

## **Service Accès Partenaire au RIE**

### Documentation

## Table des matières

1	Vue d'ensemble.....	3
2	Objet.....	3
2	A qui s'adresse ce document.....	3
3	Descriptif du service.....	3
3.1	Architecture logique.....	3
3.2	Interconnexion RIE-RENATER.....	5
3.3	Raccordement des sites Partenaires.....	6
3.3.1	Interconnexion physique.....	6
3.3.2	Routage.....	7
4	Procédures d'exploitation.....	9
4.1	Mise en place du service.....	9
4.1.1	Nommage des interfaces.....	9
4.1.2	Base l2l3vpn.....	9
4.2.1	Supervision.....	10
4.2.2	Signalement des incidents.....	10
4.3	Rappel des contacts.....	13
5	Appendice.....	14
5.1	Liste des figures.....	14

## 1 Vue d'ensemble

Le réseau interministériel de l'État (RIE) raccorde l'ensemble des services de l'État sur le territoire national. Il assure, pour ces services, le transport des flux internes aux entités, les échanges sécurisés entre entités, ainsi que les échanges sécurisés avec les réseaux tiers, notamment Internet et le réseau inter-états membres de la Communauté Européenne (TESTA).

Les sites raccordés sur RENATER ayant besoin d'échanger avec le RIE peuvent bénéficier de l'offre accès partenaire au RIE. Les échanges reposent sur la mise en place d'un transport sur RENATER (circuit L3VPN entre le site et la plate-forme de service du RIE).

## 2 Objet

L'objet du présent document est de décrire :

- ✓ L'architecture technique mise en place pour interconnecter les établissements RENATER au RIE
- ✓ Les procédures d'exploitation de ce service

## 2 A qui s'adresse ce document

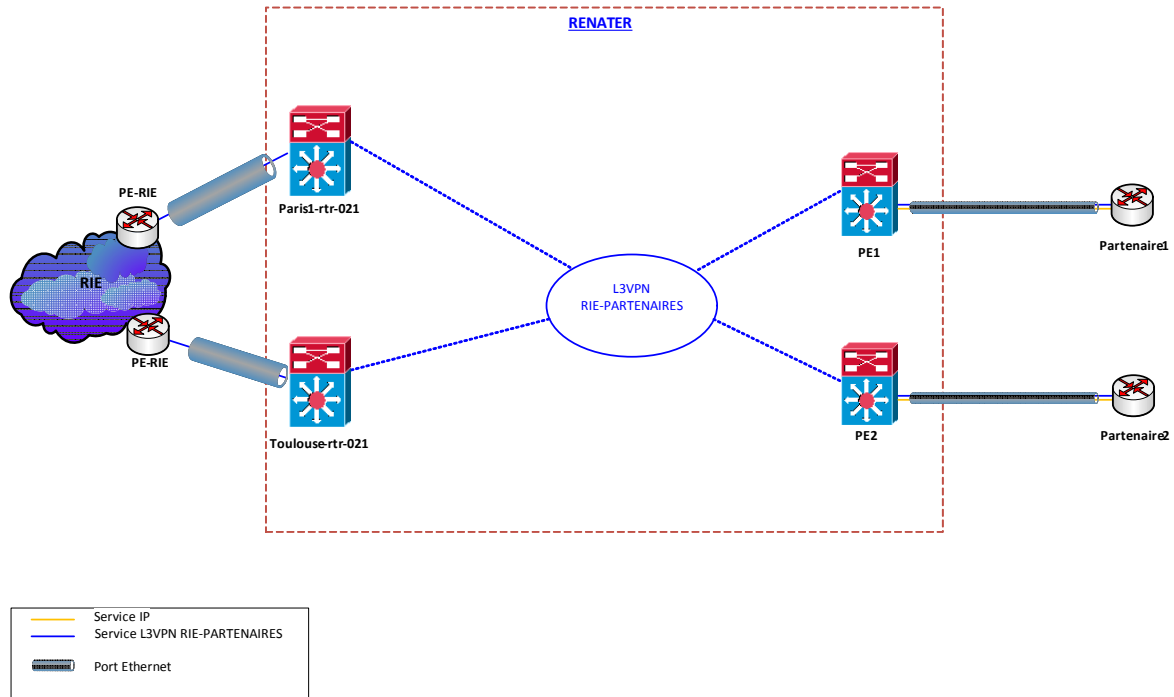
Ce document s'adresse :

- ✓ Aux utilisateurs du service
- ✓ Aux réseaux de collecte ayant des utilisateurs du service L3VPN de RENATER
- ✓ Aux équipes techniques du GIP RENATER
- ✓ Au NOC-RENATER

## 3 Descriptif du service

### 3.1 Architecture logique

Un VPN de niveau 3 de type « any-to-any » a été déployé pour interconnecter le RIE et ses partenaires raccordés sur RENATER.



**Figure 1 : VPN RIE-PARTENAIRES**

### **3.2 Interconnexion RIE-RENATER**

Deux circuits 10G optiques ont été déployés pour assurer une interconnexion redondante du RIE au backbone RENATER :

- ✓ PIB Paris1- NR Paris1
- ✓ PIB Bordeaux – NR Toulouse

Sur chaque routeur d'interconnexion RENATER, ont été configurés :

- ✓ Un port 10G dédié
- ✓ Un Vlan par VPN
- ✓ Une interconnexion IP (préfixes /30) par VPN alloué dans un bloc d'adresses RENATER
- ✓ Une session eBGP configuré entre les routeurs RIE et RENATER pour chaque VPN

Il s'agit de VPNs « any-to-any », RENATER n'applique donc aucun filtrage de routes sur ces sessions BGP.

Comme pour tout usager, RENATER met à disposition du RIE des communautés de services BGP permettant de déterminer lequel de ces accès est primaire ou secondaire.

- ✓ La communauté BGP 2200 :610 pour les routes annoncées sur l'accès primaire
- ✓ La communauté BGP 2200 :590 pour les routes annoncées sur l'accès secondaire

Sans utilisation de ces communautés, RENATER applique la même local-preference sur les préfixes reçus des PIBs Paris1 et Bordeaux. Le chemin préféré est alors celui dont le voisin BGP à l'adresse IP la plus petite, soit actuellement le routeur RENATER de Paris1.

### 3.3 Raccordement des sites Partenaires

#### 3.3.1 Interconnexion physique

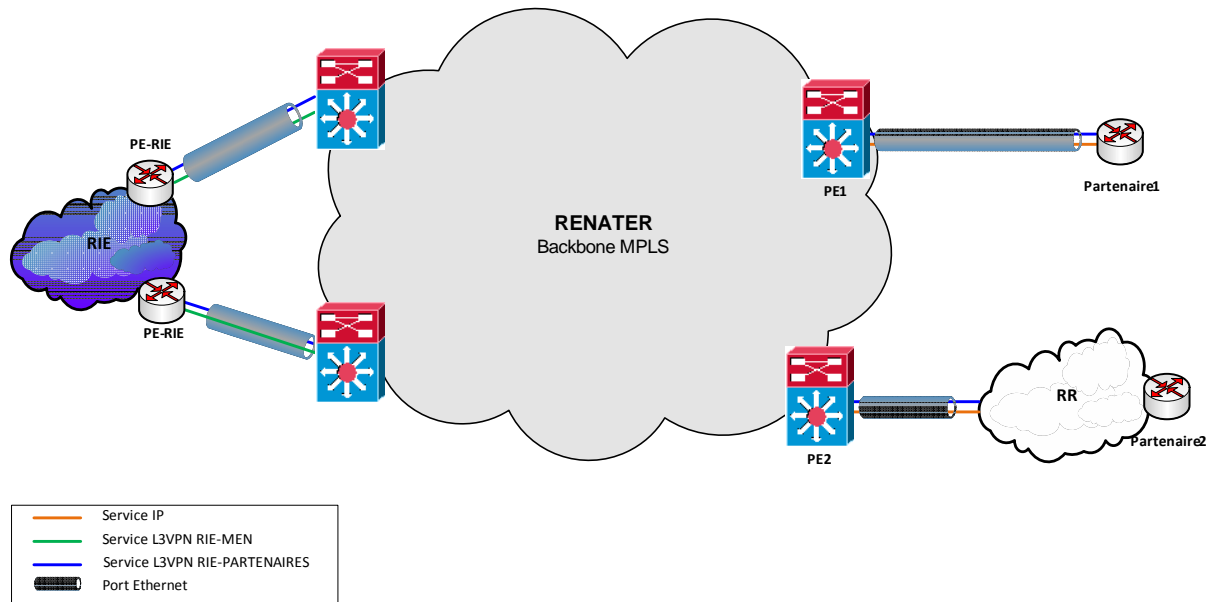


Figure 2 : Architecture physique L3VPN RIE-Partenaires

Les sites Partenaires peuvent être connectés à RENATER selon deux modes :

- ✓ Site en raccordement direct sur un routeur RENATER
- ✓ Site raccordé via un réseau de collecte

La connexion au RIE se fait au travers de l'accès existant du site Partenaire. Sur l'interface d'accès du site Partenaire ou celle du réseau de collecte, un VLAN dédié au service est ajouté.

#### **i** Remarque

Le Partenaire devra s'assurer que le service est transportable au travers de son réseau de collecte.

Une réunion tripartite Partenaire-Renater-Réseau de collecte pourra être organisée pour définir la solution technique.

### 3.3.2 Routage

Une session eBGP est établie entre le routeur RENATER et le routeur du site Partenaire.

La politique de routage en place sur RENATER est la suivante :

- ✓ VPNs « any-to-any »
- ✓ RENATER applique un filtrage de routes identique pour tous les accès Partenaire configuré, consistant à n'accepter que des routes issues du préfixe IP attribué par le SCN-RIE pour l'interconnexion ou le NAT (cf ci-dessous) ; ceci a pour but d'empêcher certains sites maladroits dans leur politique de routage d'annoncer dans le L3VPN RIE leurs préfixes RENATER, et par conséquent d'utiliser ce L3VPN comme support d'échange de flux pour ce qui relève du service IP de RENATER
- ✓ Maximum-prefix de 300 est appliqué en entrée sur RENATER
- ✓ Pour les sites « multihomés », les communautés de service sont disponibles pour priorisation des accès

Le site Partenaire réalise la translation d'adresses (NAT) entre son adressage interne et l'adressage du VPN Partenaires.

Le SCN RIE délègue à RENATER un préfixe qui est utilisé pour :

- ✓ L'interconnexion des sites partenaires à RENATER
- ✓ Le NAT : l'adresse d'interconnexion peut être utilisée pour réaliser cette opération. Cependant, pour les sites désirant un pool d'adresses plus important, un sous-réseau spécifique peut être alloué.



#### **Point d'attention**

Concernant le NAT, lorsqu'il n'y a pas d'hébergement par le Partenaire de ressources (flux entrants), mais uniquement utilisation de ressources RIE par le Partenaire (flux sortants), l'allocation par défaut est un /29, attribué par RENATER.

Si le Partenaire souhaite plus d'adresses, il sera renvoyé vers le SCN RIE qui indiquera alors au NOC RENATER la plage avec le masque retenu.

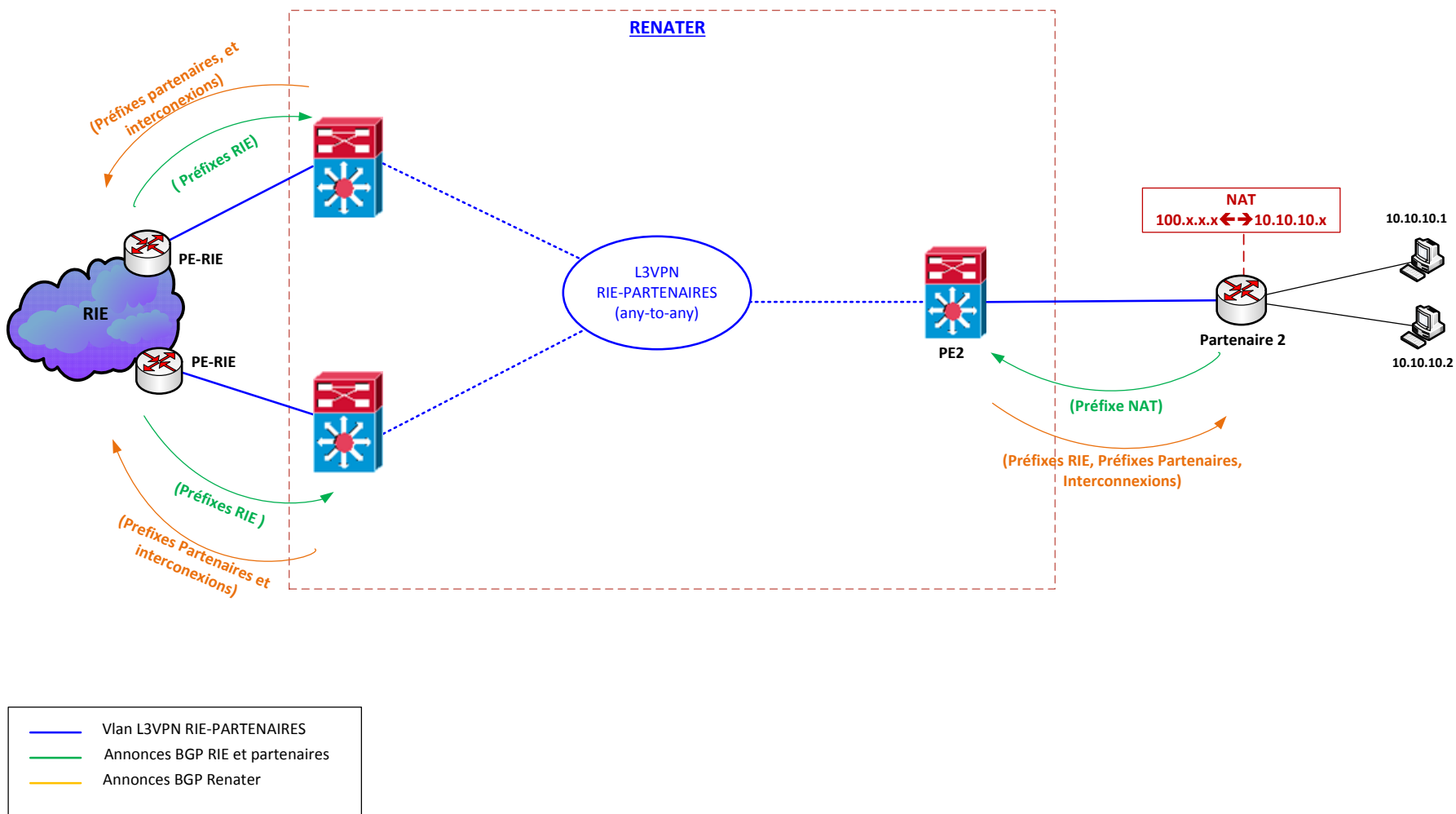


Figure 3 : Représentation logique L3VPN RIE-Partenaires



## 4 Procédures d'exploitation

### 4.1 Mise en place du service

Le NOC-RENATER est l'interface du site Partenaire pour la mise en place technique du service.

Le NOC-RENATER communique au site partenaire les informations techniques nécessaires pour son accès au service, à savoir :

- ✓ VLAN d'interconnexion
- ✓ Adressage IP d'interconnexion
- ✓ Adresses de NAT si besoin

#### 4.1.1 Nommage des interfaces

PSU doit fournir la description de l'interfaces au NOC-RENATER, description du nommage ci-dessous :

- -<type> <référence>-<id>-<RIE-PARTENAIRE-L3VPN>-<CODE SITE> (optionnel <(primaire/backup)>) ----

Exemple :

- -s13 5015-46-RIE-PARTENAIRE-L3VPN-U-LIMOGES (backup)----

#### 4.1.2 Base I2I3vpn

PSU doit enregistrer les circuits I2vpn/I3vpn dans la base I2I3vpn :

- <https://intranet.renater.fr/I2I3vpn/accueil/index.php>

Nomenclature d'enregistrement des circuits :

- Type : L2 ou L3
- Réf : référence 5015 pour les L3VPN RIE PARTENAIRES
- Description : RIE-PARTENAIRE-L3VPN-<CODE SITE>
- Dossier SAGA : Site dans saga.renater.fr
- Réseau SAGA : non utilisé
- NR raccordement : NR du site dans saga.renater.fr
- Type rac. : VLAN
- Interface : <type interface><port>.<numéro VLAN>
  - o Exemple : TenGigabitEthernet1/8.165
- Débit : débit de l'interface
  - o Exemple :10G

## 4.2 Gestion des incidents

### 4.2.1 Supervision

Le NOC-RENATER supervise le statut

- ✓ des interfaces d'accès
- ✓ des sessions eBGP

En cas de changement d'état d'un des éléments mentionnés au-dessus, le NOC-RENATER ouvrira un ticket d'incident et contactera le site concerné.

### 4.2.2 Signalement des incidents

Les incidents peuvent être de deux types :

1. Incident service : l'utilisateur n'accède plus à une ressource RIE
2. Incident routage : le routage des paquets n'est pas conforme

Il peut être difficile pour le site Partenaire de déterminer si l'origine du dysfonctionnement se trouve sur le périmètre RENATER ou le périmètre RIE.

C'est pourquoi le RIE a mis au point un processus nous permettant de valider la conformité du routage jusqu'à l'entrée du réseau RIE.

1. Tester l'accessibilité à la mire 1 : Annuaire MAIA

- ✓ URL : <http://annuaire.ader.gov.fr>
- ✓ Adresse IP : 161.48.25.223



2. Tester l'accessibilité à la mire 2 : Extranet RIE

- ✓ URL : <https://extranet-pub.noc.scn.rie.gov.fr>
- ✓ Adresse IP : [100.77.10.12](https://100.77.10.12)



3. Tester l'accessibilité aux serveurs DNS interministériels RIE sur les adresses suivantes :

- ✓ 100.77.2.20
- ✓ 100.77.6.20

Pour les flux web (http/https) la résolution DNS des URL « \*.ader.gouv.fr » ou « \*.rie.gouv.fr » est réalisée par les serveurs DNS du RIE, il est donc nécessaire de configurer vos DNS internes en mode « forward » vers ces équipements (100.77.2.20, 100.77.2.30, 100.77.6.20 et 100.77.6.30).

Avant de signaler un incident, le Partenaire devra tester qu'il accède bien aux mires et serveurs DNS du RIE :

- ✓ Si l'un des éléments n'est pas joignable, il s'agit d'un incident routage sur le périmètre RENATER. Le Partenaire contacte le NOC RENATER.
- ✓ Si l'un des éléments est joignable, il s'agit d'un incident service sur le périmètre RIE. Le Partenaire signale alors son incident au NOC RIE.

### **4.3 Rappel des contacts**

✓ **NOC-RENATER**

[noc-renater@noc.renater.fr](mailto:noc-renater@noc.renater.fr)

0800.77.47.95

✓ **Support technique de RENATER**

[support-reseau@renater.fr](mailto:support-reseau@renater.fr)

+33 1 53 94 20 40

✓ **NOC-RIE**

[noc-rie@pm.gouv.fr](mailto:noc-rie@pm.gouv.fr)

+33 2 99 32 59 00

## 5 Appendice

### 5.1 Liste des figures

Figure 1 : VPNs RIE-RENATER.....	5
Figure 2 : Architecture physique L3VPN RIE-Partenaires .....	7
Figure 3 : Représentation logique L3VPN RIE-Partenaires .....	8