UCover by Nuabee

Réseaux & PRA

Guide d'architecture technique

v3.2 02/08/2022

TABLE DES MATIÈRES

Figures :

1 - INTRODUCTION

Ce document traite des points d'architecture technique à considérer pour construire et utiliser les réseaux de télécommunication dans le cadre d'un Plan de Reprise d'Activité (PRA) informatique.

Il guide :

- lors de l'avant-vente, pour détecter les points qui méritent une attention particulière,
- lors de la mise en œuvre initiale du PRA,
- lors des opérations quotidiennes.

NB : ceci est la troisième édition de ce guide. Les précédentes éditions ont traité des VPN IPsec et réseaux étendus privatifs, puis de l'usage du VPN SSL. Cette nouvelle édition met en évidence les notions de ***Réseau nominal*** *et* ***Réseau du PRA*** *et met en avant l'intérêt des solutions fondées sur les* ***technologies SDN et SD-WAN****.*

Première partie : Réseau pour le PRA

2 - FONCTIONNEMENT DU PRA DANS LE CLOUD

Comment fonctionne le PRA dans le cloud ? Vous lirez ici un rappel de son principe de fonctionnement largement développé par ailleurs, dans d'autres documents. C'est nécessaire à la compréhension des besoins et des solutions en matière d'architecture de réseau.

Dans l'exemple suivant, nous voulons assurer un PRA pour 3 applications :

- un contrôleur de domaine AD,
- un logiciel ERP,
- un service de fichiers bureautiques.

2.1 - MODE DE FONCTIONNEMENT NOMINAL (HORS MODE SECOURS)

Le fonctionnement nominal est le fonctionnement de la solution au jour le jour, en mode normal.

L'environnement de Reprise d'Activité fonctionne dans le mode nominal pendant très grande majorité du temps.

La base de données de l'ERP et les fichiers de bureautique sont répliqués depuis la salle informatique principale de l'entreprise vers le stockage Cloud. Les 3 serveurs sont aussi répliqués sous forme virtuelle.

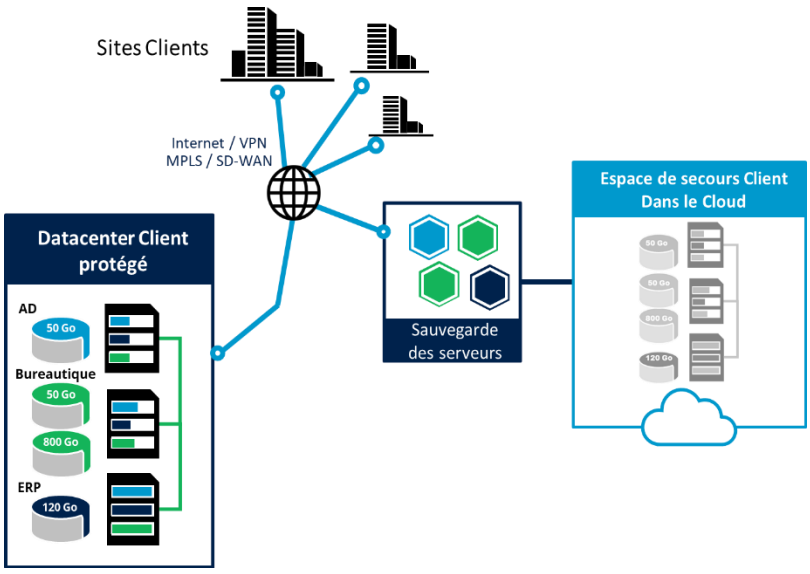

Figure 1 - Mode de fonctionnement nominal

La duplication est incrémentale. Après une première copie complète, seules les modifications sont transférées vers le Cloud, en mode bloc.

2.2 - Mode secours

En cas de sinistre, d'incident critique ou simplement de test, le site informatique principal est déclaré hors service.

Pour la Reprise d'Activité, tout se passe maintenant dans le Cloud. Les données, d'applications et de systèmes, qui avaient été répliquées dans le Cloud pendant la phase de sauvegarde, y sont restaurées sous forme de disques virtuels. Ils sont attachés aux serveurs virtuels (VM) qui sont maintenant réveillés dans le Cloud.

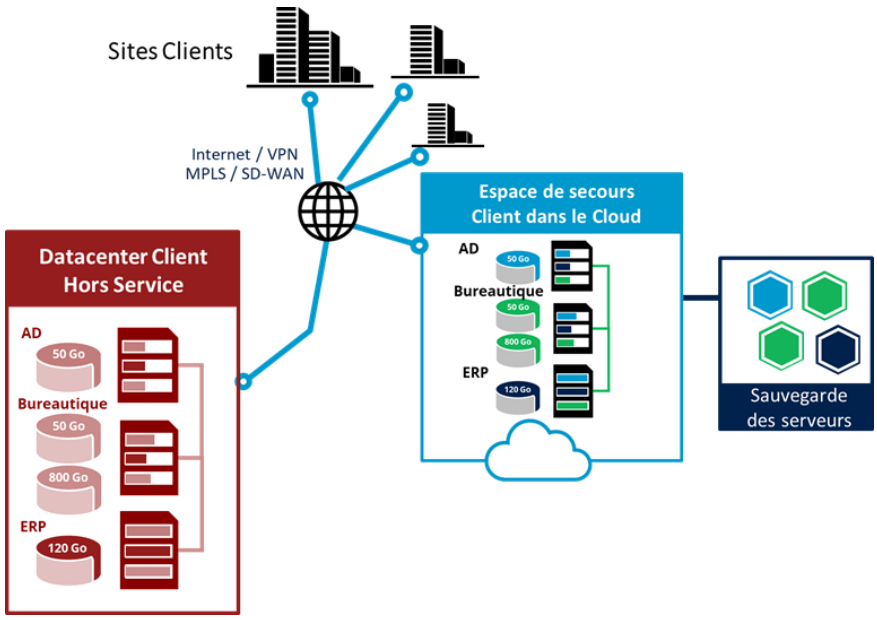

Figure 2 - Mode secours

Les réseaux qui ont été configurés au préalable, pendant la mise en service du PRA, sont activés pour permettre la reconnexion des utilisateurs.

2.3 - Le retour au mode Nominal

L'entreprise a lancé un PRA en réel. Elle a donc fonctionné en mode dégradé pendant un certain temps. Les données ont continué à être sauvegardées dans le Cloud durant le temps d'indisponibilité de son SI.

Dès que le SI principal redevient fonctionnel, l'entreprise souhaite reprendre les activités normales sur son site principal, qu'il soit *on-premise* ou dans le Cloud. Un retour arrière doit être organisé avec les données présentes dans le Cloud. Ceci peut nécessiter l'usage de dispositifs de transport des données depuis le Cloud vers le site principal.

3 - ÉLÉMENTS D'ARCHITECTURE DE RÉSEAU

3.1 - QUELS BESOINS D'ARCHITECTURE RÉSEAU POUR LE PRA ?

Le service de PRA offre la possibilité de faire fonctionner une réplique de l'infrastructure nominale dans le cloud.

En cas de sinistre grave qui détruit complètement l'infrastructure nominale, la réplique remplace dans le cloud l'infrastructure détruite. À un instant donné, avant le sinistre, puis après le sinistre, il n'existe qu'un seul exemplaire de l'infrastructure. Cela rend le principe de fonctionnement du réseau trivial du point de vue du fonctionnement des mécanismes TCP/IP.

En revanche l'existence simultanée de deux infrastructures de réseau complique les choses. Le réseau peu alors présenter des segments dont les adresses IP sont identiques. Les mécanismes de TCP/IP interdisent alors certains cas d'interconnexion.

Considérons quelques cas d'usage.

- Pendant les tests de PRA, comment faire fonctionner le réseau simultanément en mode nominal et en mode secours ? Comment connecter quels utilisateurs « testeurs » sur l'espace de secours dans le cloud pendant que l'essentiel des utilisateurs travaille sur le datacenter protégé, dans l'entreprise ?
- Si un sinistre ne détruit pas physiquement les infrastructures (une cyber-attaque par exemple), comment connecter les utilisateurs sur l'espace de secours dans le cloud ?
- Si un sinistre ne met hors service que quelques serveurs, comment assurer un fonctionnement mixte de l'infrastructure entre le datacenter protégé, dans l'entreprise, et l'espace de secours, dans le cloud (PRA partiel) ?

Comment répondre aux questions techniques qui de posent ? Qu'est-il possible de réaliser ?

3.2 - RAPPELS SUR QUELQUES NOTIONS

Il est important de rappeler quelques principes de fonctionnement de TCP/IP pour justifier les positions développées et prises dans ce document à propos de la gestion des réseaux dans un PRA.

Ce qui est énoncé suppose un adressage et un fonctionnement conforme à IPv4. L'utilisation d'IPv6 amènerait à des considérations et des conclusions différentes.

3.2.1 - Réseau et Sous-réseaux IP

Un **Réseau IP** est composé de plusieurs **Sous-réseaux IP**.

Un **Sous-réseau IP** est fondé sur l'utilisation d'un **médium de transmission qui assure la connexion physique de multiples stations**. Chaque station peut communiquer avec toutes ses voisines directement par l'intermédiaire du médium, sans invoquer la fonction de routage qui intervient dans l'interconnexion des sous-réseaux. Le médium doit offrir une faculté de

multidiffusion ; il s'agit typiquement d'un **réseau local**. Le médium peut être scindé en plusieurs parties reliées par des **ponts entre réseaux locaux**.

Un **Sous-réseau IP** est caractérisé par **une plage d'adresse** dont l'adresse de début est un multiple d'une puissance de 2 et dont le nombre d'adresses est la même puissance de 2.

Un **Réseau IP** doit être **composé de Sous-réseaux IP** dont **les plages d'adresses sont différentes et qui ne se recouvrent pas**.

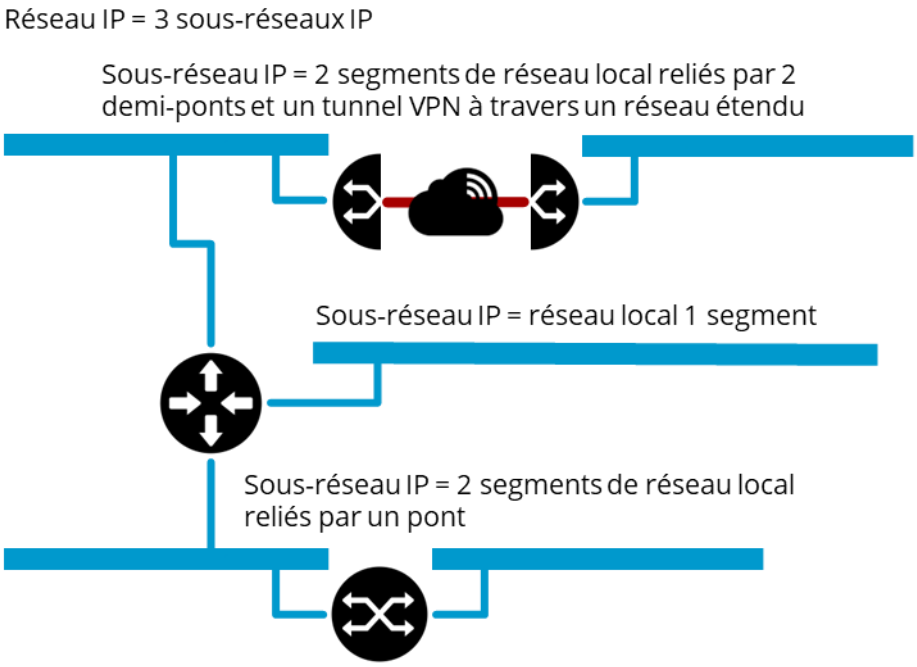

Figure 3 – Réseau et Sous-réseaux IP

3.2.2 - Coexistence de réseaux privés

L'ensemble du Web est constitué

- d'une épine dorsale, Internet,
- et de de réseaux privés d'entreprises.

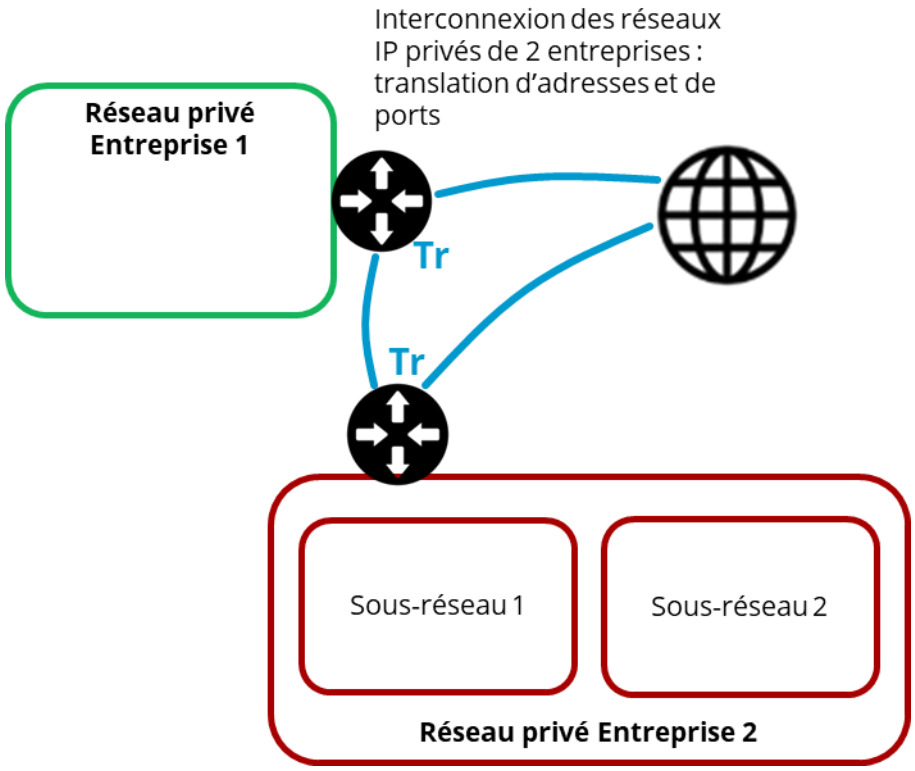

Figure 4 – Interconnexion de réseaux privés IP

Chaque entreprise construit son propre réseau privé. Il s'agit d'un Réseau IP, tel qu'il est exposé au chapitre précédent.

Les règles de construction des réseaux IP privés font que chaque entreprise doit adopter un plan d'adressage qui se confond avec celui de nombre de ses voisines. L'application des règles explosées au chapitre précédent implique que **les réseaux privés d'entreprise ne peuvent communiquer entre eux**. Si des réseaux privés d'entreprises doivent **communiquer en eux et avec Internet, c'est par l'intermédiaire d'artifices de translation d'adresses et de règles de routage spécifiques** installées dans des équipements tels que routeurs et firewalls à des points de passage frontières entre ces réseaux.

3.2.3 - Unifier des sous-réseaux à travers un réseau tiers

Une entreprise peut être installée sur plusieurs sites. Le Réseau IP privé couvre l'ensemble des sites. Chaque site compte un ou plusieurs sous-réseau IP.

Sur chaque site un routeur interconnecte les Sous-réseaux entre eux. Ces routeurs sont interconnectés par un « câble virtuel », un **tunnel VPN** (Virtual Private Network. Ce tunnel VPN est porté par une infrastructure de réseau tiers, Internet ou offre d'opérateur.

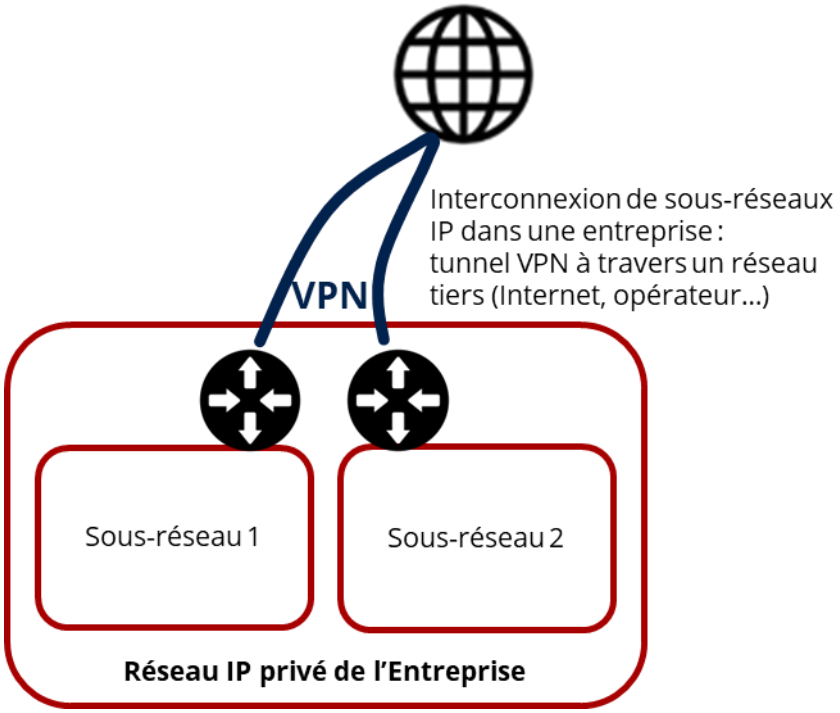

Figure 5 – Interconnexion de sous-réseaux IP privés à travers un VPN

3.3 - Application au PRA

Ces rappels à propos de la technologie des réseaux sont capitaux dans le fonctionnement de la solution du PRA.

Le fonctionnement du PRA est fondé sur une réplication d'infrastructure. **Les adresses des stations sont les mêmes pendant le fonctionnement nominal de l'infrastructure et pendant celui du PRA**, qu'il soit en test ou en réel.

Le constat est le suivant : **l'infrastructure de réseau** de l'entreprise **doit être scindée en 2 Réseaux IP**, faute de quoi son fonctionnement est impossible :

- le **Réseau** (IP) **nominal**,
- le **Réseau** (IP) **du PRA**.

3.3.1 - Réseau nominal

Ensemble des sous-réseaux qui constitue le **Réseau IP privé pour son fonctionnement nominal**, en exploitation normale. Son plan d'adressage est privé et/ou public.

Ce Réseau IP dispose d'une ou plusieurs évasions Internet.

Il est constitué de

- segments de réseaux locaux,
- d'un réseau étendu fondé sur des technologies variées : Internet + routeurs privés, MPLS, SDWAN.

3.3.2 - Réseau du PRA

Ensemble des sous-réseaux qui constitue le **Réseau IP privé pour son fonctionnement en mode secours**.

Il recouvre géographiquement le réseau nominal sauf à propos de l'implantation des serveurs : ceux-ci sont installés dans le cloud.

Il peut fonctionner simultanément avec le réseau nominal. C'est le cas des tests de PRA.

Il a **le même plan d'adressage que le réseau nominal**. C'est une obligation pour les équipements qui ont des adresses IP statiques : serveurs, imprimantes, équipements annexes. C'est facultatif pour les équipements qui disposent d'une adresse IP dynamique fournie par un service DHCP : postes de travail.

Le Réseau nominal et le Réseau du PRA ayant **des plans d'adressage qui se chevauchent**, ils doivent être **étanches l'un par rapport à l'autre** sous peine d'empêcher les mécanismes TCP/IP de fonctionner.

À partir de maintenant, les notions de **Réseau nominal** et de **Réseau du PRA** sont fondamentales. Elles sont définies et ne peuvent être ignorées pour évoquer les problématiques d'architecture de réseau pour le PRA.

3.4 - ARCHITECTURES TECHNIQUES ET OUTILLAGES

Les architectures techniques et outillages utilisés jusqu'à présent dans la mise en œuvre du PRA d'une entreprise ne référencent pas les notions de Réseau nominal et de Réseau du PRA. Réparons ici cette absence qui n'empêchait pas les approches les plus simples.

3.4.1 - NCA

Nuabee propose à ses clients une solution de connexion entre le(s) site(s) de repli des utilisateurs (des bureaux loués hors de l'entreprise si ses locaux sont détruits par un sinistre) et les serveurs redémarrés dans le cloud lors de l'activation d'un PRA. Cette équipement appelée **Nuabee Cloud Access** (**NCA**) permet également de procéder aux tests réguliers de PRA en permettant au Client de tester à distance la fourniture du service de PRA.

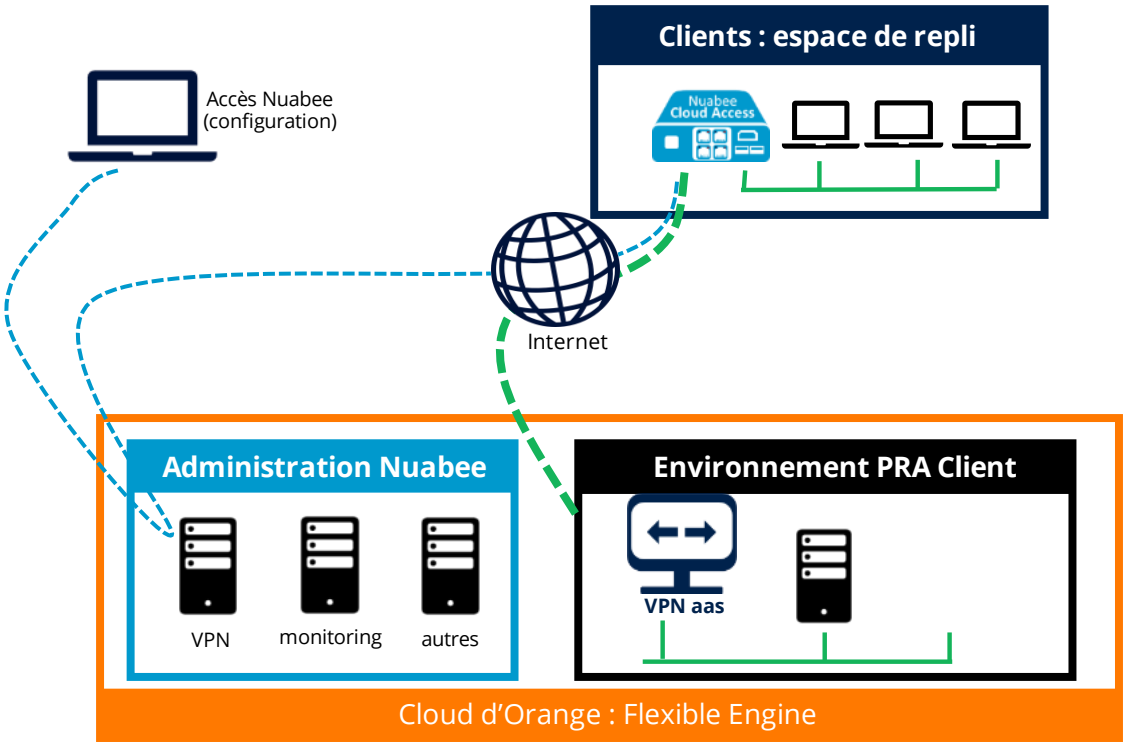

Figure 6 – Fonctions d'un équipement Nuabee Cloud Access (NCA)

Cette solution est fondée sur ordinateur de petit format qui embarque la distribution de sécurité **OPNsense**. Il s'agit d'un routeur/pare-feu Open Source sur le système d'exploitation **FreeBSD**.

Figure 7 - Boîtier routeur NCA

Le réseau privé virtuel (VPN) prend la forme d'un **tunnel** logique établi en protocole **IPsec**.

L'équipement NCA fournit un ensemble de services de base DHCP et DNS « *forwarder only* » qui peuvent être étendus en fonction du besoin.

L'appliance NCA est configurée automatiquement à distance en se connectant à un service de télé-configuration fourni par Nuabee.

La documentation est disponible sur le Wiki de Nuabee : Nuabee Cloud Access (NCA).

D'une façon générale, l'utilisation de la NCA permet de construire des architectures de réseau qui sont conformes aux notions de Réseau nominal et de Réseau du PRA.

Usages :

Le NCA permet d'ajouter un réseau local (un Sous réseau IP) au Réseau du PRA.

Mise en œuvre :

- Dans le Réseau nominal, le réseau local en question est constitué par ses propres équipements en fonctionnement normal.
- Dans le Réseau du PRA, initialement constitué du seul cloud, le réseau local est déconnecté du Réseau nominal et est reconnecté dans le Réseau du PRA. Le NCA permet de remplacer les fonctions de routage du Réseau nominal par celles du Réseau du PRA.

3.4.2 - Réseau privatif loué à un opérateur

Un tel réseau est proposé par Orange sous la dénomination Business VPN.

Une telle offre de service est conçue pour constituer un Réseau IP privé pour une entreprise. De ce fait, il est très réfractaire à la connexion simultanée de 2 sous-réseaux dont les plages d'adresses sont identiques. Il n'est donc pas conçu pour prendre en charge simultanément le Réseau nominal et le Réseau du PRA, comme cela est nécessaire pour effectuer un test de PRA. (Rappelons que le traitement du PRA réel est trivial à propos de l'adressage IP : le Réseau du PRA se substitue au Réseau nominal, pour les parties du réseau qui ne sont pas touchées par le sinistre, et remplace les parties du Réseau nominal qui sont devenue hors service).

Les chapitres suivants exposent comment le Réseau nominal et le Réseau du PRA peuvent être construits et comment ils fonctionnent dans les différents cas de figure.

4 - PRA SUR UN ACCÈS INTERNET SIMPLE

4.1 - FONCTIONNEMENT NOMINAL

L'entreprise est implantée sur un site unique.

Ce site dispose d'un réseau local qui interconnecte

- les serveurs,
- les postes de travail,
- les imprimantes…
- les équipements de réseau, notamment le routeur (la *box*) d'accès à Internet,

Le site principal compte un seul sous-réseau qui regroupe serveurs et postes de travail.

Le **Réseau nominal** est donc constitué de ce seul sous-réseau IP.

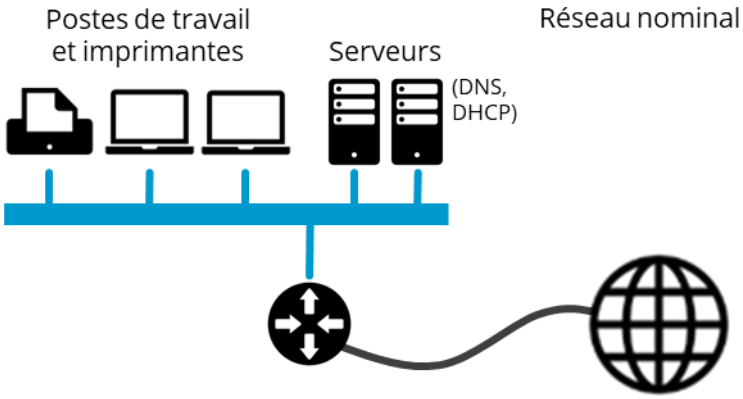

Figure 8 – Accès Internet simple. Réseau nominal.

4.2 - ACTIVATION DU PRA RÉEL

<u>Réseau nominal, sur le site de l'entreprise :</u>

Le **Réseau nominal disparait**, du fait du sinistre.

Le **Réseau du PRA se substitue** complètement au **Réseau nominal**.

Réseau du PRA, dans le cloud :

Il regroupe les serveurs restaurés et redémarrés dans le cloud. Ceux-ci **gardent l'adressage qu'ils avaient sur le Réseau nominal**.

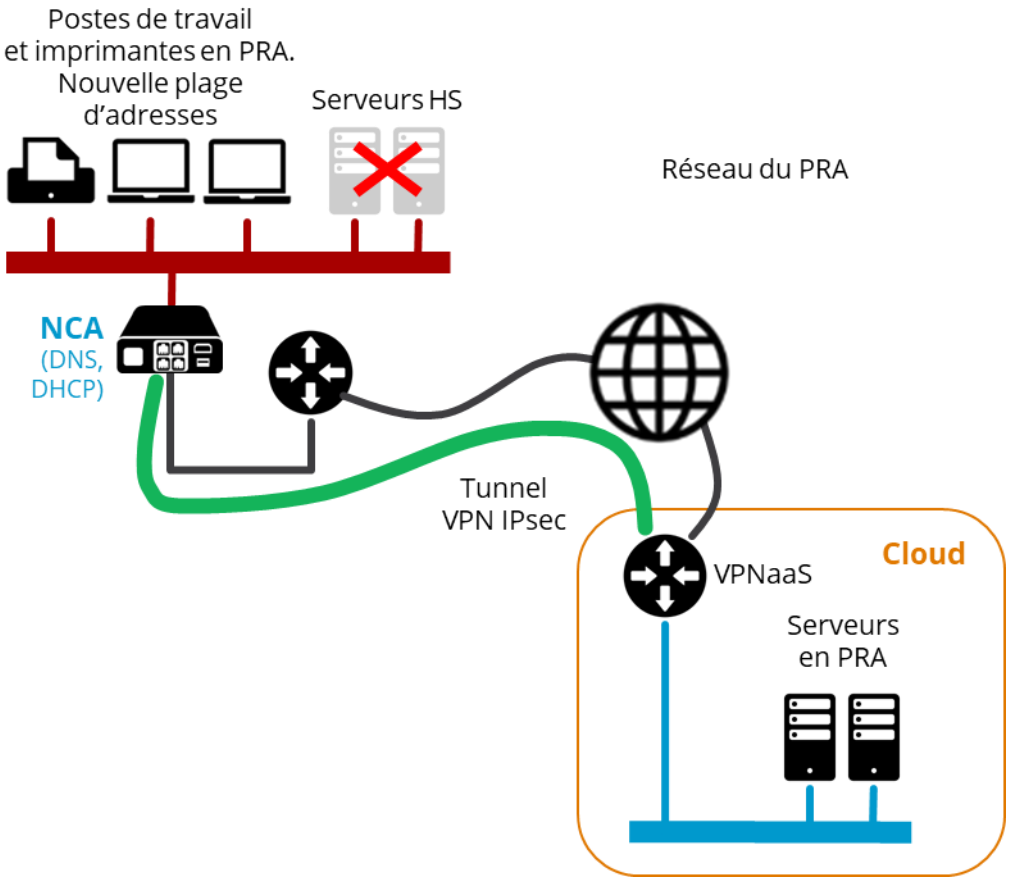

Figure 9 - Accès Internet simple. PRA réel activé en cas de sinistre.

Le **service VPN IPsec** (*VPN as a Service*, **VPNaaS**) du cloud Flexible Engine est utilisé. Il répond à la demande d'établissement du tunnel IPsec de l'équipement NCA installé pour l'accès des postes de travail et imprimantes. Ce service est associé au *tenant* dédié au PRA du client. Il est instancié et activé lors de l'activation du PRA.

Réseau du PRA, sur le site de l'entreprise, ou déporté en position de repli :

Il **remplace le Réseau nominal**. Il est localisé sur site, ou hors site dans une position de repli, en fonction des dégâts subis dans les locaux. Il regroupe les postes de travail et imprimantes.

Les serveurs originaux, sur site, sont mis hors service du fait du sinistre.

Le réseau local des équipements des utilisateurs **doit changer de plage d'adresses**.

Le réseau local doit disposer de ses propres fonctions de routage pour être connecté au **Réseau du PRA**. Les postes de travail (ordinateurs, imprimantes, autres équipements connectés au réseau…) doivent recevoir un nouveau paramétrage ; cette opération est triviale si le mécanisme DHCP est utilisé ; elle fait l'objet d'actions manuelles pour tous les équipements qui ne bénéficient pas de DHCP.

4.3 - TEST DE PRA

Le Réseau nominal et le Réseau du PRA fonctionnent simultanément. Pour cela, ils **doivent être séparés**.

Réseau nominal, sur le site de l'entreprise :

Il reste **sans modification**.

Réseau du PRA, dans le cloud :

Il regroupe les serveurs restaurés et redémarrés dans le cloud. Ils **gardent l'adressage qu'ils avaient sur le Réseau nominal**.

Le **service VPN IPsec** (*VPN as a Service*, **VPNaaS**) du cloud Flexible Engine est utilisé. Il répond à la demande d'établissement du tunnel IPsec de l'équipement NCA installé pour l'accès des postes de travail et imprimantes en test. Ce service est associé au *tenant* dédié au PRA du client. Il est instancié et activé lors de l'activation du PRA.

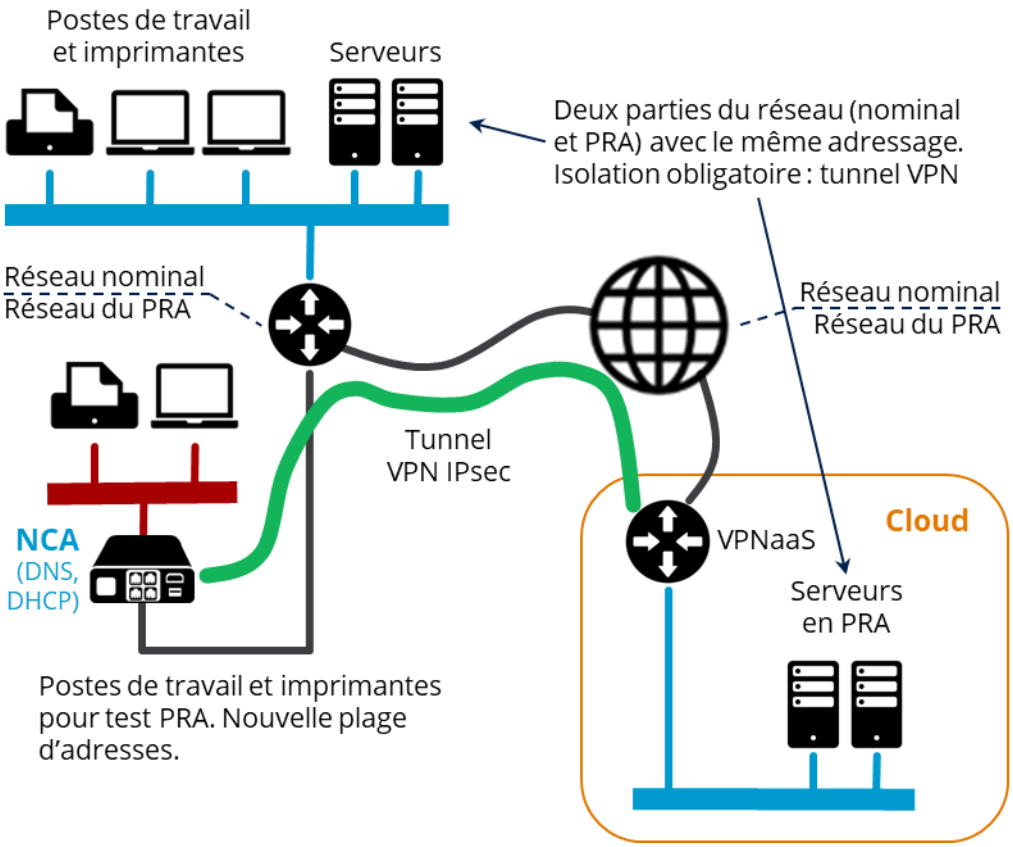

Figure 10 - Accès Internet simple. PRA activé en test.

Réseau du PRA, sur le site de l'entreprise :

Il est constitué d'**un réseau local qui compte quelques postes de travail et imprimantes** qui doit être installé **séparément du Réseau nominal**. Un commutateur séparé ou un réseau local virtuel peut être utilisé pour ce faire.

L'équipement NCA est utilisé et connecté :

- d'une part au réseau local, vers les équipements des utilisateurs,
- d'autre part à Internet.

L'équipement NCA ne peut pas être connecté à Internet en utilisant le réseau local du Réseau nominal. Il y aurait alors confusion du Réseau nominal et du Réseau du PRA. Il doit **disposer de son propre accès Internet** ou **utiliser une zone démilitarisée**.

5 - PRA SUR UN RÉSEAU ÉTENDU PRIVATIF

5.1 - QU'EST-CE QU'EN RÉSEAU ÉTENDU PRIVATIF ?

Un **réseau étendu privatif** permet à une entreprise de construire son infrastructure de télécommunications entre plusieurs sites (sièges, unités de production, agences…). Cette infrastructure est fondée sur l'utilisation de produits et services fournis par un ou des opérateurs de télécommunication ainsi que des équipementiers.

Plusieurs équipementiers et opérateurs de télécommunication utilisent le terme anglo-saxon de *Virtual Private Network* (**VPN**).

Les technologies utilisées sont :

- Multi-Protocol Layer Switching (**MPLS**),
- Software Defined Wide Area Networking (**SD-WAN**).

Les produits commerciaux des opérateurs sont :

- Orange Business Services : Business VPN,
- SFR : SD-NET,
- Bouygues Télécom : VPN / MPLS…

Les produits commerciaux des équipementiers sont :

- VMware : VeloCloud,
- Cisco : Meraki,
- Fortinet : Fortigate…

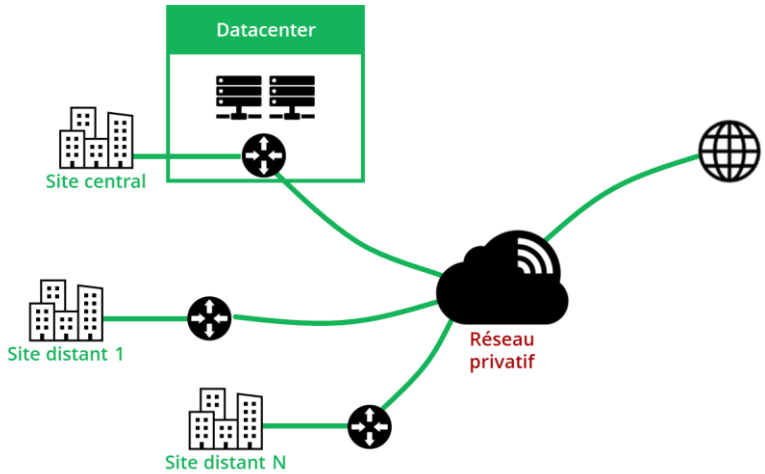

Figure 11 - L'entreprise multisite utilise un réseau étendu privatif

5.2 - CONNEXION PRIVATIVE AVEC LE CLOUD

5.2.1 - Connexion au cloud

Le cloud Orange Flexible Engine est accessible par une **connexion cloud privative** depuis un réseau étendu privatif.

La solution est fondée sur une **connexion directe du réseau privatif de l'entreprise vers le cloud Orange Flexible Engine**.

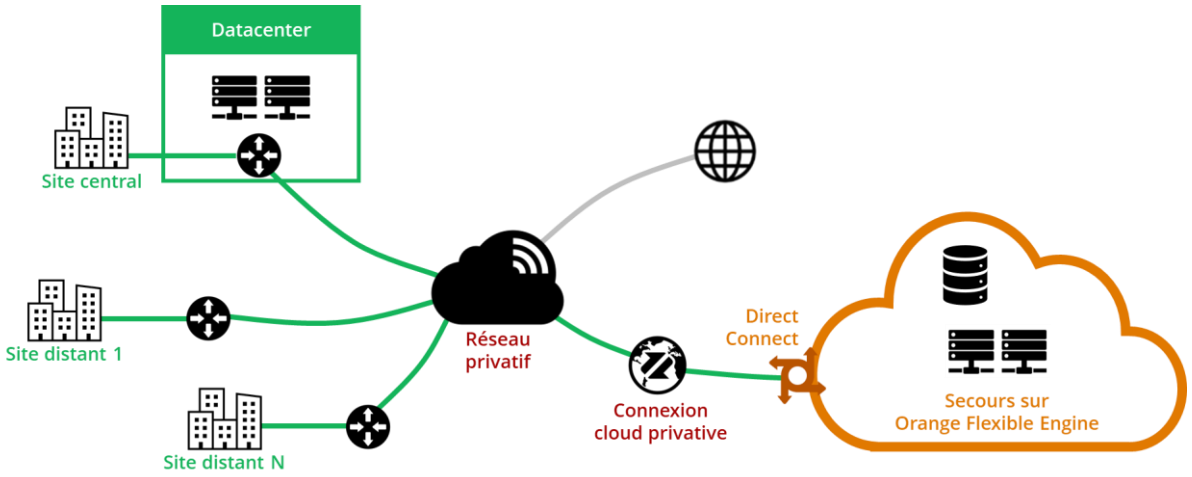

Figure 12 - Connexion privative avec le Cloud

Ce type de connexion est proposé par la plupart des opérateurs de réseaux étendus privatifs et de clouds publics. Ce type de connexion permet, par sa construction fondamentalement isolée des autres réseaux, la **sécurisation du transfert des données entre l'entreprise et le cloud**.

Cas Orange Business VPN Galerie :

La solution d'Orange est fondée sur :

- un réseau privatif **Business VPN**,
- une connexion cloud privative **Business VPN Galerie**,
- et le service **Direct Connect** de Flexible Engine, sur le cloud Flexible Engine.

Cette solution est présentée de façon intégrée par Orange à ses clients. Elle masque la complexité de la solution technique décrite plus haut.

Elle offre également la **haute disponibilité** via une **redondance des liens entre les zones de disponibilité** (*Availability Zones*, AZ) du cloud Flexible Engine.

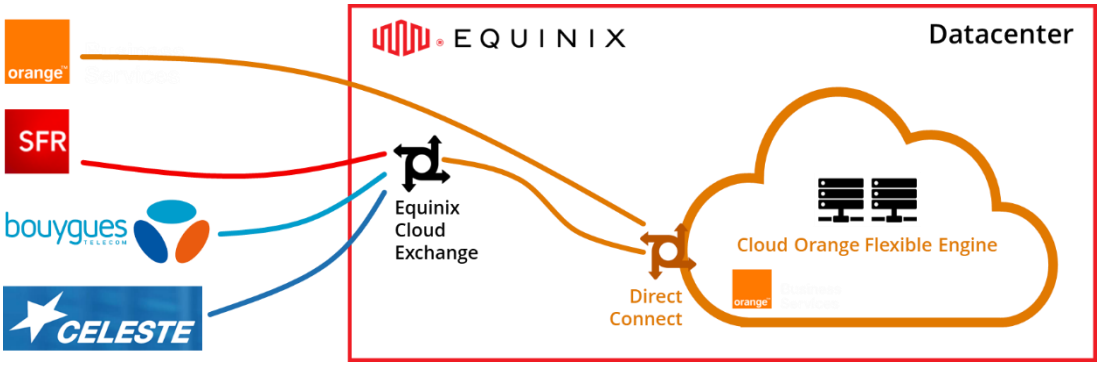

Figure 13 - Connexion au cloud directe (Orange) ou via Equinix Cloud Exchange

<u>Cas général : le mécanisme est disponible pour tous les opérateurs de réseau privatif :</u>

La solution d'interconnexion dépend de l'opérateur du réseau privatif (SFR, Bouygues Telecom, Céleste…). Celui-ci doit **construire une connexion physique qui aboutit dans le datacenter** qui héberge le cloud Flexible Engine.

Puis intervient l'opérateur qui exploite les locaux qui hébergent le cloud Flexible Engine : **Equinix**. Cet opérateur de datacenter accueille des arrivées de réseau en provenance de tous les opérateurs de télécommunication. Cette intervention de l'opérateur de datacenter est matérialisée par un service, **Equinix Cloud Exchange**, qui unifie les connexions des différents opérateurs de télécommunication.

5.2.2 - Conditions de la mise en œuvre

La connexion privative directe est nécessaire dès lors que le PRA est activé, en test ou en réel. Sa **mise en œuvre est soumise à des délais d'installation de plusieurs semaines** de la part du ou des opérateurs qui interviennent. À cause de ce délai, la connexion directe **doit donc être installée dès la mise en service du PRA**.

L'entreprise bénéficiaire du PRA doit supporter le coût récurrent de la mise à disposition de la connexion directe, même en l'absence de sinistre ou de test de PRA. Dans le cas d'une solution de connexion Orange de bout en bout, **le coût peut être optimisé** :

- dans le cas général, **hors d'une situation de crise**, une bande passante de **5 Mbit/s** est configurée, pour un coût d'environ 75 € HT par mois ;
- **en situation de crise**, lorsque le **PRA est activé en réel**, la connexion au cloud est configurée avec la **bande passante nécessaire pour acheminer tout le trafic** dû aux utilisateurs, dans une plage de 5 à 500 Mbit/s, pour un coût exceptionnellement élevé.

5.2.3 - Routage sur le réseau privatif

<u>Exclusivité entre fonctionnements nominal et PRA :</u>

L'espace de secours activé dans le cloud pour le PRA a strictement le même plan d'adressage privé que celui du datacenter d'origine en fonctionnement nominal. Un serveur dans le

datacenter de l'entreprise, et sa réplique redémarré dans le cloud en cas de PRA, ont la même adresse IP.

Par conséquent, **un serveur et sa réplique ne peuvent pas être démarrés et adressés simultanément sur le réseau**.

Même si cela est une contrainte technique, cette caractéristique est le fondement de la transparence du redémarrage des serveurs vis-à-vis des utilisateurs.

Cette situation d'exclusivité de fonctionnement est évidente en cas de sinistre puisque les serveurs en fonctionnement nominal sont hors service. Elle n'existe pas en cas de test de PRA.

BGP :

Le routage sur le réseau étendu privatif et sur la connexion coud privative est régi par l'utilisation du protocole **BGP** (*Border Gateway Protocol*).

Ce mécanisme de routage automatique **est conçu pour calculer une route alternative** entre 2 ordinateurs si les liens d'une connexion principale sont en défaut.

Ce mécanisme **n'est pas conçu pour trouver une route vers un ordinateur alternatif** si l'ordinateur principal est en défaut. C'est pourtant un mécanisme utilisé pour permettre des routes différenciées par région géographique vers de multiples serveurs Web. C'est le mécanisme qui nous intéresse dans le cadre d'un PRA.

Pour ce faire, l'utilisation de BGP nécessite **d'apporter une attention particulière à l'utilisation des mécanismes de routage automatique**.

Routage BGP sur le réseau privatif :

Quelques mots pour décrire le principe de fonctionnement de BGP. Cette explication est fonctionnelle. **Le point de vue est celui d'un utilisateur du réseau** privatif et de sa connexion au cloud. Il n'est pas important, et il n'est pas question d'expliquer ici les mécanismes internes au réseau fourni par l'opérateur.

Des équipements, physiques ou virtuels, sont placés à la frontière entre le réseau privatif et ses utilisateurs :

- routeurs d'accès des sites de l'entreprise sur le réseau privatif (**Customer Edge**, **CE**),
- service **Direct Connect** de Flexible Engine.

Ces équipements connaissent les plages d'adresses IP des réseaux locaux ou de cloud qu'ils connectent sur le réseau privatif.

Ces équipements annoncent, par le protocole BGP, ces plages d'adresses IP à l'infrastructure de réseau privatif. **Le réseau privatif calcule alors les routes** qu'il doit mettre en œuvre pour acheminer le trafic.

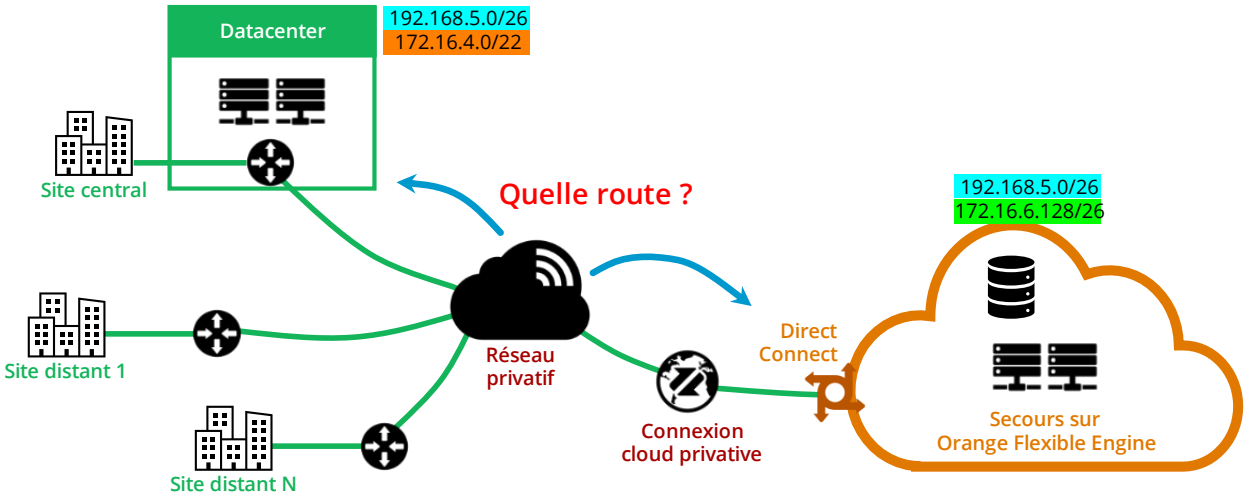

Figure 14 – Routage calculé avec annonces BGP

Que se passe-t-il si **2 équipements de frontière annoncent des plages d'adresse qui se chevauchent** ?

Cas 1 : les plages d'adresses sont exactement les mêmes

Les plages ont **même adresse** et **même masque**. Dans notre exemple : 192.168.5.0/26.

Le comportement du réseau Business VPN est **inconnu**. C'est insatisfaisant et il faut éviter ce cas.

Cas 2 : une plage d'adresse est un sous-ensemble de l'autre :

L'adresse de la plage la plus fine est incluse dans la plus grande. Le masque de la plage la plus fine est plus long que celui de la plus grande. Dans notre exemple :

- plage la plus grande : 172.16.4/22,
- plage la plus fine : 172.16.6.128/26.

Une équivoque existe pour le **routage de la plage la plus fine** : les datagrammes IP sont-ils routés vers l'équipement frontière qui annonce la plage la plus grande, ou celui qui annonce la plus fine ?

Réponse : les datagrammes IP sont routés **vers l'équipement qui annonce la plage la plus fine**.

Pour **le reste de la plage la plus grande**, les datagrammes sont routés **vers l'équipement frontière qui annonce la plus grande**.

Déclaration manuelle des plages d'adresses dans le cloud et calcul automatique des routes :

Pour assurer le fonctionnement correct du réseau, **l'exploitation du PRA fait l'objet de procédures gérées par Nuabee**.

En fonctionnement **nominal** (absence de sinistre ou de test), **Nuabee supprime** le paramétrage des plages d'adresses de serveurs **dans le service Direct Connect**. Ces plages ne sont donc pas annoncées par BGP en ce point. **Le datacenter de l'entreprise est la destination** obligatoire de toutes les routes vers les serveurs.

En cas **d'activation du PRA**, en réel, **Nuabee paramètre les plages d'adresses de serveurs dans le service Direct Connect**. **Chaque serveur secouru fait l'objet de sa propre plage** (masque **/32**). BGP annonce donc autant de plages qu'il existe de serveurs. **Le cloud devient la destination obligatoire vers tous les serveurs secourus**.

Cette méthode permettrait de proposer un **PRA partiel** : ne secourir que quelques serveurs qui seraient sinistrés (**cet exposé n'explique pas comment les serveurs situés dans le datacenter de l'entreprise et ceux situés dans le cloud communiquent ; c'est un problème qui doit obligatoirement être traité par ailleurs**).

Test du PRA :

Pendant le test du PRA, **les serveurs redémarrés dans le cloud** fonctionnent en même temps que ceux, en exploitation nominale, dans le datacenter de l'entreprise. **Il n'est pas question de les rendre visibles sur le cloud** par l'intermédiaire du service Direct Connect. Cela interromprait l'exploitation.

Compte tenu des mécanismes décrits plus haut, **le test du PRA doit être décomposé**.

La vérification du fonctionnement des applications doit être réalisée **par la reconnexion de quelques postes de travail, sur un réseau local isolé**, vers les serveurs en PRA dans le cloud. Pour ce faire, la solution consiste dans un VPN IPsec établi avec un NCA. Voir le chapitre 5.5 - TEST DE PRA SUR LE RÉSEAU PRIVATIF.

La vérification du fonctionnement de la connexion directe sur le cloud est réalisée en ne montrant qu'un **serveur de test de VPN Galerie** redémarré dans le cloud en utilisant une **plage d'adresses IP dédiée à cet usage**.

5.2.4 - Routage dans le cloud

Les flux sont transportés par la connexion cloud privative jusqu'au dispositif Direct Connect dans le cloud Orange Flexible Engine. **Comment ces flux sont-ils routés dans le cloud** vers les ressources qui sont nécessaires

- aux sauvegardes,
- et au PRA s'il est activé ?

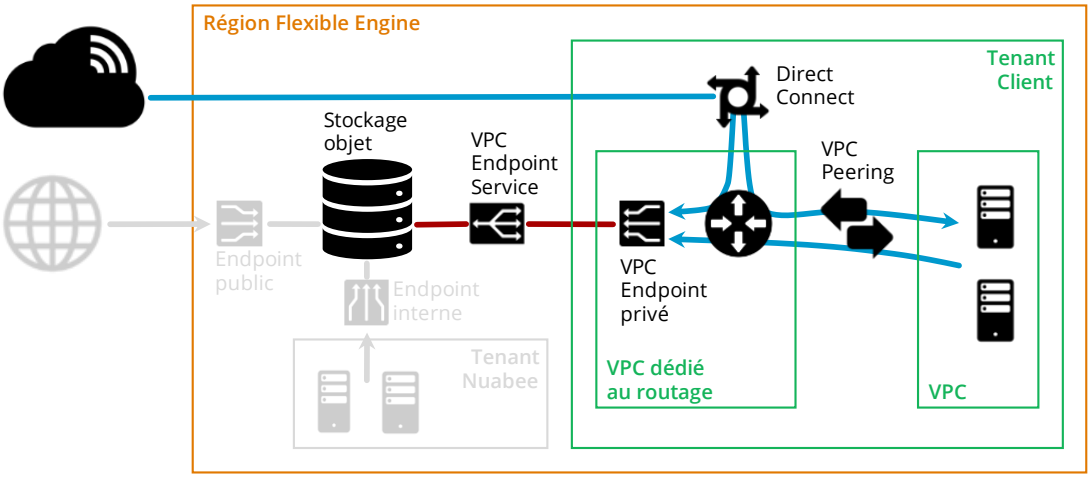

Figure 15 - Routage dans le tenant *client*

Organisation des ressources du cloud :

Toutes les ressources sont situées dans une **région unique** du cloud.

Les ressources sont imputées sur un ***Tenant*** (littéralement : locataire) dédié au PRA et aux opérations de routage des flux. Nuabee en réserve **un pour chacun de ses clients**.

Ressources cibles :

Elles font l'objet de la mise en œuvre des solutions pour y accéder.

Il s'agit :

- du **stockage objet**, nécessaire aux sauvegardes
- des **VPC** (**Virtual Private Cloud**, réseau virtuel dans le cloud) dédié et serveurs virtuels nécessaires au PRA.

Ressources auxiliaires :

Elles participent à la mise en œuvre des solutions d'accès aux ressources cibles.

Il s'agit :

- de **Direct Connect**,
- du **VPC dédié au routage**,
- du **VPC Peering**, entre les VPC du *tenant* client,
- des **VPC Endpoint privé** et **VPC Endpoint Service** entre les *tenants* client et Nuabee.

Routage IP :

La fonction permet les échanges de données

- réseau privatif client / stockage objet, pour les sauvegardes, en fonctionnement nominal,
- réseau privatif client / VPC dédié au PRA, pour l'accès des utilisateurs sur les serveurs, en cas d'activation du PRA,
- VPC dédié au PRA / stockage objet, pour les sauvegardes des serveurs, en cas d'activation du PRA.

La fonction est implantée dans **un VPC dédié du *tenant* client**.

Les tables de routage sont établies par plusieurs mécanismes :

- définies statiquement, par un paramétrage manuel ;
- définies indirectement, par le paramétrage d'autres objets dans le cloud ;
- acquises automatiquement par le fonctionnement d'un protocoles tel que BGP (Border Gateway Protocol).

Liaison entre VPC dédié au routage et VPC dédié au PRA :

Il s'agit d'une liaison logique, similaire à un câble, établie entre deux réseaux.

La liaison est fondée sur l'utilisation d'un **VPC Peering entre les deux VPC** qui se situent dans le même ***tenant* client**.

Le paramétrage de ce VPN Peering porte mutuellement à chacun des VPC la connaissance des sous-réseaux IP que l'autre peut atteindre. **Ceci permet à chacun des VPC d'établir ses tables de routage**.

Accès au stockage objet :

Moins que construire une liaison logique avec le stockage objet, **il s'agit de le rendre accessible au *tenant* Client**. On pourrait dire : le montrer ou le publier.

Le rôle du couple d'objets **VPC Endpoint Service / VPC Endpoint** est de **faire apparaitre virtuellement le stockage objet dans le VPC** dédié au routage, pratiquement comme s'il s'agissait d'une machine virtuelle.

Le stockage objet est vu, dans le cas présent, avec **son adresse IP et son nom dans un domaine public Internet**. Il pourrait l'être aussi une adresse IP et un nom dans le domaine privé du client.

La présence du VPC Endpoint induit trivialement la **route vers le stockage objet dans la table de routage du VPC** dédié au routage.

Remarque :

Dans de nombreux cas, l'implantation de la solution décrite ici est simplifiée : dans le *tenant* du client, le VPC dédié au routage et celui dédié au PRA sont regroupés en un seul, sans que cela change le principe et la sécurité de fonctionnement de la solution.

5.3 - FONCTIONNEMENT NOMINAL SUR LE RÉSEAU PRIVATIF

L'entreprise est implantée sur plusieurs sites.

Chaque site dispose d'un réseau local qui interconnecte

- les serveurs, sur le site principal,
- les postes de travail,
- les imprimantes,
- les équipements de réseau, notamment le routeur d'accès au réseau étendu privatif,

Chaque site est connecté sur le réseau étendu privatif par un routeur.

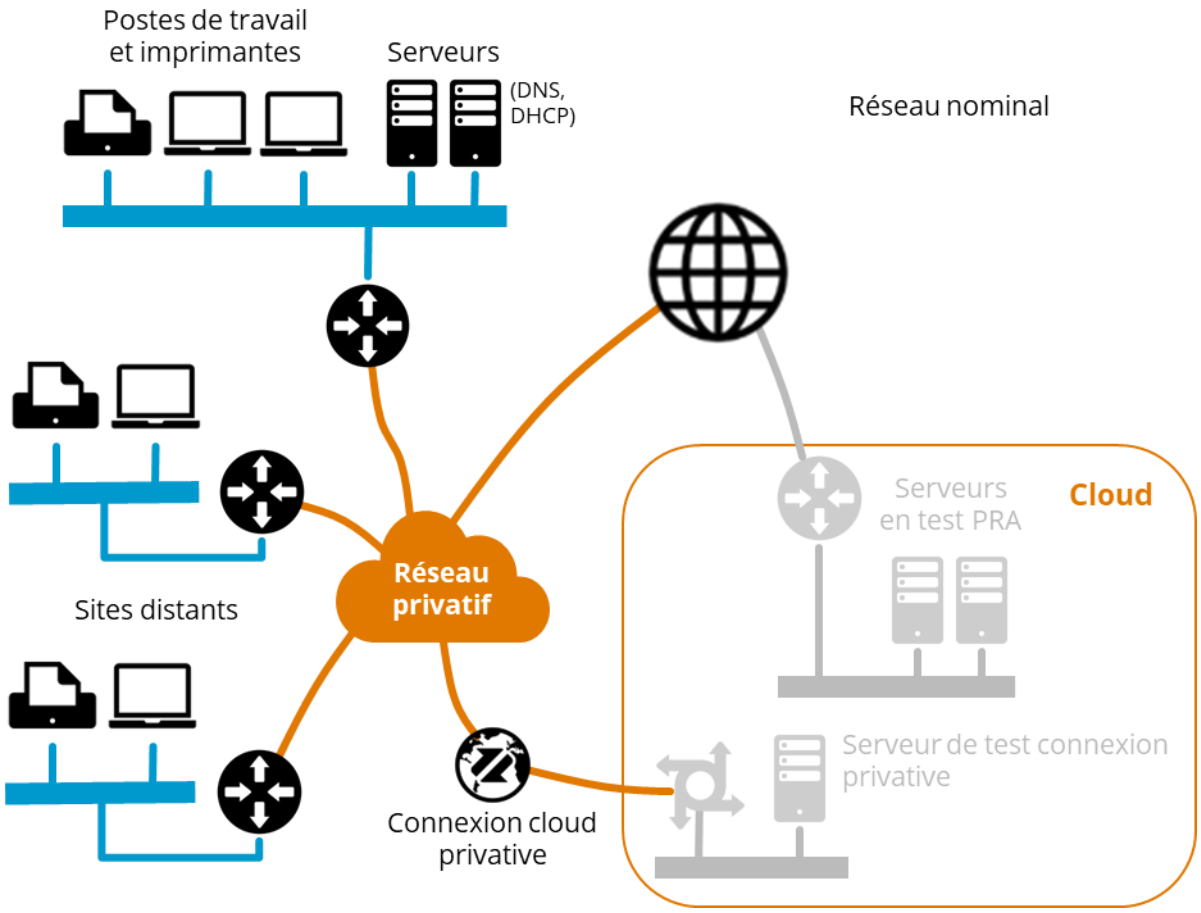

Figure 16 – Réseau étendu privatif. Réseau nominal.

<u>Important, sur le site principal :</u>

Le réseau du site principal doit être organisé en **plusieurs sous-réseaux IP**.

Cette architecture permet de **séparer**

- **les serveurs** du datacenter protégé
- du reste **des autres équipements** tels que postes de travail et imprimantes.

Il existe donc un routeur IP pour ce faire.

L'implantation physique peut varier :

- un seul routeur, qui assure interconnexion des sous-réseaux IP du site et accès au réseau étendu privatif,
- séparation des fonctions d'interconnexion des sous-réseaux IP du site et d'accès au réseau étendu privatif sur deux routeurs.

5.4 - ACTIVATION DU PRA RÉEL SUR LE RÉSEAU PRIVATIF

Un sinistre est survenu.

Réseau nominal, sur le site de l'entreprise :

Il **disparait**, en termes de configuration logique.

Le **Réseau du PRA se substitue** complètement au **Réseau nominal**.

Réseau du PRA, sur le site de l'entreprise, ou déporté en position de repli :

Il **remplace le Réseau nominal**. Il est localisé sur site, ou hors site dans une position de repli, en fonction des dégâts subis dans les locaux. Il regroupe les postes de travail et imprimantes.

Les serveurs originaux, sur site, sont mis hors service du fait du sinistre.

Le réseau local des équipements des utilisateurs **change de plage d'adresses**. Les équipements sont **reconfigurés le service DHCP installé dans le NCA**.

Le NCA est installée, **en rupture du réseau local**. Le NCA est connectée :

- d'une part sur le routeur d'accès à Internet,
- d'autre part au réseau local, vers les équipements des utilisateurs.

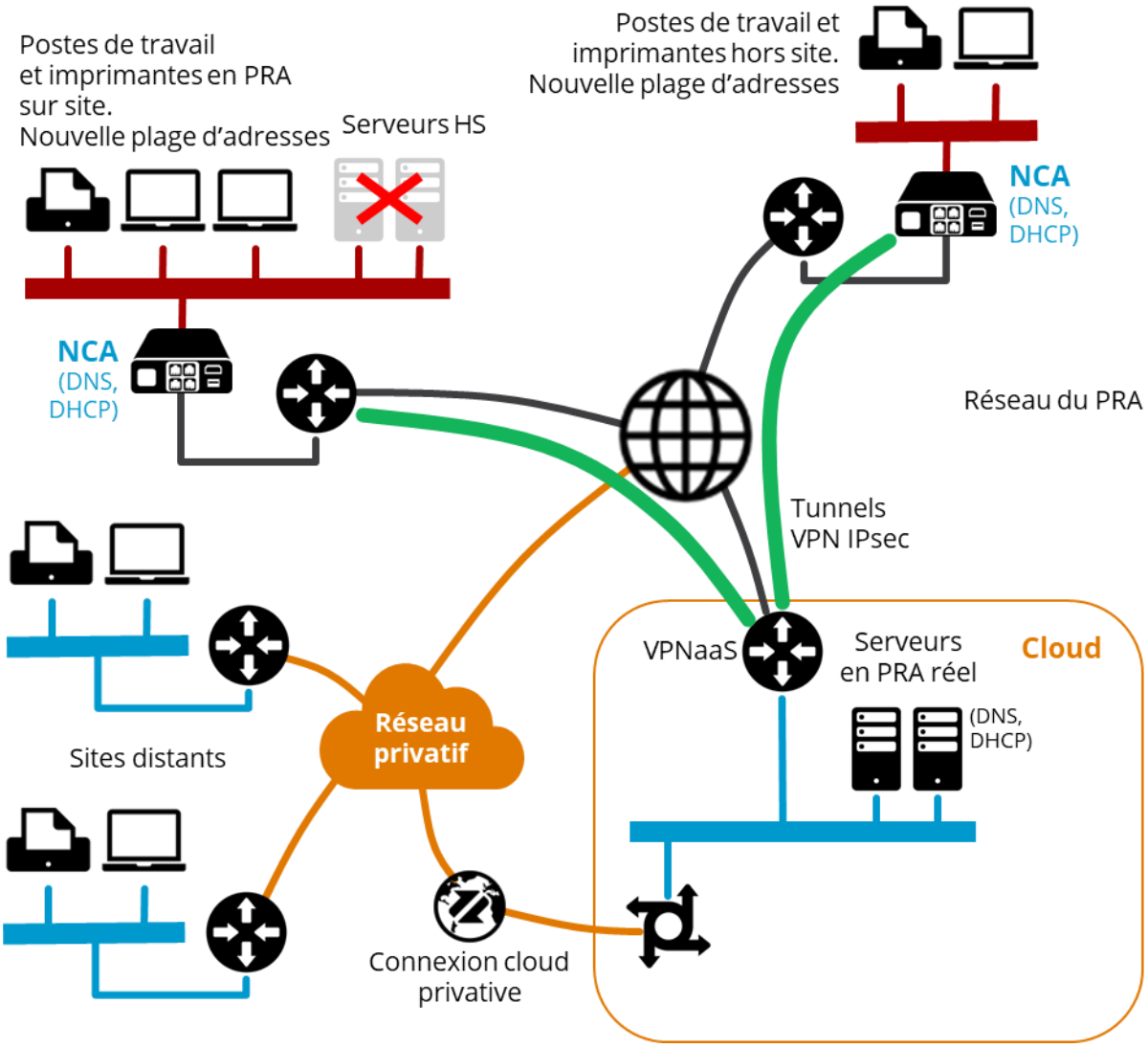

Figure 17 - Réseau privatif. Pra réel.

Réseau du PRA, dans le cloud :

Il regroupe les serveurs restaurés et redémarrés dans le cloud. Ils gardent l'adressage qu'ils avaient sur le Réseau nominal.

Le **service VPN IPsec** (*VPN as a Service*, **VPNaaS**) du cloud Flexible Engine est utilisé. Ce service est associé au *tenant* dédié au PRA du client. Il est instancié et activé lors de l'activation du PRA.

Réseau du PRA, sur les sites distants de l'entreprise :

Les sites ne sont pas impactés par le sinistre.

Le statut de leur réseau change de Réseau nominal à réseau du PRA sans que l'adressage change.

Leur connexion sur le cloud change de cheminement et emprunte la connexion cloud privative (voir le chapitre 5.2.3 - Routage sur le réseau privatif).

5.5 - TEST DE PRA SUR LE RÉSEAU PRIVATIF

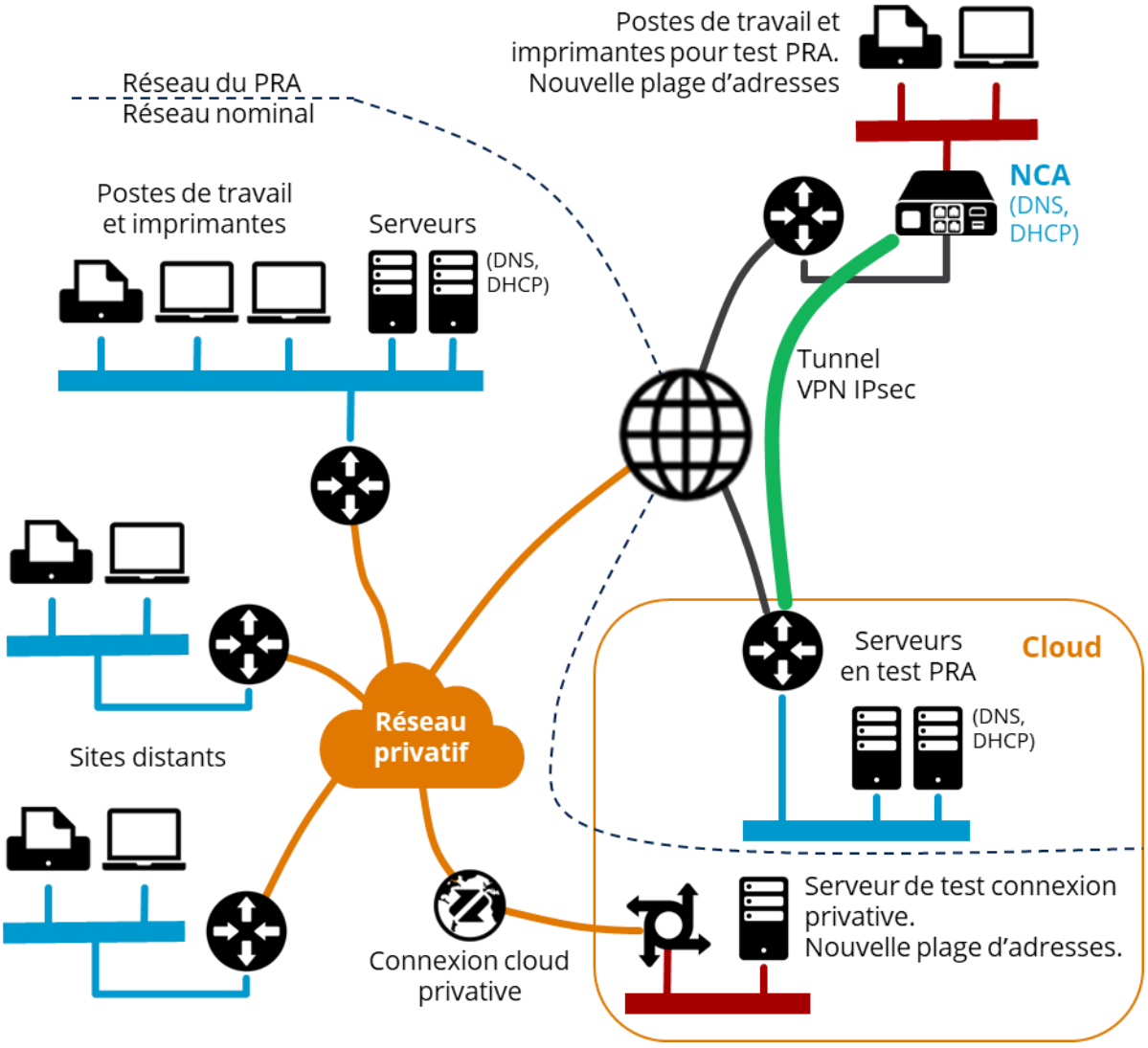

Figure 18 - Réseau privatif. Test de PRA.

Le Réseau du PRA et le Réseau nominal fonctionnent simultanément. Pour cela, **ils doivent être séparés**.

Réseau nominal, sur le site de l'entreprise :

Il reste sans modification.

Réseau du PRA, sur le site de l'entreprise :

La solution est similaire à celle du cas de l'accès à Internet simple.

Un réseau local qui compte **quelques postes de travail et imprimantes doit être installé séparément du Réseau nominal**. Un commutateur séparé ou un réseau local virtuel peut être utilisé pour ce faire. Le réseau local doit être un sous-réseau IP spécifique, qui **dispose de sa propre plage d'adresses IP**.

Le NCA est connectée :

- d'une part au réseau local, vers les équipements des utilisateurs,
- d'autre part à Internet.

La connexion Internet du NCA ne peut être une connexion physique sur le Réseau nominal.

Réseau du PRA, dans le cloud :

Il regroupe les serveurs restaurés et redémarrés dans le cloud. **Ils gardent l'adressage qu'ils avaient sur le Réseau nominal**.

Le **service VPN IPsec** (*VPN as a Service*, **VPNaaS**) du cloud Flexible Engine est utilisé. Ce service est associé au *tenant* dédié au PRA du client. Il est instancié et activé lors de l'activation du PRA.

Test de la connexion directe au cloud

Le test est fondé sur une **extension du Réseau nominal dans le cloud** pendant les tests.

Un serveur de test est implanté dans le cloud. Son rôle est de fournir **une application qui réponde aux requêtes des postes de travail situé dans le Réseau nominal**. Ce peut être un serveur Web, par exemple.

Ce serveur de test, dans le cloud, est instancié uniquement lors des tests.

6 - PRA SUR SD-WAN ET SDN

Terminologie :

- SDN = *Software Defined Networking*.
- SD-WAN = *Software Defined Wide Area Networking*.

Par bien des aspects, l'utilisation des seules technologies, équipement et logiciels SD-WAN aboutit à la construction d'un réseau étendu privatif pour une entreprise. Si nous nous arrêtons là, il ne serait pas nécessaire de développer plus avant ce chapitre.

L'exploitation des technologies et solutions liées aux SDN et SD-WAN n'ont d'intérêt pour nos affaires que si **nous utilisons le modèle et la technologie SDN sur l'ensemble du réseau de l'entreprise**, sans se limiter à son utilisation sur le réseau étendu privatif (le seul SD-WAN).

La technologie SDN doit obligatoirement être utilisée en exploitant sa capacité à **construire plusieurs Réseaux IP sur la même infrastructure physique**. Dans ces conditions le Réseau nominal et le Réseau du PRA cohabitent.

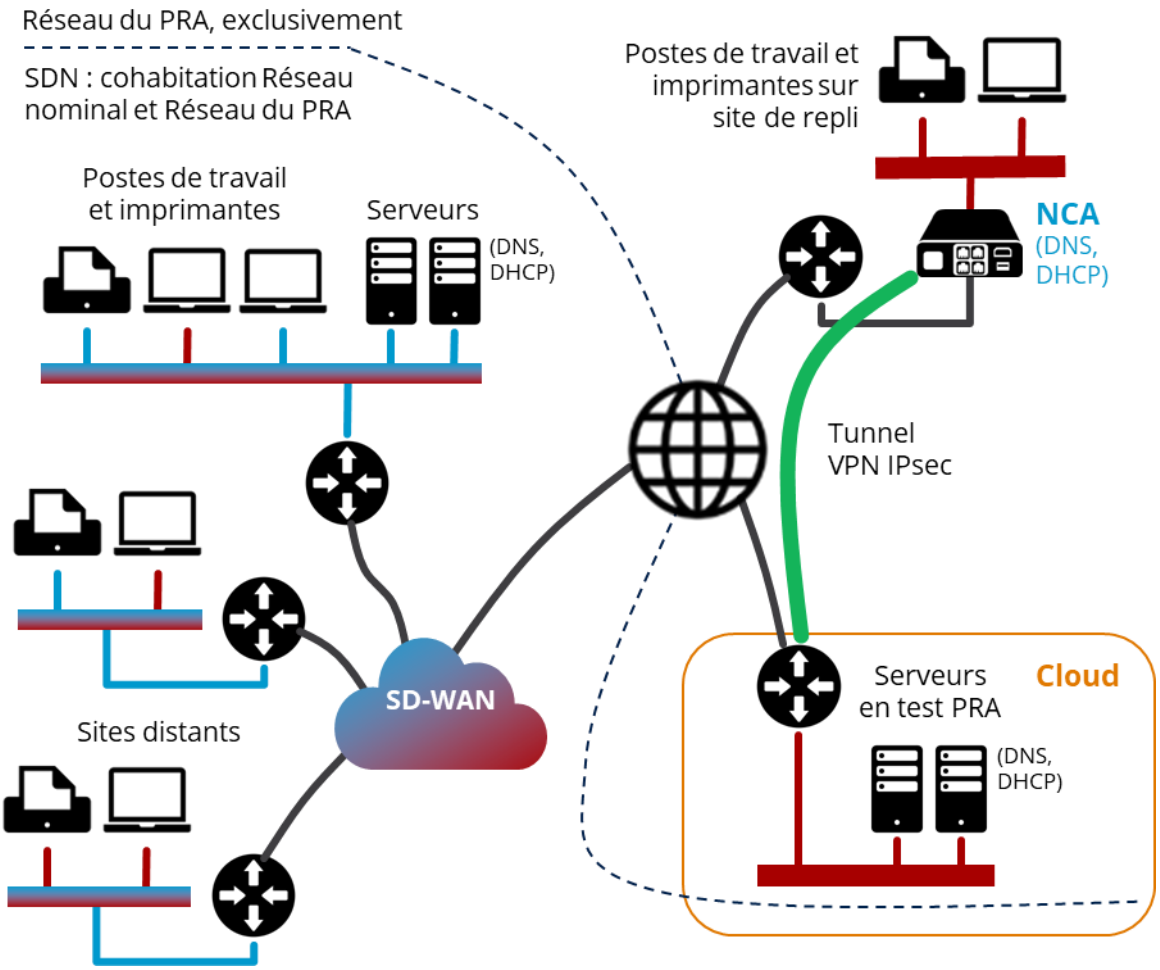

Figure 19 - Réseau SDN

Plusieurs configurations doivent être préparées initialement :

- exploitation nominale,
- test de PRA,

- PRA en cas de sinistre qui détruit le site principal,
- PRA en cas de cyber-attaque.

Chacune peut être activée en cas de besoin, à la demande d'un opérateur. Le basculement ne dure que quelques secondes. La gestion du réseau par rapport au PRA devient alors triviale.

7 - PRA PARTIEL

7.1 - CAS D'USAGE

Le cas d'usage est celui de la réaction à **un sinistre qui n'impacte pas tous les serveurs**. Nous envisageons de continuer l'exploitation en implantant

- une partie des serveurs dans le datacenter original,
- la partie restante des serveurs (qui s'étaient trouvés en défaut) dans le cloud.

Cette configuration fait naître quelques problèmes techniques.

7.2 - IMPLANTER UN PONT ETHERNET

Si la configuration IP des serveurs n'est pas modifiée, il faut considérer que **tous les serveurs font partie du même sous-réseau IP**. Lors du déclenchement d'un PRA partiel, **ce sous-réseau est donc réparti sur les deux sites**. Nécessairement **les deux sites sur lesquels s'appuie le sous-réseau IP doivent être interconnectés par une fonction de pont de niveau liaison de données** (couche 2 du modèle OSI).

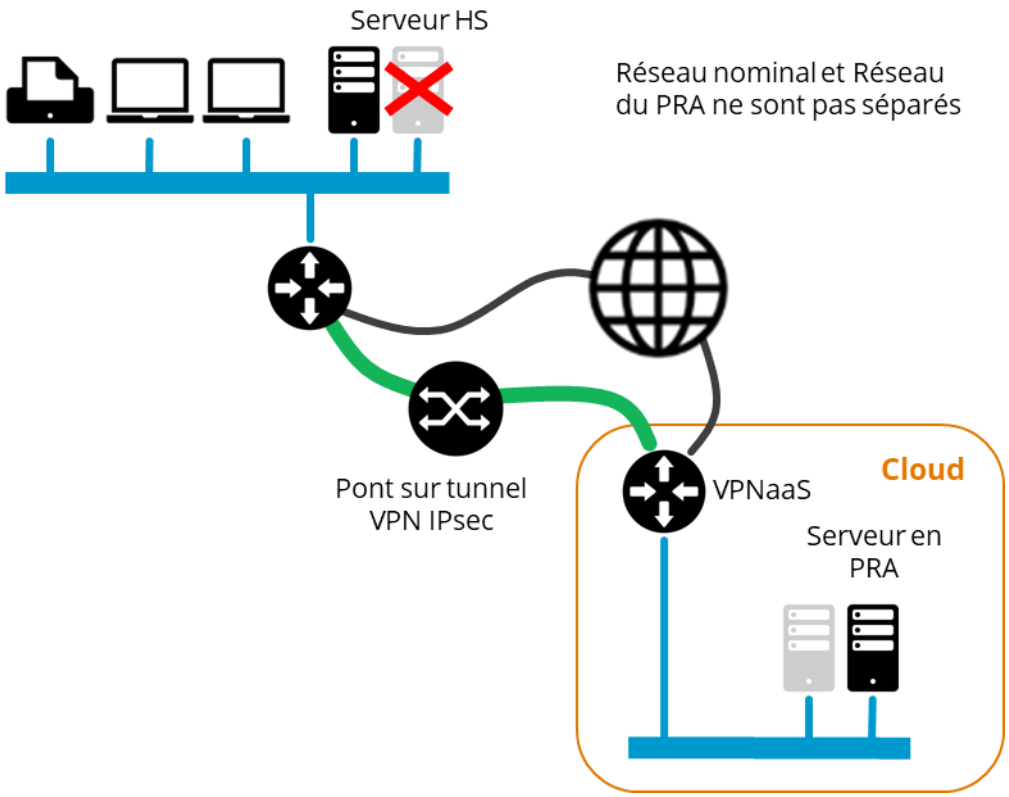

Figure 20 - PRA Partiel

Comment construire ce pont ?

- établir un **VPN IPsec entre le datacenter et le cloud** à travers Internet et/ou un réseau étendu privatif, puis ouvrir le **pont entre les réseaux locaux Ethernet à travers ce**

tunnel ;

- ou utiliser une architecture SDN, qui a le même le même principe technique, mais qui permet de préparer la configuration de secours de façon plus aisée que précédemment.

7.3 - SÉPARER 2 SOUS-RÉSEAUX IP

Hors la solution du pont, il faut **modifier le découpage du réseau en 2 sous-réseaux IP** (datacenter et cloud), et par conséquent modifier

- la configuration de routage de l'ensemble du réseau,
- la configuration IP de chacun des serveurs !

Le lecteur appréciera le risque que constitue la réalisation de l'opération le jour d'un sinistre.

8 - SECOURS PAR RÉSEAU PRIVÉ VIRTUEL SSL

8.1 - ARCHITECTURE, PRINCIPE DE FONCTIONNEMENT

La solution proposée consiste mettre en œuvre un **VPN** sous **protocole SSL** entre les postes de travail des télétravailleurs et le cloud Flexible Engine. Le VPN est porté par Internet.

L'extrémité d'entrée du tunnel VPN est installée dans chaque poste de travail équipé d'un logiciel client pour le VPN : **OpenVPN Connect**. Le logiciel est disponible pour tous les systèmes de postes de travail : **Windows**, **MacOS**, **Linux**, **Android**, **iOS**.

L'image installable du logiciel client **OpenVPN Connect** est téléchargeable sur le site https://openvpn.net/downloads/.

Les utilisateurs de l'entreprise sont déclarés sur le portail d'administration Nuabee Atlas. **Un fichier de paramètre est automatiquement généré** et y est disponible pour **chaque utilisateur**.

Dans le cloud, l'extrémité de sortie du tunnel VPN il est installée dans un serveur de VPN. Ce serveur est fondé sur une machine virtuelle instanciée dans le cloud au moment du besoin, en cas de sinistre. La machine virtuelle fonctionne sous le système **Free BSD**. Le logiciel serveur de VPN est **OPNsense**.

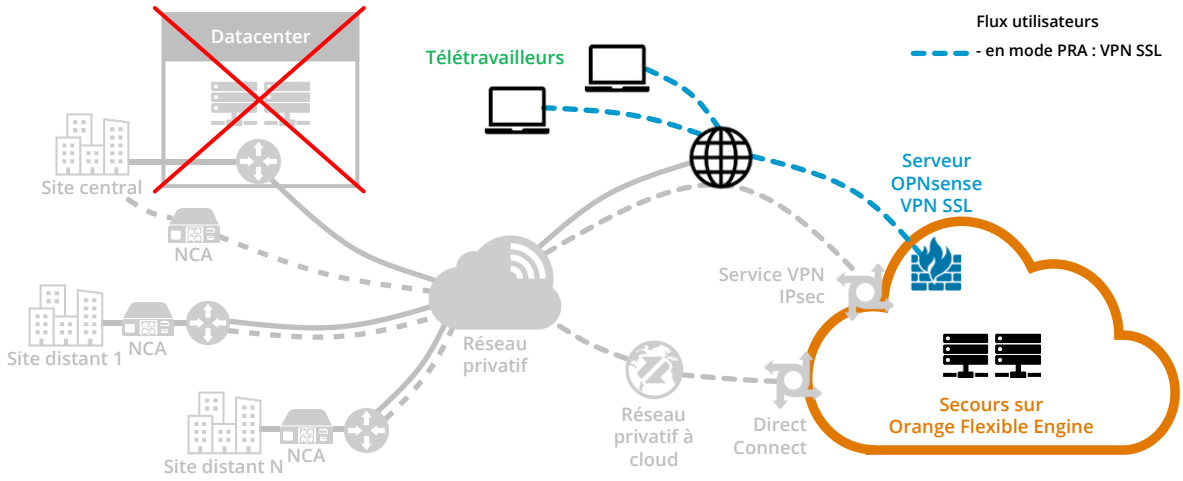

Figure 21 - Reconnexion d'utilisateurs télétravailleur

8.2 - RECONNEXION EN CAS D'ACTIVATION DU PRA

8.2.1 - Au moment du sinistre ou d'un test

Lorsque le PRA est activé, le sinistre peut rendre les locaux du site central hors service.

Les utilisateurs télétravailleurs changent de lieu de travail. Ils sont installés dans des bureaux loués pour remplacer ceux détruits dans un sinistre, ou chez eux. Ils sont équipés chacun d'un poste de travail mobile (PC portable).

Chaque poste de travail doit disposer d'un accès Internet, quelle qu'en soit la forme : accès câblé, WiFi ou 4G/5G.

Chaque utilisateur démarre le logiciel client de VPN SSL sur son poste de travail.

8.2.2 - Préparation de l'utilisation

Comme toute opération dans le PRA, il est préférable que la mise en œuvre de ce VPN SSL soit anticipée et qu'elle fasse l'objet de tests récurrents.

(Décrire la préparation du côté du cloud : serveur de VPN virtualisé. Solution Nuabee : FreeBSD/OPNsence)

La mise en œuvre du serveur de VPN dans le cloud est traitée par Nuabee dans le processus standard de mise en service, de tests et d'activation du PRA.

Il appartient cependant à l'entreprise utilisatrice d'anticiper la configuration des postes de travail. Cette configuration nécessite :

- l'installation du logiciel client de VPN SSL,
- le téléchargement des paramètres propres à chaque utilisateur qui contiennent notamment un certificat d'accès.

Deuxième partie : Sauvegardes dans le Cloud

9 - STOCKAGE OBJET DANS LE CLOUD

Les sauvegardes sont stockées dans le cloud sur un **service de stockage objet** compatible avec la norme **S3** (norme de facto, d'origine AWS).

La **classe de stockage** utilisée est en général **Standard** (stockage chaud), sauf dans le cas du service **d'archivage à long terme** des sauvegardes pour lequel la classe **Cold** (stockage froid) est utilisée.

9.1 - NOTIONS

Les notions exposées dans ce chapitre ne sont pas toute liées directement aux réseaux. Leur connaissance est néanmoins nécessaire pour la compréhension des mécanismes d'interfaçage avec les réseaux.

Bucket, objets stockés :

La solution de sauvegarde utilise un **Bucket** (littéralement, un seau ou un baquet) de stockage objet. Un *Bucket* est **la plus grande unité logique de stockage qui puisse contenir des données**.

Le *Bucket* contient des objets : dans notre cas, des fichiers de sauvegardes.

Les objets de sauvegarde sont organisés hiérarchiquement dans le *Bucket* :

- au plus haut niveau : une branche par client,
- puis aux niveaux intermédiaires : par site et par serveur,
- et au niveau le plus bas : par espace sauvegardé (disque, base de données, fichiers) et par date.

End Point, point d'accès :

Dans le stockage objet, *Buckets* et objets sont accessibles par le réseau à travers une interface de **service Web de type RESTful**.

Le stockage objet présente des **Endpoints** (points d'accès terminaux) qui permettent de l'adresser depuis le Web ou l'intérieur du cloud.

Lors de la mise en œuvre du PRA, une attention particulière est portée à ces points d'accès en termes d'adressage IP et de nommage DNS.

9.2 - ACCÈS AU STOCKAGE OBJET

Les différentes méthodes d'accès au Stockage Objet

- **Accès depuis Internet** : c'est le cas le plus souvent rencontré.
- Accès depuis le **Cloud Flexible Engine** :

- Via le plan d'adressage interne de Flexible Engine,
- Via un mécanisme de **VPC Endpoint Service** + **VPC Endpoint**.

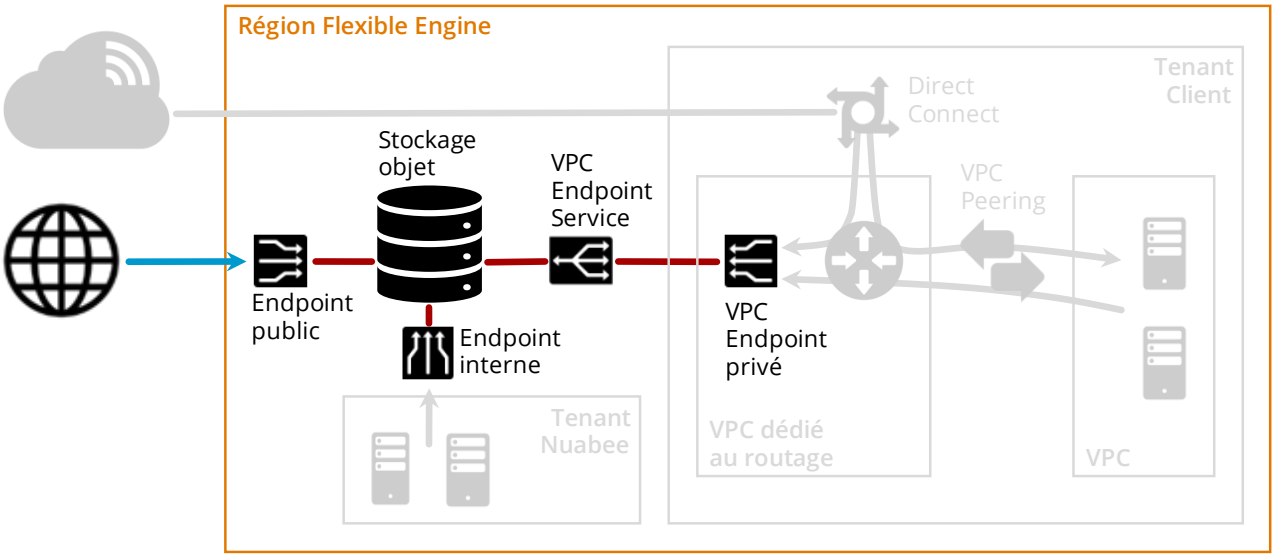

Figure 22 - Stockage objet et endpoints

Endpoint public : accès depuis Internet

Le **Endpoint public** présente **des adresses IP v4 et IP v6** qui sont **dans le plan d'adressage public** d'Internet.

Il possède aussi **un nom** qui est dans un **domaine public d'Internet** et qui est **résolu par le service DNS global d'Internet**.

Typiquement, ce nom est de la forme :

```
bucket_name.oss.eu-west-0.prod-cloud-ocb.orange-business.com
```

Dans ce cas, **le trafic sortant** du stockage objet vers Internet **donne lieu à redevances** (0,0703€ par Go au-delà de 15Go par mois).

Ce cas d'accès est typiquement utilisé par les sauvegardes qui transitent par Internet.

Les adresses IP et le nom utilisé sont documentés par Nuabee auprès des clients afin qu'ils puissent paramétrer leur routeurs et firewall.

Endpoint interne : accès depuis le cloud

Le **Endpoint interne** présente des adresses IP v4 et IP v6 qui sont **dans le plan d'adressage interne de Flexible Engine**. Pour IP v4, l'adresse est dans la plage **100.64.0.0/10** (RFC 6598 : *Reserved IPv4 Prefix for Shared Address Space*, pour implanter *Carrier-Grade NAT*).

Il possède aussi **un nom** qui est dans un **domaine public d'Internet** (le même que précédemment) et qui est **résolu par le service DNS interne de Flexible Engine**.

Ce **Endpoint interne** n'est accessible que **depuis l'intérieur de la région** dans laquelle il se trouve.

Dans ce cas, **le trafic sortant** du stockage objet vers l'intérieur de la région du cloud **ne donne pas lieu à redevance**.

Ce cas d'accès est typiquement utilisé par Nuabee pour restaurer les machines virtuelles d'un client lorsque le PRA est activé.

VPC Endpoint Service + VPC Endpoint : accès depuis le cloud

Le couple **VPC Endpoint Service** + **VPC Endpoint** offre un mécanisme très puissant : le **déport d'un Enpoint de stockage objet en n'importe quel point d'une région** de Flexible Engine, dans un **Virtual Private Cloud** (**VPC**) mis en œuvre par un locataire du cloud.

Le **VPC Endpoint** peut présenter 2 types d'adressage et de nommage :

- **Adresse IP privée**, conforme au RFC 1918 associée à un **nom dans un domaine privé**. Sa résolution doit être assumée par un **service DNS privé**.
- **Adresse IP dans le plan d'adressage public** d'Internet associée à **un nom dans un domaine public d'Internet** et qui est **résolu par le service DNS global d'Internet**.

Dans ce cas, **le trafic sortant** du stockage objet vers l'intérieur de la région du cloud **ne donne pas, aujourd'hui, lieu à redevance**.

À terme, les redevances seront dues :

- VPC Endpoint Service et VPC Endpoint : environ 30 €/mois pour un point d'accès ;
- Trafic : facturé au Go, avec une franchise pour une première tranche de volume ; pas d'indication de prix.

S'il est **routé vers Internet**, par le locataire du cloud, **le trafic sortant donne lieu à redevances** (0,0703€ par Go au-delà de 15Go par mois).

Le 2ème cas d'adressage est typiquement utilisé par les sauvegardes qui transitent par le réseau étendu privatif et sa connexion privative vers le cloud ou qui sont issues du cloud, lorsque le PRA est activé.

Cette solution d'accès permet de **bénéficier d'accès homogènes et universels sur les ressources de stockage objet**, que les sauvegardes soient réalisées via Internet, le réseau étendu privatif ou depuis le cloud.

10 - FLUX DE SAUVEGARDES VERS LE CLOUD

Les serveurs hébergés dans le datacenter de l'entreprise sont **sauvegardés vers un stockage objet dans le cloud**. Plusieurs chemins existent :

- via **Internet**,
- via le **réseau étendu privatif**.

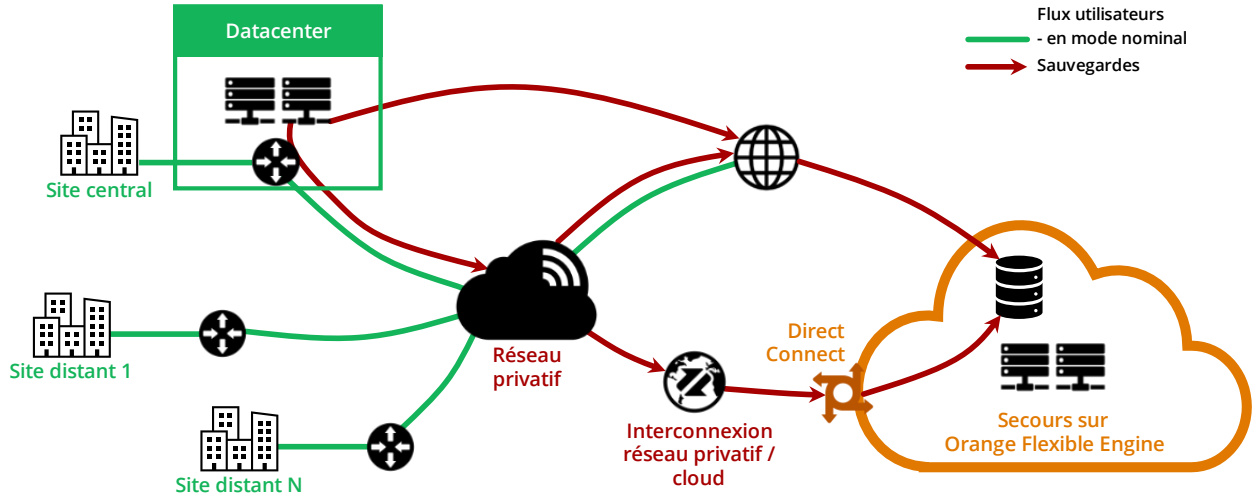

Figure 23 - Cheminement des sauvegardes

10.1 - SAUVEGARDES VIA INTERNET

La solution consiste à utiliser une **connexion directe du datacenter vers Internet**. Cette connexion est fondée sur un accès de type professionnel ou « grand public » porté par une fibre optique et une « box » terminale.

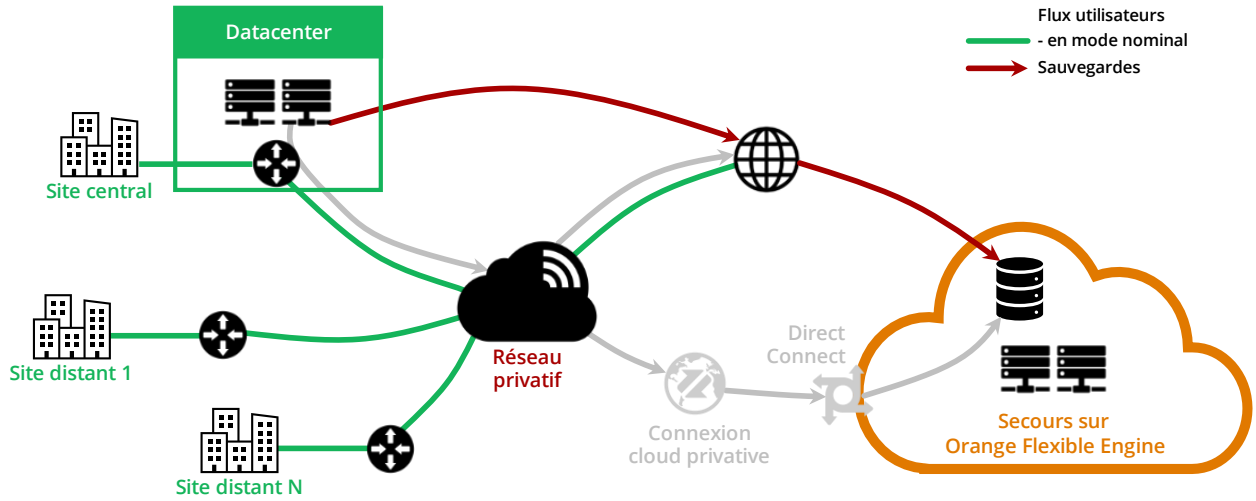

Figure 24 - Sauvegardes via Internet

Rapport performance/prix :

La connexion directe à Internet est généralement beaucoup plus rapide, à prix égal, que l'accès à Internet par le réseau privatif.

Sa qualité de service n'est pas garantie, mais ce n'est pas le plus important si on considère que **c'est un moyen supplémentaire plus performant** en débit par rapport au réseau privatif.

10.2 - SAUVEGARDE VIA RÉSEAU ÉTENDU PRIVATIF ET INTERNET

La solution consiste à utiliser le chemin suivant entre le datacenter de l'entreprise et le stockage objet dans le cloud :

- d'abord le réseau étendu privatif,
- puis Internet à partir du cœur de réseau privatif jusqu'au cloud.

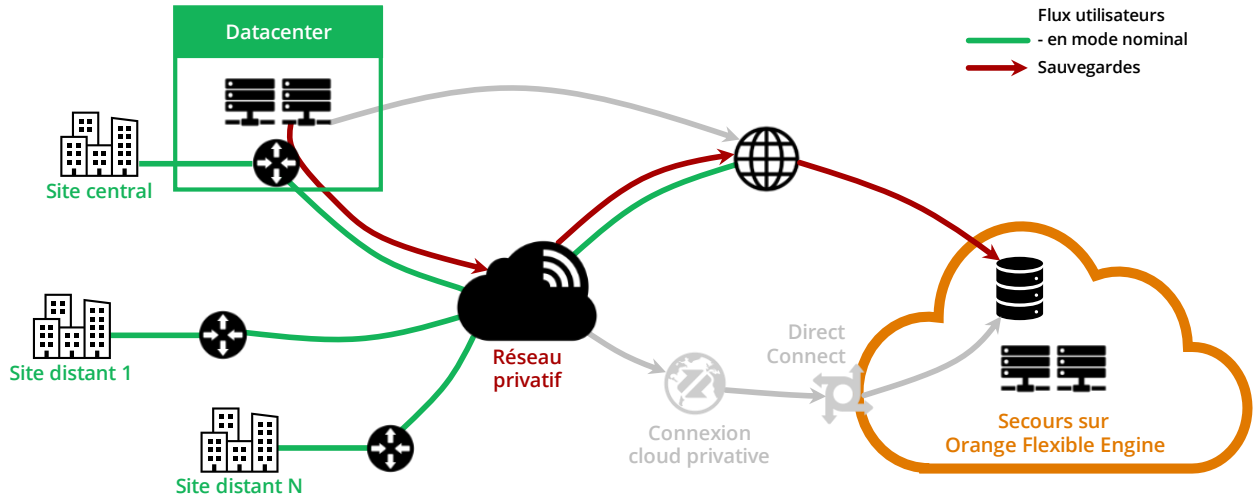

Figure 25 - Sauvegarde via réseau étendu privatif et Internet

Rapport performance/prix :

Le réseau étendu privatif de l'entreprise est opéré par un prestaire de service opérateur qui en garanti les performances, la disponibilité et la sécurité.

Sur le plan des performances en débit rapportées au prix, cette solution est moins favorablement placée que celle fondée sur l'accès direct à Internet.

10.3 - SAUVEGARDE VIA LE SEUL RÉSEAU PRIVATIF

La solution consiste à utiliser le chemin suivant entre le datacenter de l'entreprise et le stockage objet dans le cloud :

- d'abord le réseau étendu privatif,
- puis une interconnexion privée entre le réseau étendu privatif et le cloud.

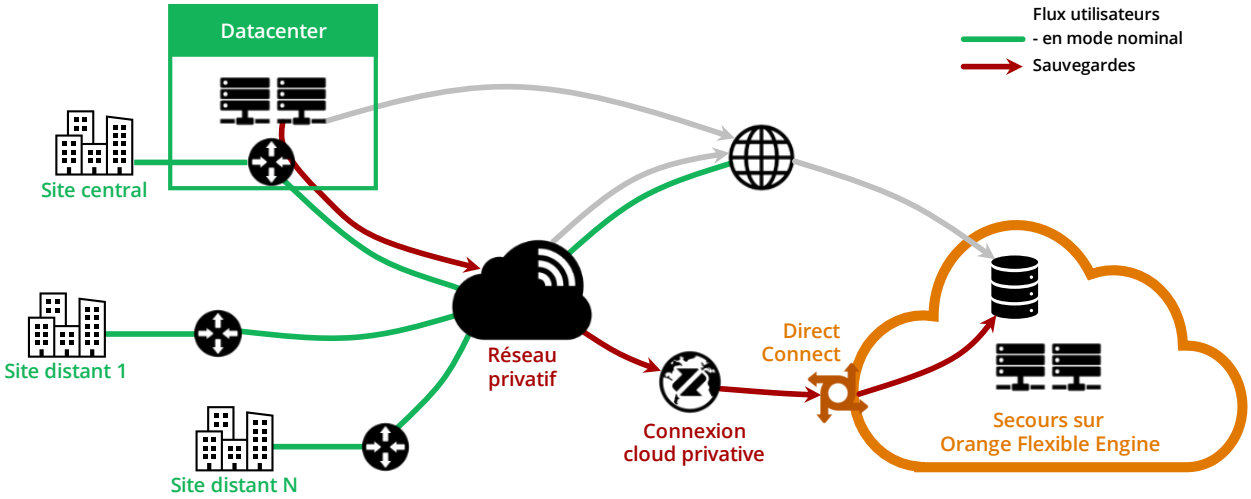

Figure 26 - Sauvegarde via réseau étendu privatif et interconnexion privée au cloud

Coût des ressources du cloud

Pour l'heure, les fonctions VPC Endpoint Service et VPC Endpoint sont en test. Elles ne donnent pas lieu à redevance d'utilisation.

À terme, les redevances seront dues :

- VPC Endpoint Service et VPC Endpoint : environ 30 €/mois pour un point d'accès ;
- Trafic : facturé au Go, avec une franchise pour une première tranche de volume ; pas d'indication de prix.

Rapport performance/prix :

Le réseau est opéré dans sa totalité par un prestaire de service opérateur qui en garanti les performances, la disponibilité et la sécurité.

Sur le plan des performances en débit rapportées au prix, cette solution est moins favorablement placée que les deux autres.