RAPPORT DE STAGE

MAITRE DE STAGE : POSTY ALAIN

STAGIAIRE : BERNOIS DAMIEN

PERIODE : 8 JANVIER AU 23 FEVRIER 2024

Centre National de la Propriété Forestière

Table des matières

1. Remerciements

Je tiens tout d'abord à exprimer ma profonde gratitude envers toute l'équipe du CNPF, et en particulier à Alain Posty pour m'avoir offert l'opportunité d'effectuer ce stage au sein de leur structure et Sylvain Guichard pour avoir supervisé mes missions tout au long de mon stage.

Leur accueil chaleureux, leur encadrement attentif et leurs précieux conseils ont grandement contribué à enrichir mon expérience professionnelle et mes connaissances en informatique.

Mes remerciements s'adressent également à mes enseignants, dont les enseignements ont posé les bases de mes connaissances, et qui m'ont encouragé à saisir cette opportunité de stage pour mettre en pratique mes compétences.

Enfin, je tiens à exprimer ma reconnaissance envers ma famille et mes amis pour leur soutien indéfectible tout au long de cette expérience professionnelle.

Ce stage a été une véritable source d'enrichissement personnel et professionnel, et je suis reconnaissant envers toutes les personnes qui ont contribué à sa réussite.

2. Glossaire

- **Instance :** Une instance représente une entité de traitement virtuelle déployable sur le cloud AWS. Elle peut être ajustée en fonction des besoins spécifiques de l'application en termes de CPU, de mémoire et de stockage, offrant ainsi une grande adaptabilité. Elles peuvent être assimilées à des machines virtuelles (VM).

- **ACL :** Une ACL réseau, acronyme pour Access Control List, est un ensemble de règles de sécurité qui contrôlent le trafic entrant et sortant au niveau du sous-réseau ou d'une instance dans un VPC AWS. Ces règles permettent de spécifier comment le trafic est autorisé ou bloqué en fonction de divers critères tels que l'adresse IP source, l'adresse IP de destination, le protocole et le numéro de port.

- **AWS EC2 :** EC2, acronyme pour Amazon Elastic Compute Cloud, est service proposé par AWS, permet de louer des serveurs virtuels pour exécuter des applications. Les utilisateurs bénéficient d'une flexibilité totale pour choisir le type de serveur, le système d'exploitation, la capacité de stockage et la région géographique.

- **AWS VPC :** VPC, acronyme pour Amazon Virtual Private Cloud, est un service de réseau privé virtuel AWS qui permet aux utilisateurs de créer un environnement réseau isolé dans le cloud AWS avec un contrôle complet sur la configuration du réseau et la sécurité.

- **IGW :** Une IGW, acronyme d'Internet Gateway, est une passerelle permettant la communication entre les instances d'un VPC et Internet. Elle sert de point d'entrée et de sortie pour le trafic Internet.

- **VGW :** Une VGW, acronyme de Virtual Gateway, est une passerelle permettant aux instances de se connecter de façon sécurisée à un réseau d'entreprise ou un autre réseau externe via une connexion VPN. Elle sert de point de liaison crypté entre le VPC et les réseaux externes, ce qui permet une extension sécurisée du réseau de l'entreprise dans le cloud AWS.

- **SSH :** Le protocole SSH, acronyme de Secure Shell, est un protocole de communication sécurisé utilisé pour établir des connexions sécurisées et chiffrées entre des ordinateurs distants sur un réseau.

- **TGW :** Une TGW, acronyme de Transit Gateway, est un service qui permet de connecter de manière centralisée plusieurs VPC au sein d'un seul et même réseau. Elle sert de passerelle entre les VPC, simplifie la connectivité entre eux et permet un routage efficace du trafic entre eux, facilitant ainsi la gestion et l'évolutivité des infrastructures réseau sur AWS.

- **Attachement :** Un attachement est un lien qui connecte des ressources réseau telles que des VPC à un Transit Gateway sur AWS. Cela permet à la TGW de router efficacement le trafic entre ces différentes ressources.

- **Acheminement :** L'acheminement d'une TGW sur AWS définit comment le trafic est dirigé entre les différentes ressources connectées à la TGW.
- **Blackhole :** Un "blackhole" dans le contexte d'un Transit Gateway (TGW) sur AWS fait référence à une situation où le trafic destiné à une destination spécifique n'est pas routé et est donc perdu ou "absorbé" par le TGW sans être acheminé vers sa destination prévue. Cette situation peut être volontairement configurée.
- **AMI :** Une AMI, acronyme d'Amazon Machine Image, est une image d'un serveur virtuel déjà existant. Elle sert de modèle pour la création de nouvelles et facilite le déploiement rapide et en masse.
- **VPC-peering :** Le VPC Peering, acronyme de Virtual Private Cloud peering, est un moyen de connecter deux VPC de manière sécurisée au sein de la même région AWS. Cette connexion permet aux ressources dans ces VPC de communiquer entre elles comme si elles étaient sur le même réseau local, tout en maintenant l'isolement logique des réseaux.

3. Introduction

3.1. Présentation du stage

L'objectif de ce rapport de stage est de fournir une synthèse approfondie de ma période de stage au sein du CNPF. Cette immersion s'insère dans le contexte de ma formation en BTS SIO (services informatiques aux organisations), avec l'option axée sur les solutions d'infrastructure, systèmes et réseaux (SISR).

La finalité principale de ce stage est de concrétiser et d'approfondir les connaissances théoriques acquises au cours de mes études, tout en découvrant de nouvelles notions et en enrichissant mon expérience professionnelle.

Au cours de mon stage, j'ai eu l'opportunité de découvrir l'environnement du cloud AWS, d'assimiler de nouvelles notions et d'explorer ses possibilités. Des réseaux m'ont été mis à disposition pour effectuer des manipulations et des tests approfondis, permettant ainsi de mieux comprendre cet environnement et de remplir les missions qui m'ont été confiées. La découverte de cet environnement cloud a enrichi mes connaissances en réseau, mettant particulièrement l'accent sur le cloud computing.

3.2. Présentation du CNPF

3.2.1. Le CNPF

Le Centre National de la Propriété Forestière est l'organisme public responsable de la gestion de la forêt privée en France, représentant environ 75% des forêts du pays. Son rôle majeur est d'accompagner les 3,5 millions de propriétaires privés dans la gestion durable de leurs 12,6 millions d'hectares de forêts, soit 23% du territoire métropolitain.

Pour ce faire, il agrée les plans de gestion forestière, élabore des schémas régionaux et des codes de bonnes pratiques. Il conseille, informe et forme les propriétaires, notamment par des publications et des outils en ligne, pour promouvoir une gestion forestière efficace. Il encourage également le regroupement des petites parcelles forestières dispersées pour une exploitation plus efficace et durable, tout en contribuant à la recherche et à l'innovation dans des domaines tels que l'adaptation au changement climatique et l'amélioration génétique. Enfin, il sensibilise les propriétaires à l'importance de la préservation de la biodiversité forestière.

3.2.2. L’équipe du CNPF

La principale mission du Service du Développement Numérique (SDN) du CNPF est d'assurer la stabilité et la sécurité du système d'information, tout en développant des solutions logicielles innovantes spécifiquement adaptées pour améliorer les opérations des forestiers à travers toute la France.

L'équipe du SDN se distingue par sa diversité de compétences, qui englobe notamment le développement logiciel ainsi que l'administration des systèmes et des réseaux. Cette variété de compétences permet au SDN de répondre aux besoins et aux exigences des forestiers de manière efficace.

4. Missions

4.1. Présentation du besoin

Le CNPF a entrepris une révision de son infrastructure réseau sur le cloud AWS en raison du besoin d'évolution résultant d'un manque de sécurité, de fiabilité et d'organisation au sein de celui-ci.

Ma mission consiste à préparer la transition des machines du réseau actuel d'AWS vers un réseau futur mieux organisé, en utilisant des tests et des procédures appropriés.

En outre, j'ai été chargé(e) de mener une étude de cas sur leur infrastructure cloud AWS, d'examiner diverses solutions réseau évolutives pour répondre aux éventuels changements d'infrastructure, et de classifier les risques et les avantages liés à chacune de ces solutions.

4.2. Déroulement des missions

- Au cours des deux premières semaines, je me suis familiarisé avec l'environnement AWS, réalisé divers tests, et réussi à mettre en place mon propre réseau opérationnel. J'ai également documenté certaines fonctionnalités AWS et conçu des schémas réseau afin d'améliorer la compréhension globale de mes manipulations.

- Durant la troisième et quatrième semaine, j'ai documenté et testé une procédure de migration permettant de déplacer une instance (machine) d'un réseau à un autre sur AWS. L'objectif était de préparer la migration des machines du réseau AWS actuel du CNPF vers leur futur réseau. (! Une définition du terme instance se trouve dans le glossaire page 4 !)

  Pendant les cinquième et sixième semaines, j'ai eu l'opportunité d'analyser et de concevoir trois options d'infrastructure réseau sur AWS en utilisant les fonctionnalités disponibles. J'ai également recueilli, analyser et ajusté les règles ACL du réseau, ainsi que des informations sur les machines déjà présentes dans le réseau AWS actuel, dans le but de faciliter la future migration du réseau. (! Une définition du terme ACL se trouve dans le glossaire page 4 !)

- Finalement, la dernière semaine a été dédiée à finaliser mes tâches et à rédiger ce rapport.

5. Environnement Matériel et Technique

5.1. Communication

- **Talkspirit :** Talkspirit est une plateforme de réseau social conçue pour faciliter la communication et la collaboration au sein des entreprises. Cette application a été particulièrement utile pendant mon stage, notamment lorsque j'avais besoin de transmettre ou de récupérer des informations au sein de l'équipe CNPF.

5.2. Partage et Documentation

- **Google Drive :** Google Drive est une plateforme de travail collaboratif en ligne qui offre la possibilité de créer, stocker et partager des documents avec d'autres utilisateurs. Grâce à cette application en ligne, j'ai pu partager, stocker et éditer des documentations, tout en travaillant en étroite collaboration avec le deuxième stagiaire Alexandre Ernandez sur l'infrastructure du CNPF.

5.3. Schématisation

- **Draw.io :** Draw.io est un logiciel de diagrammes en ligne à la fois simple et robuste, offrant la possibilité de créer aisément des organigrammes, des schémas et bien d'autres éléments visuels. Grâce à cette application, j'ai pu schématiser mes procédures et tests sur AWS, ainsi que les diverses solutions d'infrastructure pour le réseau AWS à venir. Cela m'a permis de simplifier et de mieux comprendre l'architecture ainsi que certaines notions réseau d'AWS.

5.4. Services utilisés pour les missions

- **AWS :** AWS, acronyme pour Amazon Web Services, est une plateforme de cloud computing d'Amazon offrant une gamme étendue de services informatiques à la demande, tels que le stockage, le calcul et l'analyse de données, permettant aux entreprises de déployer et de gérer leurs applications avec flexibilité, évolutivité et sécurité.
  Au cours de mon stage, j'ai utilisé les services EC2 et VPC d'AWS pour accomplir mes tâches avec succès. (! Une définition des termes EC2 et VPC se trouve dans le glossaire page 4 !)

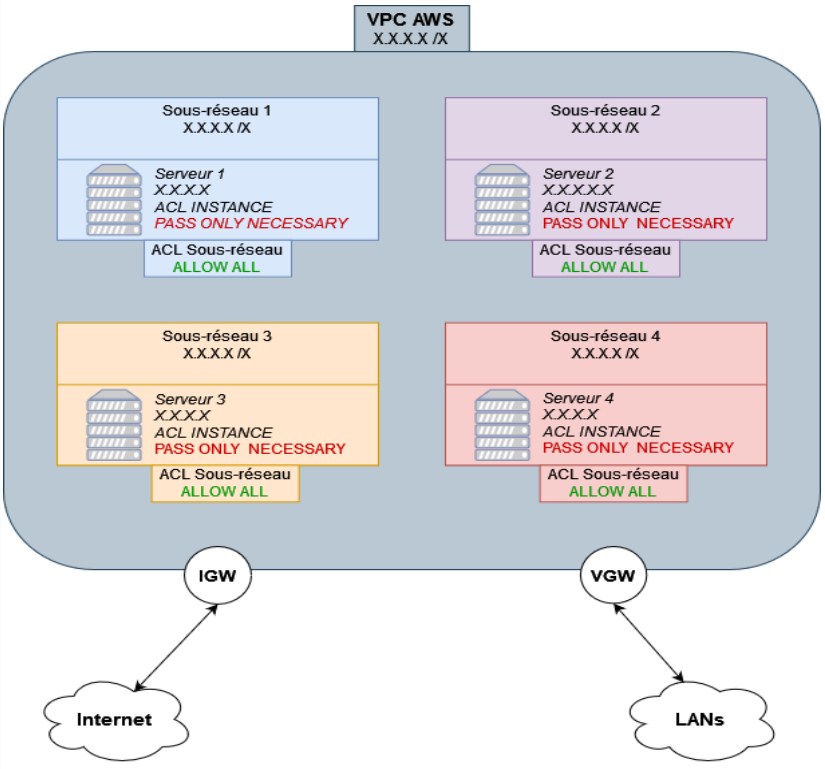
6. Contexte du projet AWS du CNPF

6.1. Infrastructure AWS actuel

Le CNPF utilise un environnement AWS pour héberger certains de ses services. Actuellement, tous les services AWS du CNPF sont regroupés dans un VPC unique, où se trouvent également leurs serveurs opérationnels, de test et autres. Cette approche d'infrastructure présente diverses contraintes en termes de sécurité, tel que :

- La structure du réseau est très simplifiée, avec tous les serveurs localisés dans le même VPC mais dispersés à travers divers sous-réseaux. Cette disposition peut entraîner des complications en ce qui concerne la gestion des différents services et la limitation des interactions et des communications entre les serveurs et les sous-réseaux.
- La sécurité entre les serveurs et les sous-réseaux de cet unique VPC est seulement réglementée par des ACL (ACL réseau et ACL machine). Cette méthode peut rapidement devenir complexe en termes d'organisation et de suivi des règles, augmentant le risque d'oublier certaines règles de sécurité primordiales.

On peut schématiser le réseau AWS actuel du CNPF de cette façon :



Tous les serveurs AWS du CNPF sont regroupés dans un seul VPC, répartis dans divers sous-réseaux.

Les ACL des sous-réseaux sont configurées en mode "ALLOW ALL", ce qui signifie qu'elles autorisent le passage de toutes les trames entrantes et sortantes au sein du sous-réseau.

En fin de compte, seules les ACL machine jouent un rôle effectif en matière de sécurité pour les instances. Elles sont les seules à être configurées de manière à n'autoriser que les protocoles utilisés à communiquer avec les serveurs.

(! Une définition des termes IGW et VGW se trouve dans le glossaire page 4 !)

Cette approche d'infrastructure met en évidence des lacunes en termes de sécurité et de fiabilité, c'est pourquoi le CNPF a décidé de revoir son infrastructure cloud afin d'assurer la sécurité, l'efficacité et la disponibilité des services du CNPF déployés sur AWS.

6.2. Future infrastructure AWS

Le CNPF envisage une refonte complète de son infrastructure AWS et la migration de chaque serveur de l'infrastructure actuelle vers la nouvelle. Avant de procéder à cette refonte, des études doivent être menées pour déterminer la solution la plus efficace en termes de sécurité, de fiabilité et de rentabilité.

C'est pourquoi le CNPF m'a confié la mission de m'approprier l'environnement cloud AWS, de comprendre ses principes et ses possibilités, et d'étudier les différentes solutions d'infrastructure qui répondent à leurs besoins.

7. Familiarisation avec l'environnement AWS

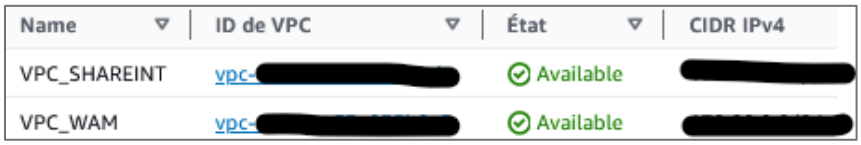
7.1. Création des réseaux et des instances

Pour me familiariser avec l'environnement AWS, j'ai eu accès à de nombreuses documentations AWS grâce à un accès à l'environnement cloud. Ces documents m'ont fourni des explications détaillées et des schémas illustratifs sur les principes fondamentaux et le fonctionnement du réseau cloud sur AWS. Après cela, j'ai pu commencer à effectuer des tests en utilisant deux VPC déjà existants.

Je vais créer deux instances AWS dans deux sous-réseaux de deux VPC distincts et configurer leur communication mutuelle.

- Afin que 2 instances puissent communiquer entre elles, il faut tout d'abord qu'elles soient au sein d'un réseau (et d'un sous-réseau) :

  - Les deux VPC utilisés :



  - Les deux sous-réseaux utilisés (chacun dans un VPC différent) :

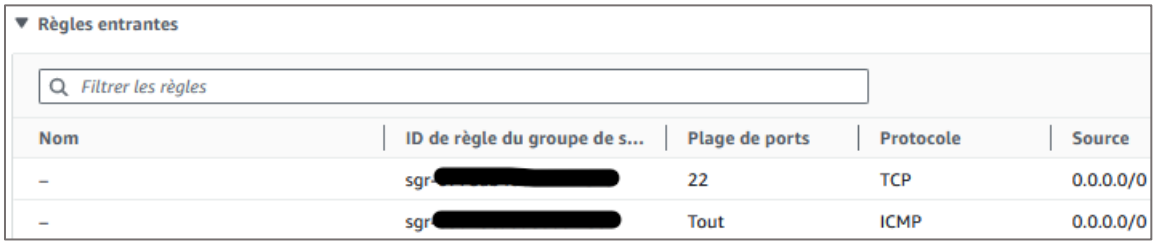
  - Les deux instances créées :

Télécharger les clés SSH afin de pouvoir s'y connecter via le terminal.

7.2. Connexion aux instances

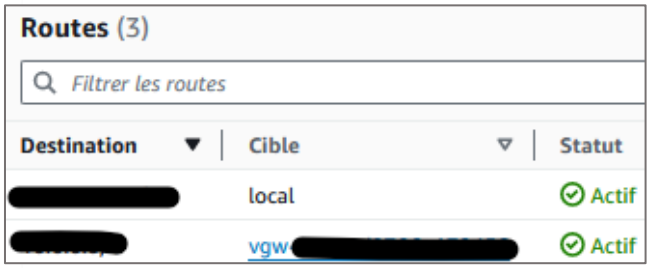
- Pour permettre la connexion à l'instance depuis une machine sur le réseau d'entreprise (LAN), il est nécessaire d'autoriser les requêtes SSH entrantes. De plus, il est important de configurer une VGW pour permettre aux réseaux externes d'accéder au VPC :

- Autoriser les requêtes SHH entrantes (attention à la source si le VPC à une IGW) :



(! Une définition du terme SSH se trouve dans le glossaire page 4 !)

- Pour permettre l'accès aux deux VPC depuis un réseau externe, il est nécessaire de créer une VGW pour chaque VPC où sont situées les instances. Cette opération implique d'ajouter la VGW préalablement créée dans la table de routage des deux VPC concernés.

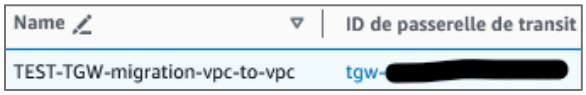


Ajouter une route sur le VPC en question où la VGW point vers un réseau externe.

7.3. Communication entre les deux VPC

➢ Pour permettre la communication entre les deux VPC, il est nécessaire de mettre en place une TGW qui agira comme un point central entre les VPC. Cela permettra aux instances situées dans des VPC différents de communiquer entre eux :

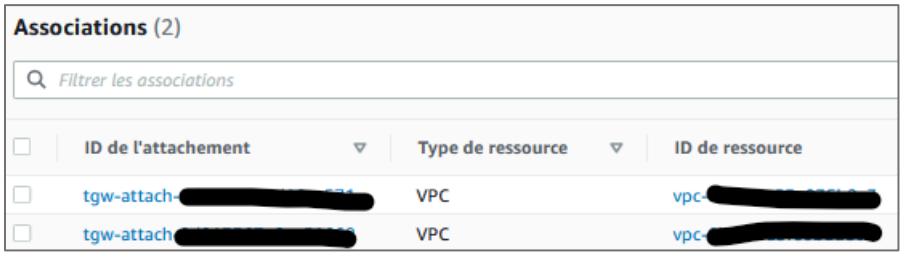
- Créer la TGW :



- Créer les attachements :

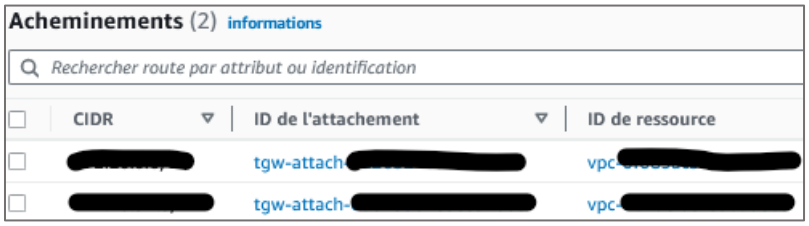
(! Une définition du terme attachement TGW se trouve dans le glossaire page 4 !)

- Liaison des attachements à la TGW :



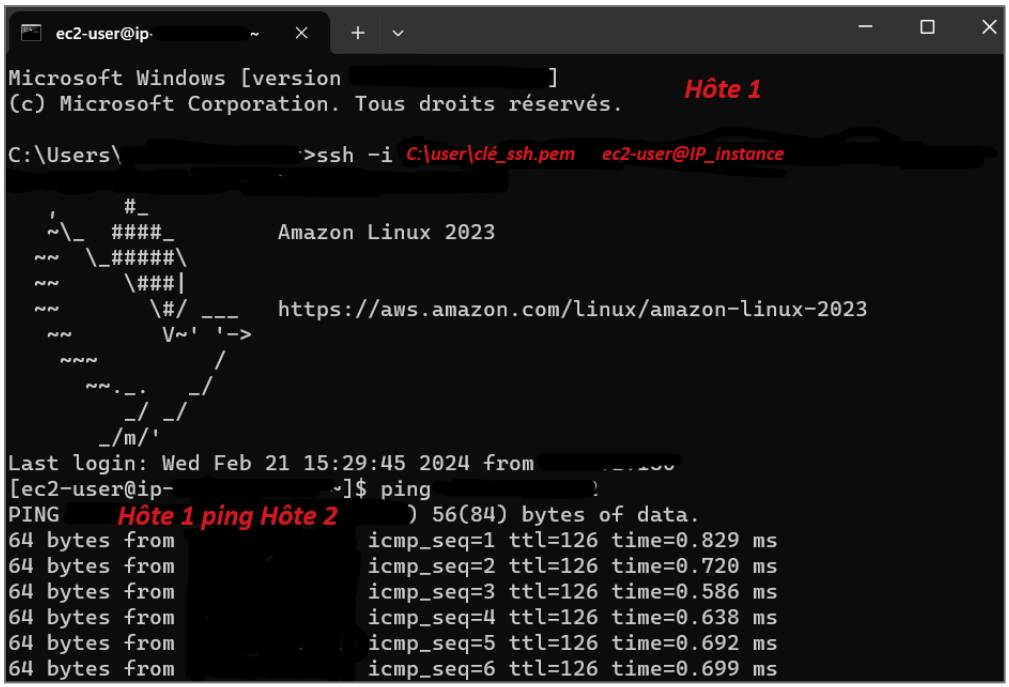
- Acheminements de la TGW :

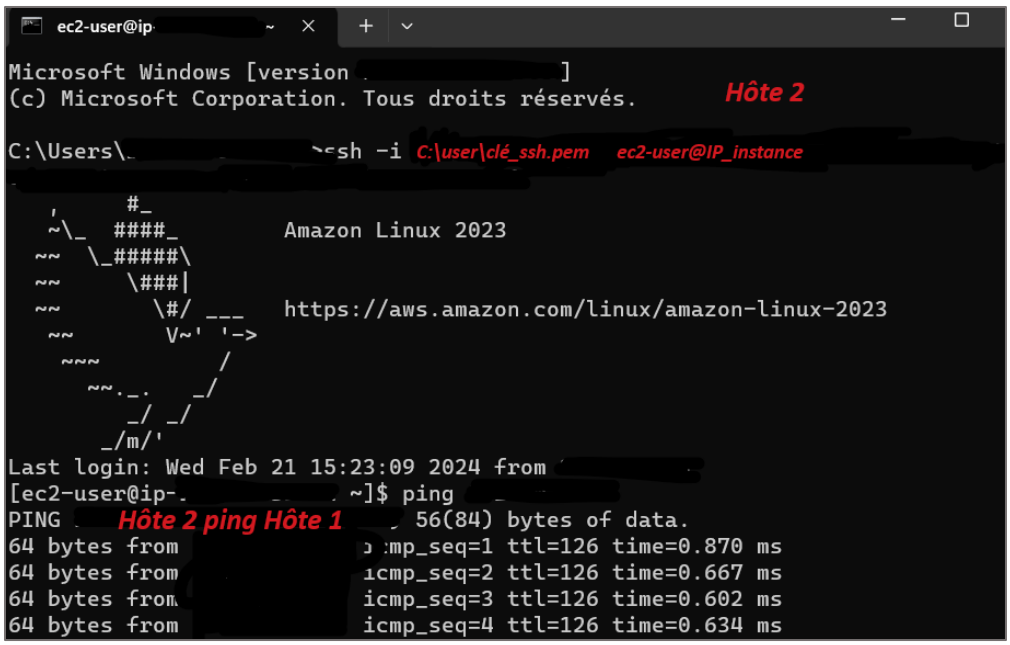
(! Une définition du terme acheminement TGW se trouve dans le glossaire page 5 !)



7.4. Vérification de la communication des deux instances

➢ Connexion aux deux instances à l'aide du terminal de ma machine :





Ici, les 2 instances Hôte 1 et Hôte 2 arrivent bien à communiquer entre eux en étant dans 2 VPC différents à l'aide de la TGW.

7.5. Approfondissement TGW

Suite à ces nombreux tests fonctionnels, j'ai pu approfondir les possibilités de manipulation avec la TGW mise en place, tel qu'introduire la notion de blackhole (trou noir) TGW.

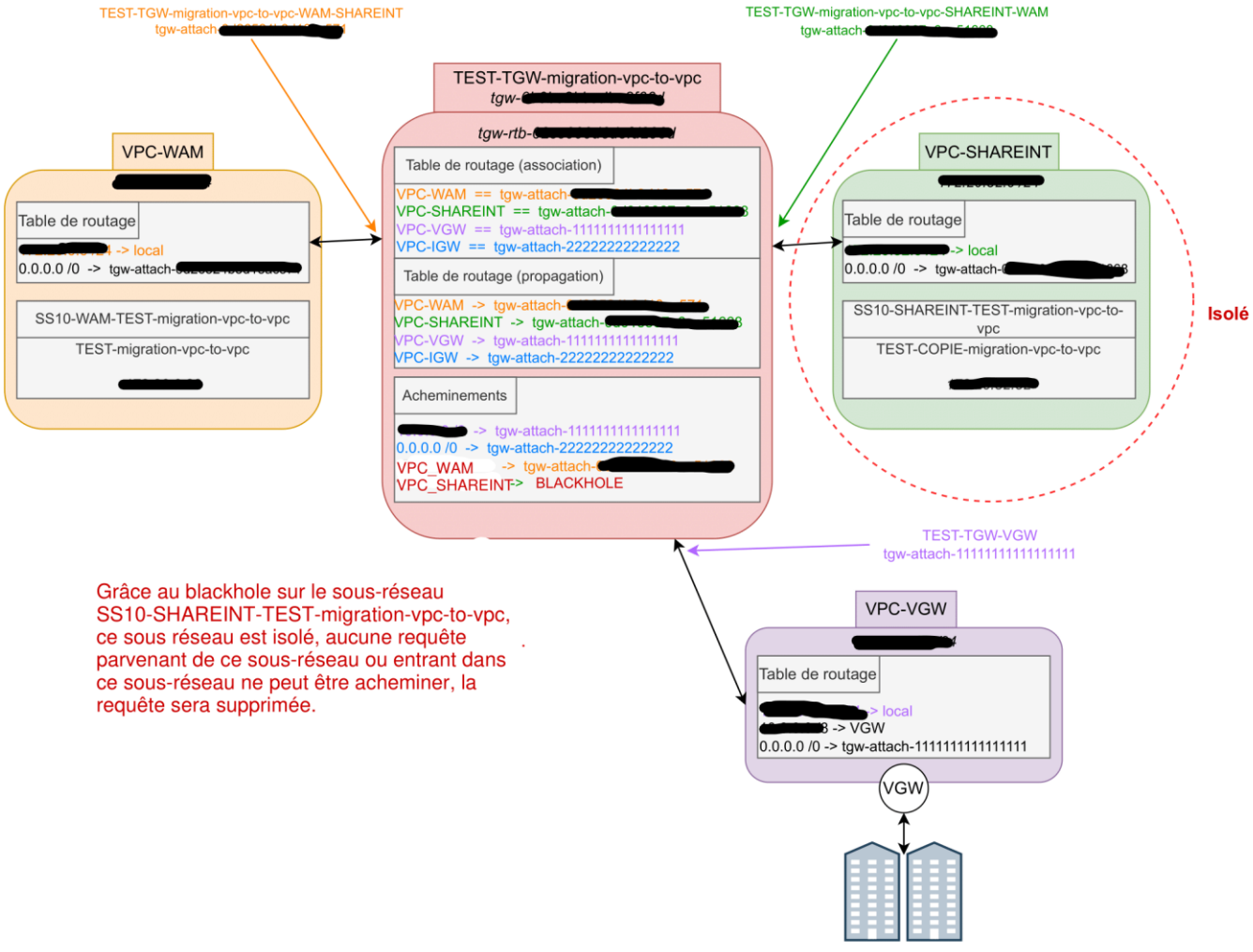
(! Une définition du terme blackhole TGW se trouve dans le glossaire page 5 !)

Acheminements (3) informations

Rechercher route par attribut ou identification

CIDR	ID de l'attachement	ID de ressource	Type de ressource	Type d'acheminement	État de l'acheminement
[redacted]	tgw-attach-[redacted]	vpc-[redacted]	VPC	Propagé	Actif
[redacted]	tgw-attach-[redacted]	vpc-[redacted]	VPC	Propagé	Actif
SS10-SHAREINT-TEST-migration-vpc-to-vpc	–	–	–	Statique	Blackhole

- Voici un schéma représentant le réseau complet que j'ai pu créer sur AWS, la fonctionnalité d'une TGW, avec l'utilisation du blackhole à l'aide de la TGW :



8. Procédure de migration d'une instance entre VPC

Pour migrer toutes les machines du réseau AWS existant vers le nouveau réseau du CNPF, j'ai dû effectuer des tests et élaborer une procédure visant à garantir la fiabilité et l'intégrité des données lors de la migration d'une instance vers un nouveau VPC.

Durant ces essais, j'ai exploité les réseaux, sous-réseaux et instances déjà présents afin d'éviter de surcharger le réseau AWS du CNPF.

- Dans un premier cas, j'ai créé un fichier test sur l'instance hôte 1 :

```
C:\Users\                >ssh -i C:\user\clé_shh.pem    ec2-user@IP_instance
                                                              Hôte 1
       #_
       ~\_  ####_        Amazon Linux 2023
      ~~  \_#####\
      ~~     \###|
      ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
       ~~       V~' '->
        ~~~         /
          ~~._.   _/
             _/ _/
           _/m/'
Last login: Thu Feb 22 09:13:44 2024 from
[ec2-user@ip-          ~]$ touch test
[ec2-user@ip-          ~]$ ls
test
```

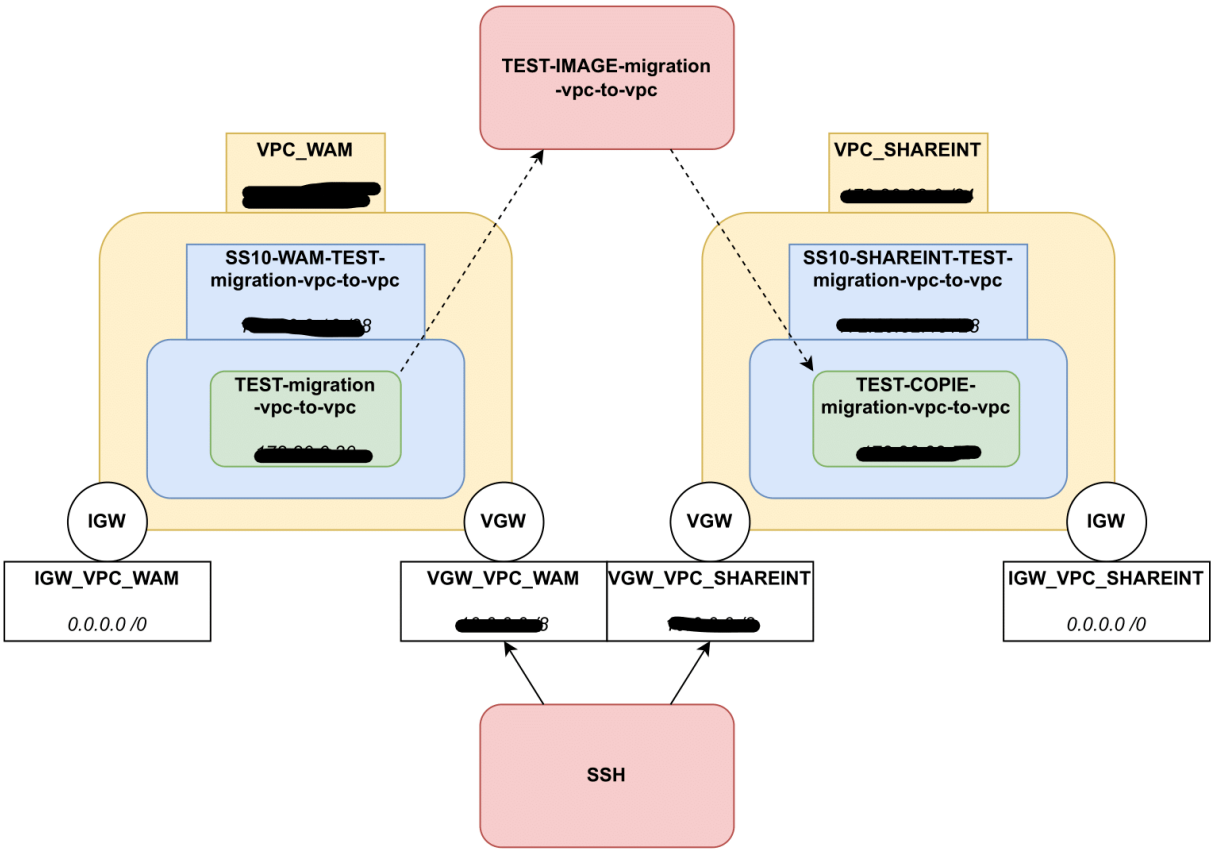
- Suite à la création du fichier test sur l'instance source, j'ai créé une AMI à partir de cette dernière :
  (! Une définition du terme AMI se trouve dans le glossaire page 5 !)

Name	Nom de l'AMI	ID AMI	Source
	TEST-COPIE-migration-vpc-to-vpc	ami[redacted]	[redacted]/TEST-COPIE-migration...

- Création de l'instance copie à partir de l'AMI de l'instance source et vérification de l'intégrité des données :

```
C:\Users\                >ssh -i C:\user\clé_shh.pem    ec2-user@IP_instance
                                                              Hôte 2
       #_
       ~\_  ####_        Amazon Linux 2023
      ~~  \_#####\
      ~~     \###|
      ~~       \#/ ___   https://aws.amazon.com/linux/amazon-linux-2023
       ~~       V~' '->
        ~~~         /
          ~~._.   _/
             _/ _/
           _/m/'
Last login: Wed Feb 21 15:30:00 2024 from
[ec2-user@ip-          ~]$ ls
test
```

- Voici un schéma représentant les manipulations effectué lors des tests de la migration d'une instance d'un VPC à un autre :



9. Étude et évolution d'une solution pour la nouvelle infrastructure réseau AWS du CNPF

9.1. Première solution d'infrastructure

Le directeur des systèmes d'information du CNPF, Alain Posty, a suggéré cette première solution d'infrastructure réseau. J'ai donc pris en charge sa modélisation, son analyse, ainsi que la compréhension des enjeux et des concepts associés tels que le VPC-peering. De plus, j'ai évalué ses avantages et ses inconvénients.

(! Une définition du terme VPC-peering se trouve dans le glossaire page 5 !)

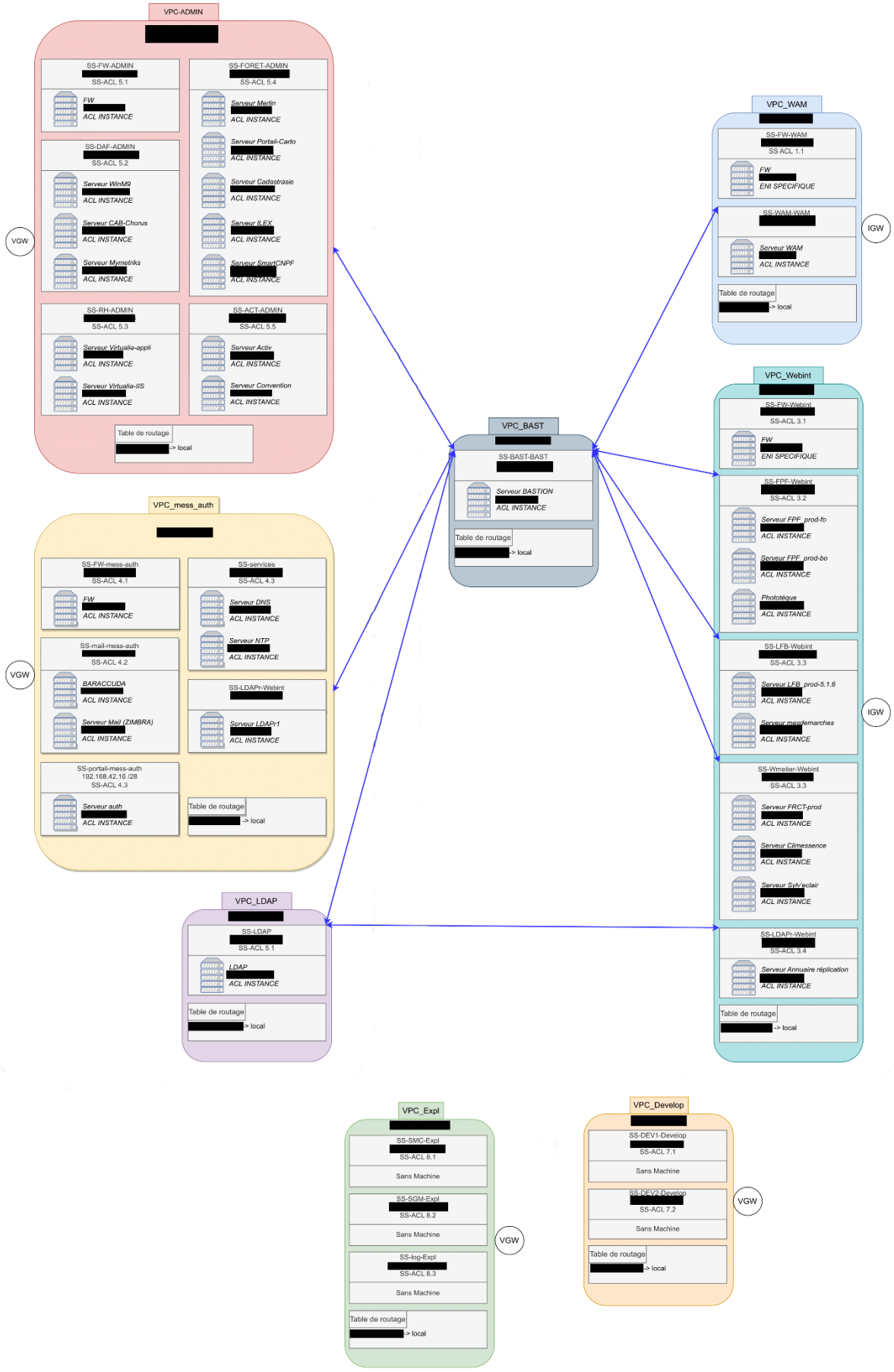
Dans cette configuration d'infrastructure, certains serveurs doivent échanger des données au sein du réseau CNPF. Les VPC Peering servent de liaison directe entre les machines nécessitant une communication et ne se trouvant pas dans le même réseau.

Toutefois, les VPC Peering n'offrent pas de sécurité intrinsèque, autorisant le passage de toutes les trames ou protocoles du point A au point B. C'est donc grâce aux ACL réseau ou aux ACL machine que le filtrage des différentes trames en circulation est assuré.

En analysant cette solution qui utilise des VPC-peering, j'ai identifié les avantages et les inconvénients suivants :

- Avantages :
  - Les frais des VPC-peering sont basés uniquement sur le volume de données transférées.
  - Il n'existe aucune restriction de bande passante.
  - Il est possible d'établir jusqu'à 125 connexions sur un même VPC.
  - Il est envisageable de créer des VPC-peering entre différentes régions et comptes AWS.

- Inconvénients :
  - Chaque ajout de VPC accroît la complexité du réseau.
  - La visibilité est restreinte (seulement les journaux de flux VPC) par rapport à TGW.
  - Les tables de routage sont plus complexes à gérer que celles de TGW et ne permettent pas le transit de routage.
  - Les chemins directs des VPC-peering ne bénéficient d'aucune sécurité.
  - Il n'est pas possible de créer des VPC-peering entre des VPC déjà en peering.


VPC-ADMIN
[redacted]
SS-FW-ADMIN
[redacted]
SS-ACL 5.1
FW
[redacted]
ACL INSTANCE
SS-FORET-ADMIN
[redacted]
SS-ACL 5.4
Serveur Merlin
[redacted]
ACL INSTANCE
Serveur Portail-Carto
[redacted]
ACL INSTANCE
Serveur Cadastrasie
ACL INSTANCE
Serveur ILEX
ACL INSTANCE
Serveur SmartCNPF
[redacted]
ACL INSTANCE
SS-DAF-ADMIN
[redacted]
SS-ACL 5.2
Serveur WinM9
[redacted]
ACL INSTANCE
Serveur CAB-Chorus
[redacted]
ACL INSTANCE
Serveur Mymetriks
[redacted]
ACL INSTANCE
SS-RH-ADMIN
[redacted]
SS-ACL 5.3
Serveur Virtualia-appli
[redacted]
ACL INSTANCE
Serveur Virtualia-IIS
[redacted]
ACL INSTANCE
SS-ACT-ADMIN
[redacted]
SS-ACL 5.5
Serveur Activ
[redacted]
ACL INSTANCE
Serveur Convention
[redacted]
ACL INSTANCE
Table de routage
[redacted] -> local
VGW
VPC_WAM
[redacted]
SS-FW-WAM
[redacted]
SS ACL 1.1
FW
[redacted]
ENI SPECIFIQUE
SS-WAM-WAM
[redacted]
Serveur WAM
[redacted]
ACL INSTANCE
Table de routage
[redacted] -> local
IGW
VPC_BAST
[redacted]
SS-BAST-BAST
[redacted]
Serveur BASTION
[redacted]
ACL INSTANCE
Table de routage
[redacted] -> local
VPC_Webint
[redacted]
SS-FW-Webint
[redacted]
SS-ACL 3.1
FW
[redacted]
ENI SPECIFIQUE
SS-FPF-Webint
[redacted]
SS-ACL 3.2
Serveur FPF_prod-fo
[redacted]
ACL INSTANCE
Serveur FPF_prod-bo
[redacted]
ACL INSTANCE
Photothèque
[redacted]
ACL INSTANCE
SS-LFB-Webint
[redacted]
SS-ACL 3.3
Serveur LFB_prod-5.1.6
[redacted]
ACL INSTANCE
Serveur mesdemarches
[redacted]
ACL INSTANCE
SS-Wmetier-Webint
[redacted]
SS-ACL 3.3
Serveur FRCT-prod
[redacted]
ACL INSTANCE
Serveur Climessence
[redacted]
ACL INSTANCE
Serveur Sylvéclair
[redacted]
ACL INSTANCE
SS-LDAPr-Webint
[redacted]
SS-ACL 3.4
Serveur Annuaire réplication
[redacted]
ACL INSTANCE
Table de routage
[redacted] -> local
IGW
VPC_mess_auth
[redacted]
SS-FW-mess-auth
[redacted]
SS-ACL 4.1
FW
[redacted]
ACL INSTANCE
SS-services
[redacted]
SS-ACL 4.3
Serveur DNS
[redacted]
ACL INSTANCE
Serveur NTP
[redacted]
ACL INSTANCE
SS-mail-mess-auth
[redacted]
SS-ACL 4.2
BARACCUDA
[redacted]
ACL INSTANCE
Serveur Mail (ZIMBRA)
[redacted]
ACL INSTANCE
SS-LDAPr-Webint
[redacted]
Serveur LDAPr1
[redacted]
ACL INSTANCE
SS-portail-mess-auth
192.168.42.16 /28
SS-ACL 4.3
Serveur auth
[redacted]
ACL INSTANCE
Table de routage
[redacted] -> local
VGW
VPC_LDAP
[redacted]
SS-LDAP
[redacted]
SS-ACL 5.1
LDAP
[redacted]
ACL INSTANCE
Table de routage
[redacted] -> local
VPC_Expl
[redacted]
SS-SMC-Expl
[redacted]
SS-ACL 8.1
Sans Machine
SS-SGM-Expl
[redacted]
SS-ACL 8.2
Sans Machine
SS-log-Expl
[redacted]
SS-ACL 8.3
Sans Machine
Table de routage
[redacted] -> local
VGW
VPC_Develop
[redacted]
SS-DEV1-Develop
[redacted]
SS-ACL 7.1
Sans Machine
SS-DEV2-Develop
[redacted]
SS-ACL 7.2
Sans Machine
Table de routage
[redacted] -> local
VGW

9.2. Deuxième solution d'infrastructure

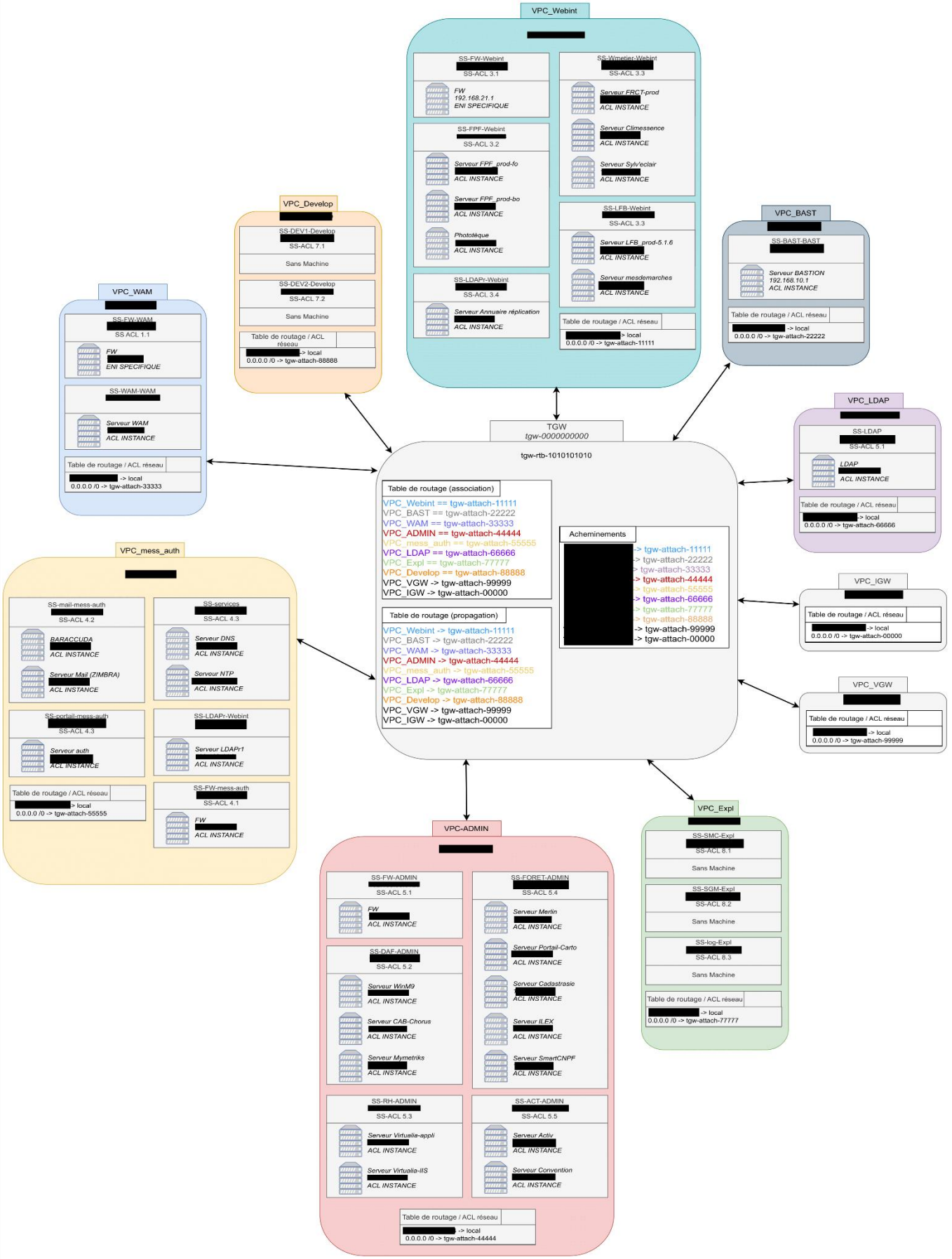
Après avoir étudié la première solution d'infrastructure présentée par Alain Posty et en utilisant les connaissances acquises sur les services AWS lors de mon stage, j'ai envisagé une deuxième solution d'infrastructure qui exploiterait la technologie d'une Transit Gateway AWS.

Dans cette configuration, nous résoudrons les problèmes de routage et de sécurité associés aux VPC-peering, car les requêtes pourront être acheminées de manière fiable et sécurisée grâce aux routes de la TGW. La TGW agira comme un point central pour tous les flux entre les VPC.

En analysant cette solution qui utilise une TGW, j'ai identifié les avantages et les inconvénients suivants :

- Avantages :
    - Permet une capacité supérieure en termes de VPC par région par rapport au peering VPC.
    - Offre une visibilité améliorée grâce à la gestion du réseau et aux journaux de flux.
    - Facilite la gestion des tables de routage et permet le transit de routage.
    - Permet l'isolation des VPC.
    - Les IGW et VGW sont centralisés en un point, évitant la redondance.

- Inconvénients :
    - Un ajout supplémentaire d'une TGW après celle-ci engendrera un délai supplémentaire.
    - Les frais sont basés sur le coût horaire par TGW, ainsi que sur le traitement et le transfert des données.


VPC_Webint
SS-FW-Webint
SS-ACL 3.1
FW
192.168.21.1
ENI SPECIFIQUE
SS-FPF-Webint
SS-ACL 3.2
Serveur FPF_prod-fo
ACL INSTANCE
Serveur FPF_prod-bo
ACL INSTANCE
Photothèque
ACL INSTANCE
SS-LDAPr-Webint
SS-ACL 3.4
Serveur Annuaire réplication
ACL INSTANCE
SS-Wmetier-Webint
SS-ACL 3.3
Serveur FRCT-prod
ACL INSTANCE
Serveur Climessence
ACL INSTANCE
Serveur Sylv'eclair
ACL INSTANCE
SS-LFB-Webint
SS-ACL 3.3
Serveur LFB_prod-5.1.6
ACL INSTANCE
Serveur mesdemarches
ACL INSTANCE
Table de routage / ACL réseau
-> local
0.0.0.0 /0 -> tgw-attach-11111
VPC_Develop
SS-DEV1-Develop
SS-ACL 7.1
Sans Machine
SS-DEV2-Develop
SS-ACL 7.2
Sans Machine
Table de routage / ACL réseau
-> local
0.0.0.0 /0 -> tgw-attach-88888
VPC_BAST
SS-BAST-BAST
Serveur BASTION
192.168.10.1
ACL INSTANCE
Table de routage / ACL réseau
-> local
0.0.0.0 /0 -> tgw-attach-22222
VPC_WAM
SS-FW-WAM
SS ACL 1.1
FW
ENI SPECIFIQUE
SS-WAM-WAM
Serveur WAM
ACL INSTANCE
Table de routage / ACL réseau
-> local
0.0.0.0 /0 -> tgw-attach-33333
TGW
tgw-0000000000
tgw-rtb-1010101010
Table de routage (association)
VPC_Webint == tgw-attach-11111
VPC_BAST == tgw-attach-22222
VPC_WAM == tgw-attach-33333
VPC_ADMIN == tgw-attach-44444
VPC_mess_auth == tgw-attach-55555
VPC_LDAP == tgw-attach-66666
VPC_Expl == tgw-attach-77777
VPC_Develop == tgw-attach-88888
VPC_VGW -> tgw-attach-99999
VPC_IGW -> tgw-attach-00000
Table de routage (propagation)
VPC_Webint -> tgw-attach-11111
VPC_BAST -> tgw-attach-22222
VPC_WAM -> tgw-attach-33333
VPC_ADMIN -> tgw-attach-44444
VPC_mess_auth -> tgw-attach-55555
VPC_LDAP -> tgw-attach-66666
VPC_Expl -> tgw-attach-77777
VPC_Develop -> tgw-attach-88888
VPC_VGW -> tgw-attach-99999
VPC_IGW -> tgw-attach-00000
Acheminements
-> tgw-attach-11111
-> tgw-attach-22222
-> tgw-attach-33333
-> tgw-attach-44444
-> tgw-attach-55555
-> tgw-attach-66666
-> tgw-attach-77777
-> tgw-attach-88888
-> tgw-attach-99999
-> tgw-attach-00000
VPC_LDAP
SS-LDAP
SS-ACL 5.1
LDAP
ACL INSTANCE
Table de routage / ACL réseau
-> local
0.0.0.0 /0 -> tgw-attach-66666
VPC_IGW
Table de routage / ACL réseau
-> local
0.0.0.0 /0 -> tgw-attach-00000
VPC_VGW
Table de routage / ACL réseau
-> local
0.0.0.0 /0 -> tgw-attach-99999
VPC_mess_auth
SS-mail-mess-auth
SS-ACL 4.2
BARACCUDA
ACL INSTANCE
Serveur Mail (ZIMBRA)
ACL INSTANCE
SS-services
SS-ACL 4.3
Serveur DNS
ACL INSTANCE
Serveur NTP
ACL INSTANCE
SS-portail-mess-auth
SS-ACL 4.3
Serveur auth
ACL INSTANCE
SS-LDAPr-Webint
Serveur LDAPr1
ACL INSTANCE
Table de routage / ACL réseau
-> local
0.0.0.0 /0 -> tgw-attach-55555
SS-FW-mess-auth
SS-ACL 4.1
FW
ACL INSTANCE
VPC-ADMIN
SS-FW-ADMIN
SS-ACL 5.1
FW
ACL INSTANCE
SS-FORET-ADMIN
SS-ACL 5.4
Serveur Merlin
ACL INSTANCE
Serveur Portail-Carto
ACL INSTANCE
Serveur Cadastrasie
ACL INSTANCE
Serveur ILEX
ACL INSTANCE
Serveur SmartCNPF
ACL INSTANCE
SS-DAF-ADMIN
SS-ACL 5.2
Serveur WinM9
ACL INSTANCE
Serveur CAB-Chorus
ACL INSTANCE
Serveur Mymetriks
ACL INSTANCE
SS-RH-ADMIN
SS-ACL 5.3
Serveur Virtualia-appli
ACL INSTANCE
Serveur Virtualia-IIS
ACL INSTANCE
SS-ACT-ADMIN
SS-ACL 5.5
Serveur Activ
ACL INSTANCE
Serveur Convention
ACL INSTANCE
Table de routage / ACL réseau
-> local
0.0.0.0 /0 -> tgw-attach-44444
VPC_Expl
SS-SMC-Expl
SS-ACL 8.1
Sans Machine
SS-SGM-Expl
SS-ACL 8.2
Sans Machine
SS-log-Expl
SS-ACL 8.3
Sans Machine
Table de routage / ACL réseau
-> local
0.0.0.0 /0 -> tgw-attach-77777

9.3. Troisième solution d'infrastructure

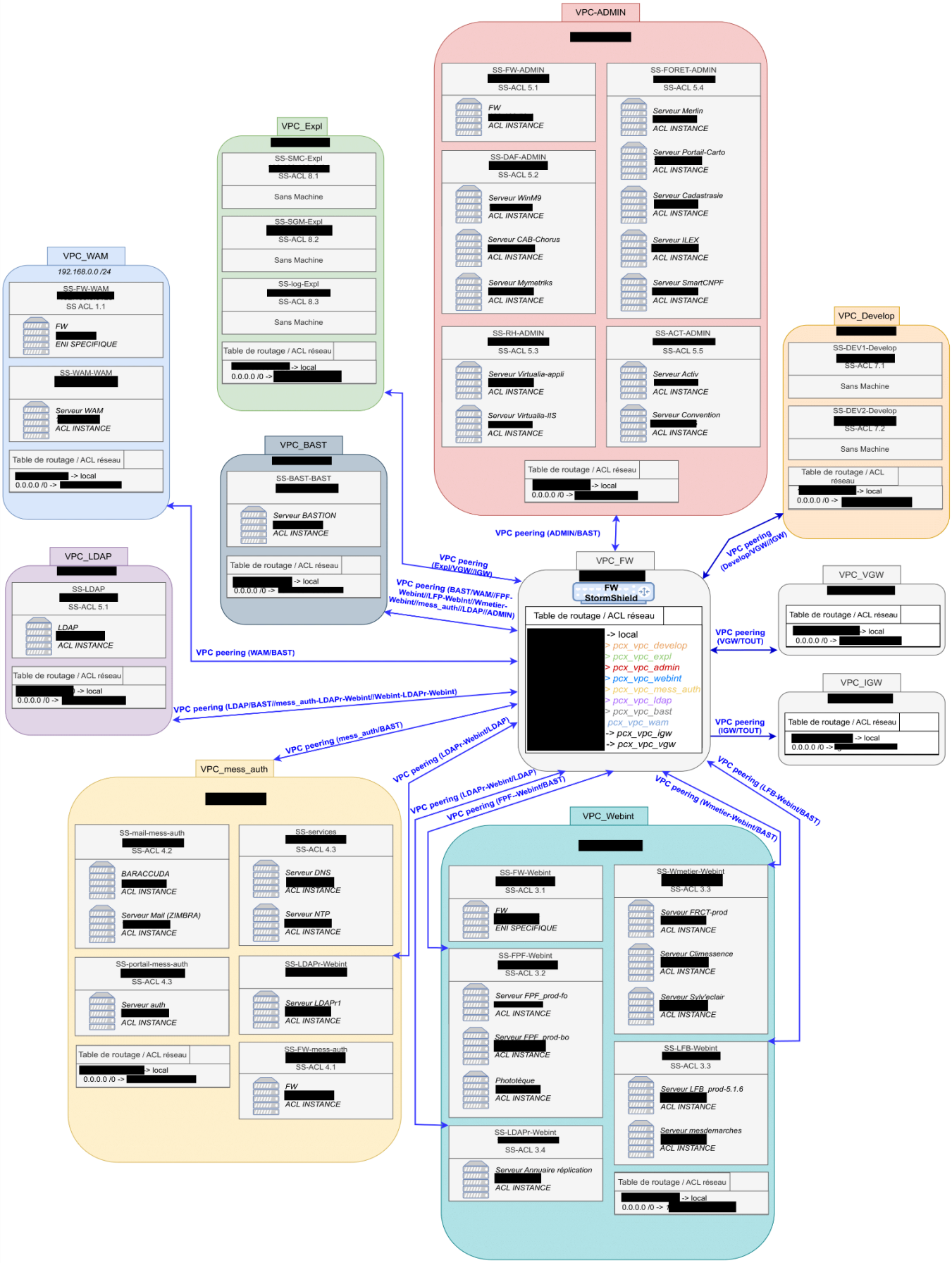
Après avoir examiné les deux premières solutions d'infrastructure, j'ai envisagé une troisième solution qui combine les technologies d'AWS avec un routeur Stormshield offrant un contrôle total sur les flux et un journal complet des flux.

Cette configuration résoudra les problèmes de routage et de sécurité liés aux VPC-peering, ainsi que les limitations de souplesse et les coûts excessifs de la TGW. Le VPC central, doté d'une instance AMI Stormshield, servira de point central pour tous les flux entre les VPC.

En analysant cette solution qui utilise un routeur Stormshield au sein d'un VPC central, j'ai identifié les avantages et les inconvénients suivants :

- Avantages :
    - Une gestion complète des routes et des règles est disponible sur le routeur Stormshield.
    - L'amélioration de la visibilité est assurée grâce aux journaux de flux disponible sur le Stormshield.
    - Les tables d'itinéraires sont faciles à entretenir, facilitant ainsi le routage.
    - Les IGW et VGW sont centralisés en un point, évitant la redondance.

- Inconvénients :
    - Aucune redondance, ce qui pourrait entraîner un blocage du réseau si l'instance Stormshield venait à être coupée.
    - Un cluster est nécessaire en cas de coupure.



Centre National de la Propriété Forestière
CNPF