Spécification (ébauche) d’architecture cible Zone d’accueil GCP basée sur la distribution TEF v4

# Introduction

MCN joue un rôle d’aviseur dans le processus de sélection des fournisseurs infonuagique par les organismes publiques (OP) et établissements (santé, éducation). MCN évalue les besoins et contraintes de ces institutions par rapport à l’adoption de l’infonuagique et avise par rapport aux aspects spécifiques fonctionnels et de conformité en relation avec les modalités et technologies disponibles avec les différents fournisseurs participants. MCN a la responsabilité d’approuver les orientations d’architecture des OP et établissements en s’assurant que l’adoption de l’infonuagique par les OP et établissements soit basée sur une zone d’accueil approuvée et se fait en concordance avec les principes directeurs établis par le programme, y compris par rapport à la conformité aux exigences de sécurité en ligne avec le modèle PBMM et optimisation des coûts.

Dans cette qualité MCN est intéressé dans un engagement en partenariat avec Google dans le cadre d’un projet dont le but est de livrer une zone d’accueil pérenne et évolutive, basée sur l’offre infonuagique Google Cloud Platform (GCP), la distribution TEF v4 et en ligne avec les exigences technologiques, de sécurité et de conformité qui régissent le secteur public dans la province de Québec.

# Survol des requis techniques à la base de l’architecture cible

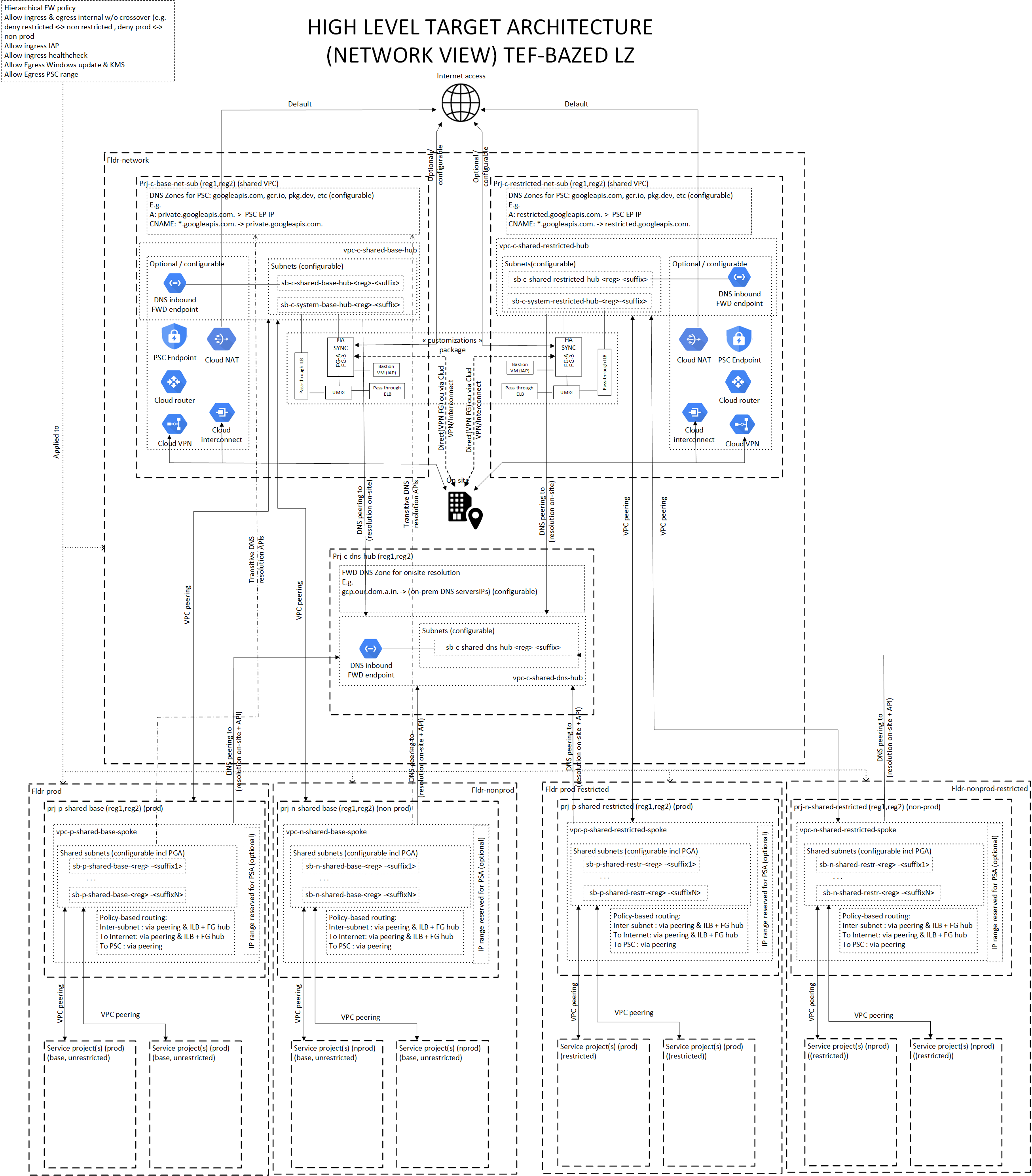
L’architecture cible de la zone d’accueil GCP / TEF envisagée devra s’aligner à quelques principes de base :

* Topologie en étoile « hub and spoke » avec séparation logique entre les environnements « spoke-réseau » (ou « zones ») à différents niveaux de sécurité. Par exemple
  + Séparation entre zones « données sensibles » (protégés « B » avec accès restreint) et « données non-sensibles »
  + Séparation entre zones « production » et « non production »
* Concentration dans le « hub » des services communs comme :
  + Fonctions pare-feu, « NAT »,interface avec Internet, routage BGP
  + Services d’interconnexion hybride entre le nuage et le site (VPN ou dédiés)
  + Services de résolution DNS
  + Services de communication en mode privé avec les services infonuagique (API)
* Possibilité de monter optionnellement (via paramétrage) des « zones » spécialisées, en tant que « spokes » dans cette architecture :
  + Zone de « gestion » pour l’accès administratif aux charges de travail déployées dans les autres zones ainsi que pour des solutions de surveillance spécifiques déplacées dans le nuage en mode « lift & shift »
  + Zone d’identité, en général dédié à l’hébergement des charges de travail type GIA déplacées en mode « lift & shift » dans le nuage (par exemple ADDS)

C’est à noter qu’il n’y a rien de spécial par rapport à ces zones, à part le paramétrage au niveau routage, des règles pare-feu, des contraintes organisationnelle et des permissions d’accès.

* Montage optionnel dans le « hub » d’une solution pare-feu de type « appliance virtuelle », comme le pare-feu Fortigate, avec la capacité d’inspecter le trafic nord-sud et est-ouest entre les zones.
  + Séparer dans un colis de déploiement à part l’écosystème « virtual appliance », dont une instance particulière est l’écosystème Fortigate (mais pour certains OP ou établissements pourrait être par exemple Checkpoint, PaloAlto ou autre)
  + Spécifiquement pour Fortigate le colis déploie aussi les autre ressources nécessaires comme ELB, ILB, « health-check », UMIG, sous-réseau internes, externes, de gestion et de haute-disponibilité, PBR, etc
* Les « spokes » fournissent des sous-réseaux partagés avec des projets de type « service » qui sont en effet les projets qui hébergent
  + les VM « charge de travail » déployées avec leurs vNIC sur les sous-réseaux partagées
  + D’autre services déployés niveau VPC comme des nœuds GKE, GAE « flex », etc
* Les réseaux-virtuels (« VPC ») des spokes sont appariées aux « VPC » des « hub » pour permettre aux projets de « service » l’accès aux services communs
* Les réseaux-virtuels (« VPC ») des spokes sont appariées D’un point de vue résolution DNS aux « VPC » « DNS hub » pour permettre aux projets de « service » l’accès aux services communs et acheminement des flux de résolution publique ou vers le site
* L’architecture est conçue à 3 niveaux, dans 2 « tours » isolés
  + Tour « base » pour déployer des charges de travail données non-sensibles
    - Projet qui héberge le VPC « hub » de base
    - Spokes Production et non-production
    - Projets de type « service » qui hébergent les charges de travail en utilisant les sous-réseaux partagés dans les spokes
  + Tour « restreint » pour déployer des charges de travail données non-sensibles
    - Projet qui héberge le VPC « hub » d’accès restreint
    - Spokes Production et non-production
    - Projets de type « service » qui hébergent les charges de travail en utilisant les sous-réseaux partagés dans les spokes
  + « Hub » DNS dont le rôle est l’acheminement des flux de résolution DNS entre les « spokes » et respectivement le « hub » ou le « site »
* Les contraintes organisationnelles à déployer doivent répondre aux critères de sécurité établis par les exigences de conformité PBMM. Par exemple certaines interdictions
  + Des adresses IP publiques sur les VM charges de travail
  + Des « peering » supplémentaires une fois la zone d’accueil déployée
  + Déploiement dans d’autres zones que celles désignées
  + Accès aux attributs « guest » par les charges de travail sur des VM
  + Virtualisation imbriquée
  + Accès à la console via le port série
  + Connection aux VM en mode autre que OS-Login
* Les contraintes organisationnelles sont déployées au niveau du folder racine du déploiement de la zone d’accueil
* Les règles pare-feu déployées doivent répondre à certains critères de sécurité
  + Gestion centralisée (par exemple règles hiérarchiques appliquées au niveau des dossiers)
  + Basés sur des mécanismes inaltérables par les projets de service (par exemple interdire des règles pare-feu basés sur des « étiquettes réseau » manipulables au niveau des projets de service
  + Barrer de façon explicite la communication entre les zones avec niveaux de sécurité différents (par exemple production et non-production)
* Même si pas représenté en détail sur le diagramme, l’architecture inclut :
  + Paramétrage pour choisir mode de déploiement des ressources à travers régions:
    - Déploiement dans une seule région
    - Déploiement dans 2 régions
  + Paramétrage pour choisir les modalités de journalisation
    - Envoi optionnel en BigQuery
    - Durées de rétention ajustables par catégorie
    - Destinations paramétrables (p.e. « log sink » et/ou GCS et/ou BQ)
  + Déploiement multi-instance en dessous d’un folder, pour faciliter pas juste le développement mais des scénarios de déploiement hiérarchique (par exemple des branches connectées à travers un réseau isolé hors-nuage avec les quartiers-généraux de l’OP)
  + Déploiement optionnel du périmètre de sécurité dans le « hub »
* Topologie des réseaux virtuels dans les projets « spoke »
  + En fonction des besoins des OP ou établissements des sous-réseaux partagées sont déployées automatiquement au niveau des « spokes » (production et non-production) dans les 2 tours (« base » et « accès restreint »
  + Le paramétrage de ces sous-réseaux permet de choisir certaines options comme les noms, descriptions, plages d’adresse, l’accès privé Google, les règles de routage
  + En général les rôles (visibles dans les noms) des sous-réseaux approvisionnées dans un VPC « spoke » tombent dans 3 catégories
    - Publique
      * Accès permis vers et ’Internet via le pare-feu dans le « hub »)
      * Accès permis de et vers le « sur site » à travers les services d’interconnexion dans le « hub » (Interconnect ou VPN)
      * Accès permis vers sous-réseaux applicatifs
      * Accès privé vers services PaaS GCP
    - Applicatif
      * Accès permis vers Internet, à travers le pare-feu du hub, pour des raisons spéciales comme les MAJ Windows)
      * Accès permis vers les sous-réseaux « données »
      * Accès permis en provenance du sous-réseau « publique »
      * Accès privé aux services PaaS GCP
    - Données
      * Accès permis vers Internet, à travers le pare-feu du hub, pour des raisons spéciales comme les MAJ Windows)
      * Accès permis en provenance du sous-réseau « applicatif »
      * Accès privé aux services PaaS GCP
* Sécurité des flux de communication est-ouest
  + Par défaut le trafic est-ouest entre sous-réseaux avec des rôles différents est routé à travers le pare-feu dans le « hub » en utilisant le mécanisme PBR
  + Par défaut le trafic entre sous-réseaux dans le même VPC « spoke » et au niveau du même rôle n’est pas routé à travers le pare-feu dans le « hub »
  + Le routage est-ouest soit local soit à travers le pare-feu est paramétrable à travers des règles PBR qui prennent comme arguments les plages d’adresse IP des sous-réseaux
* Sécurité des flux de communication nord-sud
  + Par défaut le trafic nord-sud entre les sous-réseaux et les points d’accès privé aux services PaaS GCP ne passe pas à travers le pare-feu
  + Par défaut les flux de résolution DNS externe (Internet) passent à travers le pare-feu dans le « hub »
  + Par défaut le flux entre les charges de travail (avec des vNIC dans les sous-réseaux partagées dans les VPC « spoke ») et l’Internet passent à travers le pare-feu, pour le « sortant » et pour l’ « entrant » (dans le cas des sous-réseaux publiques)
  + Optionnellement (via paramétrage) les flux sortants vers l’Internet peuvent être routés directement à travers le service NAT à la place de les passer à travers le pare-feu (à valider avec la sécurité si conforme PBMM)
  + Pour la « tour » « accès restreint », par défaut (mais paramétrable) le flux de communication de l’internet est barré et le sous-réseau publique communique avec le sur-site seulement

# Diagramme « vue réseau » (ébauche)



Le diagramme ci-haut offre une vue conceptuelle et simplifiée pour la vue-réseautique de l’architecture cible. Cette architecture cible est alignée avec l’architecture TEF avec quelques ajustements qui seraient bénéfiques aussi pour l’architecture de la distribution TEF

* Paramétrage (enlever le codage en dur)
* Simplification en évitant la duplication des instances de services et ressources
* Rajout du colis optionnel « customisation » pour déployer le(s) « virtual appliance » et les ressources afférentes (ELB/ILB, health-check, routage PBR, jump-point gestion, etc)

L’architecture cible envisagée est similaire pas juste à l’architecture TEF actuelle mais aussi à l’architecture d’autres zones d’accueil certifiées par MCN

# Annexe – vue réseau simplifiée de l’architecture TEF actuelle telle que déployée dans l’environnement d’essais MCN

