whitelist** de vos préfixes accompagnée de la LOA.

3. Enregistrer son ASN

> Si vous souhaitez utiliser l'ASN de Tunnel-IP.com (uniquement pour les sessions autogérées), vous pouvez passer cette étape.

1. Connectez-vous à panel.tunnel-ip.com
2. Allez dans **"ASN"** (panel.tunnel-ip.com/asn/).
3. Cliquez sur **"Ajouter un ASN"**.
4. Renseignez :
   - **Votre numéro d'AS** (ex : `AS211615`).
   - **Votre AS-SET** (ex : `AS-EXAMPLE`). L'AS-SET est utilisé pour valider automatiquement les préfixes que vous êtes autorisé à annoncer.
5. Validez.

> **Important :** Assurez-vous que votre AS-SET est correctement maintenu dans une base IRR (RIPE, RADB, etc.) et qu'il contient bien les préfixes que vous souhaitez annoncer. Sans cela, vos annonces seront rejetées.

---

4. Session autogérée

La session autogérée est la méthode la plus simple : **Tunnel-IP.com gère entièrement l'annonce BGP** de vos préfixes. Vous n'avez aucune configuration BGP à faire sur votre routeur.

4.1. Comment ça fonctionne ?

```
Internet ← [Routeurs Tunnel-IP.com annoncent vos préfixes en BGP] ← Route statique → [Votre Tunnel] → [Votre Routeur]
```

1. Vous nous fournissez vos préfixes et la LOA.
2. Nous créons la session autogérée et whitelistons vos préfixes.
3. Sur le panel, vous assignez vos subnets à la session autogérée.
4. Le trafic entrant arrive sur notre infrastructure et est routé statiquement vers le tunnel de votre choix.

5. Côté sortant, vous configurez votre routeur pour envoyer le trafic de vos préfixes via le tunnel (comme pour un tunnel L3 classique — voir les docs de routage sortant).

4.2. Étapes

1. **Ouvrir un ticket** pour demander la création d'une session autogérée.
   - Précisez les préfixes à annoncer.
   - Fournissez la LOA si nécessaire.
   - Précisez si vous souhaitez utiliser votre ASN ou celui de Tunnel-IP.com.
2. **Attendre la validation** : nous vérifions le route object, l'AS-SET et la LOA.
3. **Whitelist effectuée** : une fois vos préfixes whitelistés, vous pouvez les gérer depuis le panel.
4. **Assigner vos subnets** :
   - Allez dans **"Subnets"**.
   - Créez un subnet correspondant à vos préfixes whitelistés.
   - Assignez-le à la **session BGP autogérée**.
5. **Configurer le routage sortant** sur votre routeur (tables de routage / policy routing), comme pour un tunnel L3 classique.

> Avec une session autogérée, vous n'avez **pas** besoin de configurer un démon BGP. Le routage entrant est géré par la plateforme, et le routage sortant se fait via les méthodes classiques (policy routing, VRF) décrites dans les documentations des tunnels L3.

---

5. Session normale (BGP à travers un tunnel L3)

La session normale vous donne un **contrôle total** sur vos annonces BGP. Vous configurez un démon BGP sur votre routeur qui établit une session avec les routeurs de Tunnel-IP.com à travers votre tunnel L3.

5.1. Comment ça fonctionne ?

```
Internet ← [Routeurs Tunnel-IP.com] ← Session BGP via tunnel → [Votre Routeur BGP] → [Votre Réseau]
                                        100.64.0.5 ←→ 100.64.0.6
```

- La session BGP s'établit entre l'IP plateforme du tunnel (ex: `100.64.0.5`) et votre IP client du tunnel (ex: `100.64.0.6`).
- Vous annoncez vos préfixes à la plateforme via BGP.
- La plateforme annonce vos préfixes vers Internet.

5.2. Étapes de mise en place

1. **Avoir un tunnel L3 fonctionnel** : configurez d'abord un tunnel GRE, IPIP, Wireguard, etc. et vérifiez que le ping fonctionne entre les deux côtés (ex: `ping 100.64.0.5`).
2. **Enregistrer votre ASN** sur panel.tunnel-ip.com/asn/ (voir section 3).
3. **Vérifier votre route object** : assurez-vous que vos préfixes sont correctement déclarés dans une base IRR et que votre AS-SET est à jour.
4. **Ouvrir un ticket** pour demander la création de la session BGP.
   - Précisez le tunnel sur lequel la session doit être établie.
   - Précisez votre ASN.
   - Précisez les préfixes que vous souhaitez annoncer.
5. **Attendre la création** : nous configurons la session côté plateforme et vous fournissons les détails.
6. **Configurer BGP sur votre routeur** (voir section 5.3).

5.3. Informations de la session

Une fois la session créée, vous retrouverez les informations suivantes sur la page **"Sessions BGP"** du panel :

Champ	Description	Exemple
Nom	Identifiant de la session	`BGP-41`
ASN Client	Votre ASN	`AS65000`
ASN Tunnel	ASN utilisé sur le tunnel	`AS211615`
Zone	Zone du serveur	`Default Zone V2`
IP Client	Votre IP de peering (IP de votre côté du tunnel)	`100.64.0.6`
IP Plateforme	IP de peering côté Tunnel-IP.com	`100.64.0.5`
Status	État de la session BGP	`Connect`, `Established`, `Active`
Préfixes acceptés	Nombre de préfixes que la plateforme accepte de votre part	`0`, `5`, etc.

5.4. Configurer BGP sur votre routeur

>

> Les exemples ci-dessous utilisent les valeurs suivantes. **Adaptez-les** avec lesinformations fournies sur le panel :
> - Votre ASN : `65000`
> - IP plateforme (neighbor) : `100.64.0.5`
> - Votre IP tunnel : `100.64.0.6`
> - Préfixe à annoncer : `203.0.113.0/24`

Linux (BIRD 2)

```
# /etc/bird/bird.conf

router id 100.64.0.6;

protocol device {
    scan time 10;
}

protocol static {
    ipv4 {
        table master4;
    };
    # Déclarer les préfixes à annoncer
    route 203.0.113.0/24 blackhole;
}

protocol bgp tunnel_ip {
    local 100.64.0.6 as 65000;
    neighbor 100.64.0.5 as 211615;

    ipv4 {
        import all;     # Accepter les routes de la plateforme
        export where proto = "static";  # Annoncer nos préfixes statiques
    };
}
```

Puis redémarrer BIRD :

```
birdc configure
```

Linux (FRRouting / FRR)

```
# /etc/frr/frr.conf

frr defaults traditional
hostname routeur
log syslog informational

router bgp 65000
 bgp router-id 100.64.0.6
 neighbor 100.64.0.5 remote-as 211615
 !
 address-family ipv4 unicast
  network 203.0.113.0/24
  neighbor 100.64.0.5 activate
 exit-address-family
!
ip route 203.0.113.0/24 Null0
```

Puis recharger :

```
systemctl reload frr
```

MikroTik (RouterOS v7)

```
# Ajouter l'instance BGP
/routing/bgp/connection/add name=tunnel-ip \
  remote.address=100.64.0.5 remote.as=211615 \
  local.address=100.64.0.6 local.role=ebgp \
  as=65000 \
  output.filter-chain=bgp-out \
  input.filter-chain=bgp-in

# Créer les filtres
/routing/filter/rule/add chain=bgp-out rule="if (dst == 203.0.113.0/24) { accept }"
/routing/filter/rule/add chain=bgp-out rule="reject"
/routing/filter/rule/add chain=bgp-in rule="accept"

# Route blackhole pour le préfixe annoncé
/ip/route/add dst-address=203.0.113.0/24 type=blackhole
```

Cisco (IOS/XE)

```
router bgp 65000
 bgp router-id 100.64.0.6
 neighbor 100.64.0.5 remote-as 211615
 !
 address-family ipv4
  network 203.0.113.0 mask 255.255.255.0
  neighbor 100.64.0.5 activate
 exit-address-family
!
ip route 203.0.113.0 255.255.255.0 Null0
```

Juniper (JunOS)

```
set routing-options router-id 100.64.0.6
set routing-options autonomous-system 65000

set protocols bgp group TUNNEL-IP type internal  # internal si même ASN, external sinon
set protocols bgp group TUNNEL-IP neighbor 100.64.0.5
set protocols bgp group TUNNEL-IP export ADVERTISE

set policy-options policy-statement ADVERTISE term 1 from route-filter 203.0.113.0/24 exact
set policy-options policy-statement ADVERTISE term 1 then accept
set policy-options policy-statement ADVERTISE term 2 then reject

set routing-options static route 203.0.113.0/24 discard

commit
```

Arista (EOS)

```
router bgp 65000
   router-id 100.64.0.6
   neighbor 100.64.0.5 remote-as 211615
   !
   address-family ipv4
      network 203.0.113.0/24
      neighbor 100.64.0.5 activate

ip route 203.0.113.0/24 Null0
```

6. Vérification

6.1. Vérifier l'état de la session

Le status de la session est visible sur le panel. Les états possibles :

Status	Signification
Established	La session est active et fonctionne.
Connect	La plateforme tente de se connecter — vérifiez votre configuration.
Active	La plateforme attend une connexion — vérifiez votre configuration et la connectivité du tunnel.
Idle	La session est inactive.
OpenSent / **OpenConfirm**	Négociation en cours — patientez ou vérifiez les ASN.

6.2. Commandes de vérification par constructeur

Linux (BIRD 2)

```
birdc show protocols all tunnel_ip   # Détails de la session
birdc show route export tunnel_ip    # Préfixes annoncés
birdc show route protocol tunnel_ip  # Préfixes reçus
```

Linux (FRR)

```
vtysh -c "show bgp summary"
vtysh -c "show bgp ipv4 unicast neighbors 100.64.0.5"
vtysh -c "show bgp ipv4 unicast"
```

MikroTik

```
/routing/bgp/session/print
/routing/bgp/advertisements/print
```

```
/ip/route/print where bgp
```

Cisco

```
show bgp summary
show bgp ipv4 unicast neighbors 100.64.0.5
show bgp ipv4 unicast
```

Juniper

```
show bgp summary
show bgp neighbor 100.64.0.5
show route protocol bgp
```

---

7. Dépannage

7.1. Problèmes courants

Symptôme	Cause Possible	Solution
Session en "Connect" ou "Active"	Le tunnel L3 ne fonctionne pas	Vérifiez que vous pouvez pinger l'IP plateforme du tunnel (`ping 100.64.0.5`)
Session en "Connect" ou "Active"	Port TCP 179 bloqué	Vérifiez qu'aucun pare-feu ne bloque le port 179 sur l'interface tunnel
Session en "OpenSent"	ASN incorrect	Vérifiez que l'ASN configuré correspond à celui déclaré sur le panel
Préfixes acceptés = 0	Préfixes non annoncés	Vérifiez votre configuration BGP (filtres, network, route statique blackhole)
Préfixes acceptés = 0	Route object manquant ou incorrect	Vérifiez votre route object dans la base IRR et votre AS-SET sur le panel
Préfixes rejetés	Préfixe trop spécifique	Vérifiez que vous n'annoncez pas de préfixes plus spécifiques que /24 (sauf accord)
Session "Established" mais pas de trafic	Routage sortant mal configuré	Configurez le policy routing / VRF pour que le trafic sortant passe par le tunnel (voir docs tunnel L3)

7.2. Vérifications à faire avant d'ouvrir un ticket

1. ☐ Le tunnel L3 fonctionne (ping entre les deux côtés).
2. ☐ Le port TCP 179 n'est pas bloqué par un pare-feu.
3. ☐ L'ASN est correctement enregistré sur le panel.
4. ☐ Le route object existe dans la base IRR.
5. ☐ L'AS-SET contient bien vos préfixes.
6. ☐ La configuration BGP est correcte (bon ASN, bonne IP neighbor).
7. ☐ Une route statique blackhole existe pour chaque préfixe annoncé.

---

8. BGP Communities

Les BGP communities permettent de **contrôler le comportement de vos annonces** sur l'infrastructure Tunnel-IP.com (prépend, localisation, blackhole, etc.).

La documentation complète des communities supportées est disponible ici : **BGP Communities**

---

9. Bonnes Pratiques

1. **Route objects** :
   - Maintenez vos route objects à jour dans la base IRR.
   - Utilisez un AS-SET cohérent qui regroupe tous vos préfixes.
   - Configurez le **RPKI (ROA)** pour vos préfixes afin de renforcer la sécurité de vos annonces.
2. **Filtrage** :
   - N'annoncez que les préfixes qui vous appartiennent.
   - Utilisez des filtres d'export stricts (n'exportez que vos préfixes via des `prefix-list` ou `filter`).
   - Mettez en place des filtres d'import pour ne pas accepter de routes indésirables.
3. **Blackhole** :
   - Créez toujours une route statique blackhole (`Null0`, `discard`, `blackhole`) pour chaque préfixe annoncé. Cela évite les boucles de routage.
4. **Monitoring** :
   - Surveillez l'état de vos sessions BGP régulièrement via le panel ou vos outils de monitoring.
   - Vérifiez le nombre de préfixes acceptés sur le panel.

Revision #2
Created 2026-03-30 14:53:45 UTC by Landry JUGE
Updated 2026-03-30 15:05:22 UTC by Landry JUGE