Choisir un élément de construction.

Centre de la sécurité des télécommunications
Communications Security Establishment

CENTRE CANADIEN POUR LA CYBERSÉCURITÉ

Zones de sécurité de réseau en nuage

Praticien

TLP:CLEAR

© Gouvernement du Canada
Le présent document est la propriété exclusive du gouvernement du Canada. Toute modification, diffusion à un public autre que celui visé, production, reproduction ou publication, en tout ou en partie, est strictement interdite sans l'autorisation expresse du CST.

Canada

Avant-propos

Le présent document non classifié est publié avec l'autorisation du dirigeant principal du Centre canadien pour la cybersécurité (Centre pour la cybersécurité).

Il fait partie d'une série de documents élaborés par le Centre pour la cybersécurité dans le but de sécuriser les services fondés sur l'infonuagique. Il appuie l'approche de gestion des risques liés à la sécurité infonuagique définie dans l'ITSM.50.062, *Gestion des risques liés à la sécurité infonuagique* [1][1].
Pour obtenir plus d'information ou suggérer des modifications, veuillez communiquer avec le Centre pour la cybersécurité :

Centre d'appel

contact@cyber.gc.ca

(613) 949-7048 Sans frais : 1-833-CYBER-88

Date d'entrée en vigueur

Le présent document entre en vigueur le 12 juin 2023.

Historique des révisions

Version	Modifications	Date
1	Première version	12 juin 2023

[1] Les numéros entre crochets renvoient à du matériel de référence figurant à la section Contenu complémentaire du présent document.

Vue d'ensemble

Le présent document décrit les modèles et les architectures de zones de sécurité de réseau en nuage et offre des conseils techniques sur la mise en œuvre des zones de sécurité de réseau en nuage.

L'orientation qu'il fournit est destinée aux solutions de technologie de l'information (TI) au sein du gouvernement du Canada s'exécutant au niveau NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B (c'est-à-dire, dont le niveau de sensibilité est faible ou partiel). Il convient de noter que les systèmes utilisés dans les domaines PROTÉGÉ C ou classifiés (c'est-à-dire, hautement sensibles) pourraient nécessiter d'autres considérations de conception qui dépassent la portée du présent document. Pour les organisations non gouvernementales, les conseils fournis dans le présent document sont destinés aux solutions de TI dont les ressources sont faiblement ou partiellement sensibles. Les systèmes traitant des niveaux de classification des données plus élevés nécessitent des considérations de conception supplémentaires qui dépassent la portée du présent document. Vous pouvez communiquer avec le Centre d'appel par courriel ou par téléphone pour obtenir des conseils sur les solutions cryptographiques pour les domaines PROTÉGÉ C ou classifiés.

Il incombe à votre organisation de définir les objectifs en matière de sécurité qu'il convient de fixer pour protéger ses services et ses données. Suivre les conseils formulés dans le présent document ne suffit pas pour sécuriser adéquatement un environnement informatique.

Ce document est destiné aux praticiens des TI qui sont familiers avec les principes, les normes et la terminologie de l'ingénierie des réseaux. Pour de plus amples conseils sur la sécurité de réseau, prière de communiquer avec notre Centre d'appel :

Centre d'appel :

contact@cyber.gc.ca

(613) 949-7048 Sans frais : 1-833-CYBER-88

D97-4/80-023-2023F-PDF

978-0-660-48166-1

Table des matières

Liste des figures

Liste des tableaux

Liste des annexes

1 Introduction

Ce document présente des détails et des concepts ayant trait à la segmentation réseau et à l'établissement de zones qui s'appliquent aux environnements en nuages. Il s'agit d'un complément à l'ITSP.80.022, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau* [2] du Centre pour la cybersécurité, et à ses annexes. Vous devriez vous familiariser avec les concepts présentés dans l'ITSP.80.022 avant de lire et de mettre en œuvre les conseils de la présente publication.

L'établissement de zones réseau pose les bases d'une stratégie et d'une architecture de sécurité réseau reposant sur une défense en profondeur qui peut prendre en charge toute une gamme de solutions de sécurité répondant aux exigences opérationnelles de votre organisation. Pour de plus amples renseignements sur l'approche de sécurité réseau reposant sur une défense en profondeur, consultez l'ITSG-38, *Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones* [3] et l'ITSP.80.022 [2] publiés par le Centre pour la cybersécurité. Ces zones proposent également une infrastructure réseau commune pour assurer la prise en charge de la prestation électronique de services, de l'interconnectivité et de l'interopérabilité. Si votre organisation partage une infrastructure commune pour la prestation électronique de services ou d'autres fins, vous devez vous conformer à toutes les normes de sécurité établies pour l'infrastructure en question.

Le présent document décrit les principes de conception d'architecture et de mise en œuvre de la segmentation d'un environnement en nuage en différentes zones de sécurité réseau. De plus, il explique en détail la façon dont ces principes sont adaptés et leur pertinence pour l'établissement de zones réseau sur site traditionnelles. Les conseils s'appliquent principalement à l'utilisation d'une infrastructure-service (IaaS pour *Infrastructure as a Service*) et d'une plateforme-service (PaaS pour *Platform as a Service*). Ce document offre, par exemple, des conseils sur l'utilisation des microservices et des modèles d'interface de programmation d'applications (API pour *Application Programming Interface*).

Il incombe au fournisseur de services infonuagiques (FSI) d'établir les zones réseau de l'environnement en nuage d'un logiciel-service (SaaS pour *Software as a Service*). Un environnement PaaS est une plateforme multilocataire pouvant être sujette à l'établissement de zones réseau par le FSI. Votre organisation est responsable de s'assurer que les applications SaaS et PaaS respectent la stratégie de sécurité établie, en particulier en ce qui concerne l'établissement de zones réseau. Les exigences de sécurité devant être respectées par les applications d'entreprise sont tirées de la stratégie de sécurité ou du cadre de gestion des risques de votre organisation. On peut également utiliser l'ITSG-33, *Gestion des risques liés à la sécurité : Une méthode axée sur le cycle de vie* [4] du Centre pour la cybersécurité à titre de cadre de gestion des risques afin de déterminer les contrôles de sécurité devant être mis en œuvre par votre organisation. La modélisation des menaces, ce qui comprend l'identification de menaces particulières, doit faire partie du cadre de gestion des risques de votre organisation.

Remarque :

Les conseils formulés dans le présent document évolueront au fil du temps en fonction des changements technologiques. Par exemple, les conseils mentionnés à la section 6 sur les différents modèles d'utilisation suivront l'évolution des technologies infonuagiques.

Si vous mettez en œuvre des solutions de TI et que votre organisation est un ministère ou un organisme du Gouvernement du Canada (GC), vous devez respecter toutes les politiques du Conseil du Trésor (SCT), dont les suivantes :

- *Politique sur les services et le numérique* [5];
- *Politique sur la sécurité du gouvernement* [6];
- *Directive sur la gestion de la sécurité* [7].

Les ministères et les organismes du GC doivent également consulter l'orientation relative à la résidence des données électroniques [8] du SCT pour des détails sur les exigences présentées dans le *Livre blanc : Directive sur les services et le numérique* [9]. Si votre organisation n'est pas un ministère ou organisme du GC, vous pouvez vous reporter à ces politiques pour obtenir de plus amples renseignements.

2 Facteurs à considérer en ce qui concerne le nuage

Les charges de travail des organisations migrent de plus en plus vers le nuage et le périmètre dépasse désormais l'environnement sur site. Votre organisation doit donc repenser la façon dont elle protège et surveille les environnements en nuages. Il est également essentiel de comprendre comment les principes de zone de sécurité réseau, comme ceux définis dans l'ITSP.80.022 [2], se transposent dans l'établissement des zones de sécurité de vos réseaux en nuage.

Les principes présentés dans l'ITSP.80.022 [2] sont pertinents tant pour les centres de données traditionnels que pour les environnements en nuages. Dans un environnement en nuage, la réseautique a évolué et utilise désormais des réseaux à définition logicielle (SDN pour *Software-Defined Network*). Comparativement à un réseau traditionnel, un réseau SDN présente différentes caractéristiques et capacités qu'il faut prendre en considération lors de la segmentation d'un environnement en nuage en différentes zones de sécurité réseau.

Voici certaines des différences importantes par rapport à un réseau traditionnel :

- dissociation du plan de contrôle du plan de données des appareils physiques;
- point de provisionnement et de gestion centralisé et unique des configurations;
- point de contrôle centralisé pour une réglementation rigoureuse de l'information relative à la sécurité et aux politiques.

Vous devez savoir que même si le FSI offre un accès à la gestion et au plan de contrôle de son réseau SDN, cet accès est offert en faisant appel à l'abstraction des ressources et à une couche de contrôle similaire à celle employée dans le modèle SaaS. Le FSI ne fournit pas un accès direct à ses réseaux SDN ni à leur mise en œuvre, peu importe s'il est question de composants logiciels, de matériel ou d'une partie de la structure informatique du FSI.

Les environnements de centres de données traditionnels et en nuage partagent tous deux les mêmes principes de base pour ce qui est de contrôler et de restreindre les accès et le trafic des communications de données à certains composants ou utilisateurs. Ces deux types d'environnements établissent les périmètres du réseau et la défense en profondeur des frontières connexes au moyen des fonctions suivantes :

- définir les entités qui occupent les zones;
- déterminer les points d'entrée et de sortie distincts;
- filtrer le trafic réseau aux points d'entrée et de sortie;
- surveiller l'état du réseau;
- authentifier l'identité des dispositifs réseau, des utilisatrices et des utilisateurs;
- surveiller le trafic réseau aux points d'entrée et de sortie.

L'ITSP.80.022 [2] définit plusieurs types de zones. Votre organisation doit comprendre comment convertir ces zones dans un environnement en nuage. Le tableau ci-dessous présente une mise en correspondance qui sera abordée en détail dans les sections suivantes.

Tableau 1 : Mise en correspondance des zones

Zone	ITSP.80.022 Environnement réseau traditionnel	Environnement en nuage
Zone publique (ZP)	Entièrement ouverte, elle comprend les réseaux publics comme Internet.	Entièrement ouverte, elle comprend les réseaux publics.
Zone d'accès public (ZAP)	Une ZAP négocie les accès entre les systèmes opérationnels et la ZP et protège le réseau interne. En ce qui a trait à la confiance accordée par les partenaires, les extranets qui se connectent par l'intermédiaire d'une ZAP diffèrent de ceux qui traversent une zone extranet d'accès restreint (ZEAR).	Une ZAP mise en place dans un environnement en nuage sert à atteindre les mêmes objectifs. Dans un modèle IaaS ou PaaS, la ZAP est plus décentralisée et dispose de plusieurs points terminaux publics. Le trafic qui entre dans une ZAP n'emprunte pas nécessairement un seul chemin de périmètre en périphérie. Le FSI peut fournir plusieurs options de connectivité réseau pour les extranets et les ZEAR.
Zone de travail (ZT)	Une ZT est l'environnement standard pour les activités courantes d'une organisation. Dans une ZT, le trafic n'est généralement pas restreint et peut provenir de sources internes ou de sources externes autorisées.	Il existe des similitudes et des différences entre les ZT des environnements sur site et en nuage. Une des principales différences est que les utilisatrices et utilisateurs se trouvent toujours à l'extérieur de l'environnement en nuage. Ils accèdent aux zones du nuage à partir d'une ZT sur site ou d'une ZP. Il est possible que des utilisatrices ou utilisateurs avec et sans accès privilégié se trouvent dans la même ZT réseau sur site et qu'ils accèdent à différentes zones de l'environnement en nuage, comme dans le cas dans une conception réseau traditionnelle. Des postes de travail virtuels peuvent être mis en place dans l'environnement en nuage pour répondre à différentes exigences organisationnelles et opérationnelles, ce qui est similaire au fait de fournir des stations

Zone	ITSP.80.022 Environnement réseau traditionnel	Environnement en nuage
		de travail et d'autres dispositifs dans une ZT sur site.
Zone d'accès restreint (ZAR)	Une ZAR offre un environnement réseau contrôlé qui convient généralement aux services informatiques essentiels aux activités. La ZAR convient également aux très grands dépôts de données0 sensibles. La dernière version de l'ITSP.80.022 [2] conseille que tous les accès à une ZAR à partir d'une ZP passent par une ZAP et une ZT.	Dans un environnement en nuage, la ZAR est configurée de manière à répondre aux contrôles de sécurité de base définis par l'organisation, selon les exigences opérationnelles et la fonction de la ZAR. Dans un tel cas, les utilisatrices et utilisateurs avec et sans accès privilégié se connectent à la ZAR à partir d'une ZP en passant d'une ZAP à une ZT et, au besoin, à une ZATR. On peut également utiliser un agent de sécurité d'accès au nuage (CASB pour *Cloud Access Security Broker*) dans le cadre des services de périmètre ou en périphérie. Dans un tel cas, la ZAR de l'environnement en nuage est accessible par l'intermédiaire du CASB et la ZAP depuis la ZP ou sur site.
Zone d'accès très restreint (ZATR)	La ZATR offre un environnement en réseau avec des contrôles rigoureux. Elle est conçue pour les services de plateforme d'entreprise et d'applications ainsi que pour les enclaves de client nécessitant les plus hauts niveaux de protection. Par exemple, une telle zone peut servir à l'information hautement sensible ou à l'information classifiée. La ZATR convient aux très grands dépôts de données sensibles.	À l'heure actuelle, l'environnement en nuage ne convient pas aux ZATR. Il peut toutefois être utilisé pour les grands dépôts de données sensibles, tel qu'il est énoncé dans la stratégie de sécurité de l'organisation. Prière de consulter la topologie de connectivité des enclaves de données (section 6.5) pour plus de détails.
Zone extranet d'accès restreint (ZEAR)	La ZEAR peut prendre en charge les services extranets en connexion directe avec des partenaires de confiance.	Le FSI fournit généralement plusieurs options de connectivité réseau pour les ZEAR. Il peut s'agir, par exemple, d'une passerelle de réseau privé virtuel (RPV) ou de liens vers un réseau privé prenant en charge des services extranets avec

Zone	ITSP.80.022 Environnement réseau traditionnel	Environnement en nuage
		connexion directe aux partenaires de confiance, comme un appairage de réseaux virtuels et des points terminaux de réseaux privés.
Zone de gestion (ZG)	La ZG est une zone isolée dont la robustesse est similaire à celle d'une ZAR. Elle offre aux administratrices et administrateurs réseau un réseau d'administration dédié et isolé au moyen duquel ils peuvent configurer et surveiller les infrastructures du réseau. Sur le plan de la sécurité, cette zone permet aux administratrices et administrateurs d'exécuter des opérations de commande et de contrôle tout en minimisant le risque d'interception ou de compromission. Deux approches peuvent être adoptées au moment de déployer une telle zone : la ZG isolée ou la ZG consolidée. On conseille à l'heure actuelle de privilégier l'approche de la ZG isolée. Prière de consulter l'ITSP.80.022, Annexe E [2], pour plus de détails.	L'environnement en nuage comporte des relations univoques, ce qui modifie sa posture de sécurité. C'est particulièrement vrai si on fait adopte l'approche de la ZG consolidée. Pour configurer la ZG native en nuage, le FSI offre à l'organisation des services de gestion en mode natif à partir d'un SaaS. Il incombe à l'organisation de s'assurer que les paramètres de sécurité de la ZG offrent la posture de sécurité souhaitée. La ZG native en nuage fournit des services spécialisés, comme la gestion de machines virtuelles (VM pour *Virtual Machine*). La ZG étant intégrée à la structure informatique du FSI, il n'est pas nécessaire d'avoir recours à des interfaces réseau distinctes pour assurer la gestion des ressources natives en nuage. Plusieurs des avantages offerts par cette zone en matière de sécurité seront abordés en détail à la section 4.

3 Point d'interface de zone (PIZ)

L'ITSP.80.022 [2] définit un point d'interface de zone (PIZ) comme étant un système bidirectionnel entre deux zones. La différenciation entre les zones se nomme la frontière. La frontière contient des PIZ qui représentent les seuls points de connexion entre les zones. Toutes les données doivent être transmises d'une zone à une autre par un PIZ, lequel connecte exclusivement ces deux zones et crée un chemin de communication distinct.

Le PIZ en nuage est le concept logique servant à décrire l'interface contrôlée qui relie deux zones. D'autres mécanismes de séparation logiques peuvent être employés dans un environnement en nuage. Même s'ils ne répondent pas nécessairement à toutes les exigences fonctionnelles de sécurité (voir le tableau 2) d'un PIZ, ces mécanismes peuvent jouer un rôle dans l'établissement de zones dans les réseaux.

Remarque :

On compte deux types de PIZ : les PIZ connectés à une ZG et les PIZ de chemin de données. Prière de consulter l'ITSP.80.022, Annexe F [2], pour plus de détails sur ces deux types de PIZ. Le glossaire (section 7.2) fournit également la définition des deux types de PIZ.

Certains concepts de la présente section s'appliquent à la façon dont les FSI mettent en œuvre la sécurité comparativement aux méthodes sur site patrimoniales. Ces concepts font toutefois partie d'une stratégie de défense en profondeur qui est typiquement non disponible dans un environnement réseau traditionnel ou décrite dans l'ITSP.80.022 [2]. Dans les environnements natifs en nuage, une posture de sécurité forte est étroitement liée à la gestion des identités et de l'accès (GIdA). Le service de GIdA d'une ZG en nuage exige que les organisations mettent en œuvre un contrôle d'accès basé sur les rôles (RBAC pour *Role-Based Access Control*) pour contrôler les autorisations des utilisatrices, des utilisateurs et des ressources. Le contrôle d'accès basé sur les rôles devrait être structuré de façon à appliquer le principe du droit d'accès minimal. S'il est appliqué adéquatement, le principe du droit d'accès minimal permet d'améliorer grandement la sécurité et de réduire les risques. L'objectif du droit d'accès minimal est de s'assurer que toutes les utilisatrices et tous les utilisateurs se connectent au moyen de leur compte d'utilisateur avec les autorisations minimales absolues nécessaires à la réalisation de leurs tâches, et rien de plus.

Dans un environnement en nuage, le service de GIdA de la ZG offre le niveau le plus élevé de séparation logique sous la forme d'un compte de niveau supérieur. Un compte de niveau supérieur est semblable au concept d'administrateur de domaine ou à un compte de niveau racine dans un environnement sur site. Le compte de niveau supérieur peut ensuite fournir les sous-comptes nécessaires pour organiser les RBAC du nuage en une hiérarchie similaire à celle utilisée pour les groupes dans un service d'annuaire. La structure peut servir à faire respecter la stratégie en fonction des sous-comptes ou des groupes de sous-comptes dans la hiérarchie. Elle peut fournir des fonctions de sécurité de base, comme le contrôle de l'accès, l'authentification et les filtres de trafic.

Dans un compte de niveau supérieur (construction d'un réseau en nuage de base), l'établissement de zones logiques est assuré par le réseau virtuel. Ces réseaux virtuels exigeront des services de sécurité, comme l'appairage de réseaux virtuels et les passerelles réseau, pour ce qui est du filtrage du trafic et du contrôle de l'accès.

Le tableau suivant présente les définitions des fonctions de sécurité associées à un PIZ, tel qu'il est stipulé dans l'ITSP.80.022 [2].

Tableau 2 : Fonctions de sécurité des PIZ

Fonction de sécurité	Description
Contrôle d'accès	Contrôle le trafic en fonction des adresses sources et de destination et le type de service.
Authentification de l'entité	Valide l'authenticité des entités (comptes d'entité, qu'il s'agisse d'une personne ou non) et établit une association de sécurité entre elles.
Authentification de l'origine des données	Valide l'authenticité des entités prenant part à l'association de sécurité.
Vérification de l'intégrité des données	Vérifie que le trafic réseau n'a pas été modifié ou retransmis.
Filtres de trafic	Filtre ou blocage du trafic basé sur des propriétés des flux de données de communication, dont les suivantes : • état du protocole TCP (Transmission Control Protocol); • source et destination, conformité avec les protocoles de communication autorisés; • types de données intégrés aux flux de données de communication; • contenu des flux de données de communication.
Soutien à la détection des intrusions et à la vérification	Fournit les services et les attributs nécessaires pour soutenir la mise en œuvre de fonctions de sécurité comme la détection des intrusions, la vérification et l'intervention en cas d'incident. Comme les FSI fournissent cette capacité dans leur environnement en nuage, elle ne se limite pas au PIZ.
Encapsulation des ressources	Désigne les mécanismes permettant à la zone de masquer sa structure interne. Ces mécanismes comprennent la traduction d'adresses réseau, la traduction d'adresses de port et le mappage des services. L'encapsulation des ressources prend en charge le contrôle de l'accès et la survivance.

Dans un environnement en nuage, il existe plusieurs constructions de sécurité qui répondent à certaines ou à toutes les fonctions et exigences de sécurité. Selon le FSI choisi, on peut s'attendre à ce que les constructions et les capacités varient. Votre organisation doit consulter la documentation technique du FSI. Voici quelques exemples courants de services de sécurité natifs en nuage que l'on peut intégrer aux règles de politique du FSI :

- frontières géographiques;
- authentification multifacteur (AMF);
- emplacements autorisés ou bloqués;
- contrôles de la confiance des partenaires;
- détection avancée des risques liés à l'identité et protection;

- appareils autorisés ou bloqués;
- logiciels autorisés ou bloqués;
- systèmes d'exploitation autorisés ou bloqués;
- points d'entrée définis pour le nuage.

Une instance virtualisée de PIZ ne devrait pas contenir à la fois les PIZ connectés à la ZG et les PIZ des chemins de données Toute instance virtualisée d'un PIZ connecté à la ZG et tout PIZ de chemins de données doit répondre aux exigences d'assurance dérivées de la stratégie de sécurité et du cadre de gestion des risques de votre organisation. Prière de consulter le tableau 1, Mise en correspondance des zones, à la section 2 pour plus de détails sur la ZG et les autres zones.

L'établissement des zones permet de subdiviser un réseau en sous-réseaux ou en zones qui ont les mêmes stratégies et exigences de sécurité. Les organisations doivent mettre en œuvre un zonage de sécurité de réseau pour appliquer leur stratégie de sécurité réseau. Elles pourront ainsi empêcher un auteur de menace de se déplacer latéralement sur le réseau ou de nuire aux activités de tout le réseau. L'établissement de zones regroupe logiquement les données, les logiciels ou le matériel qui font l'objet de stratégies ou d'exigences de sécurité similaires.

Remarque :

Par segmentation réseau, on entend une technique de réseautique qui consiste à diviser un réseau en sous-réseaux plus petits et distincts. Les organisations peuvent ainsi cloisonner les sous-réseaux et mettre en place des contrôles de sécurité et des services uniques à chacun. Les zones de sécurité de réseau sont des regroupements logiques qui sont basés sur la mise en œuvre sous-jacente de la segmentation réseau. Les contrôles de sécurité uniques qui protègent une zone sont définis dans le PIZ.

Les ressources infonuagiques sont déployées dans ces zones précises. Dans un environnement réseau traditionnel, on s'attend à trouver un PIZ à la frontière d'une zone. Dans un environnement en nuage, des capacités supplémentaires font en sorte qu'un PIZ puisse se trouver à la frontière d'une zone ou dans une zone associée à des interfaces réseau de ressources infonuagiques précises, comme une machine virtuelle ou un hôte.

Dans le présent document, un PIZ en périphérie d'une zone sera appelé une liste de contrôle d'accès réseau (NACL pour *Network Access Control List*) et un PIZ dans une zone sera appelé un groupe de sécurité réseau (NSG pour *Network Security Group*). Ces deux types de PIZ sont des constructions natives en nuage. En ce qui concerne le contrôle d'accès réseau, la NACL est considérée sans état, alors que le NSG est avec état.

Dans les déploiements en nuage, nous tenons compte des pare-feu de prochaine génération (NGFW pour *Next Generation Firewall*) natifs en nuage et des pare-feu de tiers qui se trouvent à la frontière d'une zone. Les organisations qui utilisent actuellement un NGFW sur site peuvent choisir de déployer la même solution NGFW au sein de l'infrastructure infonuagique afin de mettre à profit les connaissances opérationnelles, de réutiliser les outils existants et d'assurer une meilleure soutenabilité. Dans le présent document, on suppose que le NGFW peut être configuré de manière à fournir toutes les fonctions de sécurité d'un PIZ. Le NGFW se distingue du pare-feu traditionnel d'un NGFW de diverses façons. Un pare-feu traditionnel permet généralement d'effectuer une inspection dynamique de toute le trafic réseau, alors qu'un NGFW offre des fonctionnalités supplémentaires, comme la prise en compte et le contrôle des applications, la prévention intégrée des intrusions, une protection contre les menaces liées au nuage et le renseignement sur les menaces. Par exemple, un pare-feu d'applications Web (WAF) devrait servir à filtrer le trafic malveillant en direction de l'application et être placé en amont du

serveur Web ou de la ZAR d'applications. Le PIZ d'une ZAR de base de données devrait inclure un dispositif d'audit et de protection de base de données (DAP pour *Database Audit and Protection*) afin de filtrer les requêtes SQL (Structured Query Language) malveillantes et de surveiller les activités de la base de données.

Une tendance générale veut que plusieurs fonctions de sécurité traditionnelles et exigences associées à un PIZ, comme la détection des intrusions, les audits, le contrôle des accès et les filtres de trafic, soient intégrées en mode natif dans la structure informatique du FSI et qu'elles ne soient pas simplement réservées ou associées aux PIZ. Les capacités de gestion des identités et de l'accès du FSI sont intégrées à la structure informatique et offrent une fonction de sécurité en mode natif, comme la détection des intrusions (détection des menaces) et les audits (journaux d'audit). Les fonctions de sécurité, telles l'intégrité de l'origine des données et la vérification de l'intégrité des données, sont aussi intégrées à la structure informatique du FSI dans l'ensemble de l'environnement en nuage.

Prière de consulter l'annexe A pour plus de détails sur la mise en correspondance des objectifs de sécurité des PIZ et les exigences de base en matière de sécurité des PIZ en nuage. L'annexe A contient également des renseignements supplémentaires sur l'utilisation des PIZ en fonction des exigences de sécurité de votre organisation.

4 Conseils sur l'établissement de zones dans le nuage

Cette section présente des conseils sur l'établissement de zones dans le nuage, qui portent sur la zone de gestion, les conteneurs et les API d'applications.

L'établissement de zones dans le nuage doit faire appel à une stratégie globale visant à assurer un accès et une gestion sécurisés des ressources infonuagiques. La segmentation logique permet de mettre en œuvre la stratégie. Elle consiste à utiliser le zonage pour segmenter l'environnement en nuage en zones logiques distinctes, avec la possibilité qu'il soit nécessaire d'avoir recours à une segmentation physique à un niveau supérieur de sensibilité. La gestion infonuagique fait partie du plan de contrôle infonuagique. Elle vise à assurer le provisionnement et à fournir un soutien continu aux ressources du nuage, ce qui comprend la configuration des réseaux virtuels et l'établissement de zones dans ces réseaux. On peut avoir recours à des API pour réaliser les tâches de gestion dans le cadre du plan de contrôle.

La segmentation du réseau en nuage doit faire partie d'une stratégie de défense en profondeur. Prière de consulter le tableau 1, Mise en correspondance des zones, à la section 2 pour obtenir plus de détails sur les différents types de zones. Il convient d'appliquer le principe de droit d'accès minimal afin de réduire la surface d'attaque du nuage et de empêcher les auteurs de menace de se déplacer latéralement vers les autres zones.

Les communications entre les ressources infonuagiques de différentes zones doivent être limitées au trafic autorisé et être négociées par un PIZ, ce qui réduit la surface d'attaque du nuage et la zone de souffle. Une ZAP devrait être désignée comme point d'accès externe pour le trafic réseau en provenance et en direction des ressources infonuagiques. Prière de consulter la section 6, Topologies de connectivité, pour plus de détails sur les topologies qu'il est possible d'utiliser.

4.1 Segmentation

Cette section offre des conseils sur la segmentation des déploiements en nuage, dont l'établissement de zones internes et la connectivité. La segmentation des réseaux de centres de données traditionnels est une technique qui consiste à diviser un réseau en sous-réseaux distincts de plus petite taille. Les organisations peuvent ainsi compartimenter les données, les systèmes et le trafic qui y circule. L'établissement de zones de sécurité dans un réseau permet de réduire le risque associé à un réseau ouvert en segmentant les services d'infrastructure en regroupements logiques assujettis aux mêmes stratégies de sécurité et aux mêmes exigences de sécurité en matière de communication. La segmentation, que l'on appliquait jadis aux centres de données traditionnels, a évolué avec l'adoption grandissante de l'informatique en nuage. Les outils d'automatisation logiciels, comme les outils d'orchestration et les réseaux SDN, peuvent servir à mettre en œuvre une segmentation dans le cadre d'une gestion infonuagique.

La segmentation empêche les auteurs de menace de se déplacer latéralement entre les différentes zones de l'environnement en nuage. Par exemple, la compromission d'une charge de travail par un auteur de menace dans une zone donnée ne peut pas mener à la compromission d'autres charges de travail dans les autres zones de l'environnement en nuage. Il est ainsi possible de réduire la zone de souffle d'une attaque fructueuse dans le nuage.

La zone de souffle est réduite, car des zones plus granulaires sont définies et mises en œuvre. Il convient donc d'en tenir compte dans la stratégie de segmentation de votre organisation. Des ressources de calcul, de réseau et de stockage distinctes doivent être allouées à chaque zone d'un environnement en nuage. En l'occurrence, les plans de contrôle et de données doivent résider dans des zones différentes et des ressources distinctes doivent leur être allouées. Dans le cadre de

la segmentation en nuage, le plan de contrôle doit faire partie d'une ZG, alors que le plan de données doit faire partie d'une ZAR liée aux données ou aux applications.

Dans le cadre d'une stratégie de défense en profondeur, la segmentation sert à restreindre l'accès aux zones infonuagiques internes de la zone publique. Une ZAP devrait être désignée comme point d'accès externe unique pour tous les flux de trafic et ces flux devraient être négociés par un PIZ. Les contrôles relatifs au flux de trafic à l'intérieur d'une zone et entre les zones sont mis en œuvre selon la stratégie de sécurité de votre organisation. Il se peut que la politique de sécurité de votre organisation fasse partie de la conception de la sécurité d'entreprise et des stratégies de sécurité de flux de données de votre organisation.

Il convient de plus d'appliquer le principe de droit d'accès minimal à la segmentation réseau. Les communications de charges de travail à l'intérieur d'une même zone et entre différentes zones doivent se limiter aux flux de trafic et aux chemins autorisés. Il est important d'appliquer ce principe au moment d'accorder les autorisations d'accès réseau aux utilisatrices et utilisateurs avec et sans accès privilégié. Par exemple, ce principe de segmentation s'applique lorsqu'on permet aux utilisatrices et utilisateurs avec accès privilégié d'accéder aux interfaces de gestion sur le plan de contrôle et que l'on permet aux utilisatrices et utilisateurs sans accès privilégié d'accéder aux charges de travail sur le plan des données.

Le réseau SDN permet de procéder à l'abstraction des ressources infonuagique et au découplage du plan de contrôle du nuage à partir du plan de données. Il est intégré à l'environnement en nuage et est invisible aux utilisatrices et utilisateurs, peu importe s'ils disposent ou non d'un accès privilégié. Sur le plan de la taille, le plan des données est beaucoup plus gros que le plan de contrôle, souvent par plusieurs ordres de grandeur. Le modèle avec adaptateur peut être utilisé dans le cadre de la segmentation pour gérer les flux de trafic entre deux plans (voir la section 6.7, Modèle avec adaptateur).

4.2 Gestion du nuage

Dans les environnements en nuage, le FSI fournit les services de gestion en mode natif à partir d'un portail SaaS. L'organisation peut ainsi configurer la ZG native en nuage de manière à ce que les paramètres de sécurité de la ZG offrent la posture de sécurité souhaitée.

La ZG traditionnelle est remplacée et intégrée à la structure informatique du FSI. De plus, les risques liés à l'utilisation d'une ZG sont atténués par des contrôles de sécurité généralement offerts par le FSI. Votre organisation devra donc configurer les contrôles de sécurité de façon à assurer la posture de sécurité souhaitée. Le fait d'accéder aux tâches de gestion par l'entremise d'une ressource du nuage permet de réduire davantage la surface d'attaque et la zone de souffre, ce qui n'est pas le cas lorsqu'on utilise une ZG pour accéder à toutes les ressources en nuage à partir d'une zone particulière.

Selon la tendance actuelle, l'accès à la gestion n'est pas fourni à partir des points terminaux publics et des ports de gestion traditionnels, ce qui permet, dans une certaine mesure, de garder l'environnement en nuage hors de la mire des auteurs de menace. À la place, une connectivité sécurisée est d'abord établie dans l'environnement du FSI vers le point terminal de gestion autorisé. Ce dernier peut alors faire appel à la connectivité réseau sécurisée précédemment établie pour exécuter des tâches de gestion sur une ressource du nuage en particulier. Il s'agit de la procédure recommandée dans un environnement en nuage.

Il est également recommandé d'avoir recours à une solution d'identité et d'accès privilégié pour sécuriser les comptes de gestion servant à la réalisation de tâches privilégiées. La solution devrait être sécurisée en ayant recours, par exemple, à l'authentification multifacteur.

4.3 Conteneurs

Dans une architecture d'applications à trois niveaux traditionnelle, une application est divisée en fonction des niveaux suivants : Web, application et base de données. Chaque niveau dispose de ses propres ressources de calcul, de réseau et de stockage dans chacune des zones distinctes. Prière de consulter l'ITSG-38 [3] pour des conseils supplémentaires.

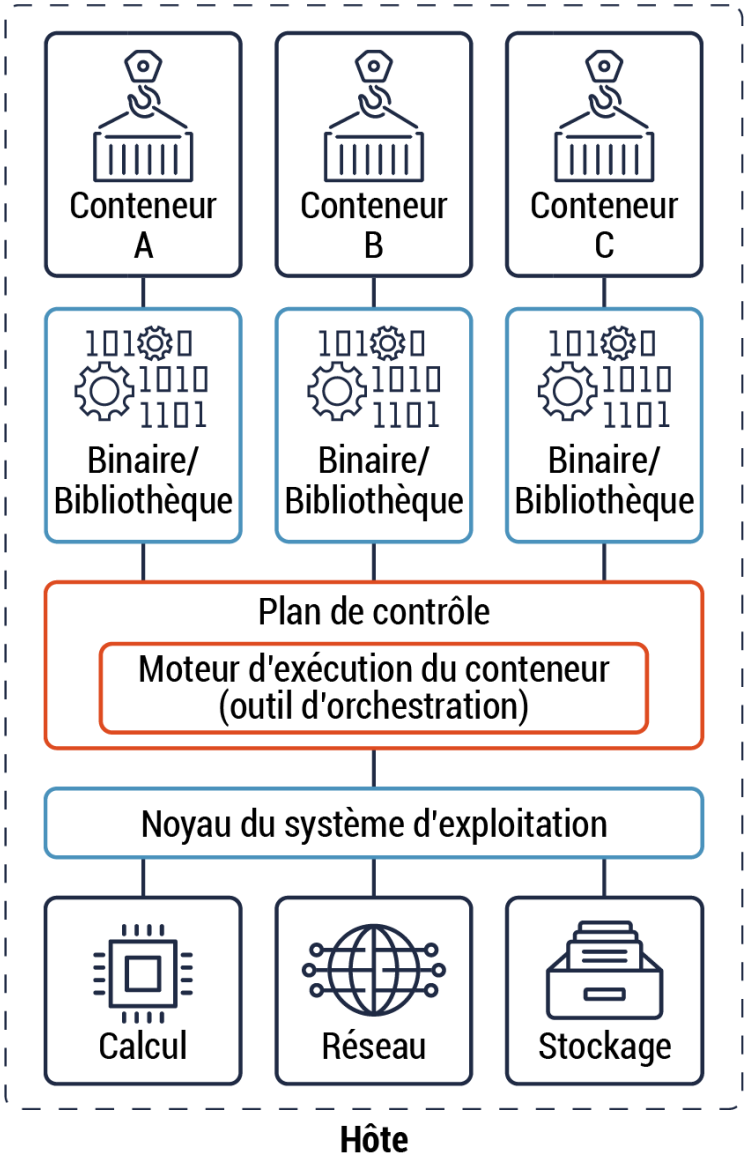
Dans une architecture avec microservices, une application est divisée en plusieurs sous-composants. Chaque sous-composant comporte généralement une seule fonction bien définie, qui consiste en un processus unique exécuté dans un conteneur dédié et séparé. Un processus exécuté dans un conteneur unique permet d'assurer l'isolation du processus. Par défaut, les flux de trafic entre les conteneurs ne sont pas restreints. Des conseils sur la façon de restreindre ces flux de trafic seront fournis dans la présente section.

Une des différences importantes entre les conteneurs et les machines virtuelles est que les premiers sont constitués d'un processus unique, vraisemblablement exécutés sur une machine virtuelle, alors que les seconds exécutent une application et ses dépendances (le cas échéant). En l'occurrence, un ou plusieurs conteneurs peuvent être exécutés sur une seule machine virtuelle ou dans le noyau d'un seul système d'exploitation (SE). Un conteneur qui contient des données dont le niveau de classification est élevé peut, par exemple, s'exécuter sur une machine virtuelle dédiée lorsque les zones sont établies adéquatement et que d'autres contrôles de sécurité appropriés sont mis en place, alors que plusieurs conteneurs avec des données dont le niveau de classification est peu élevé peuvent résider dans le noyau d'un système d'exploitation.

Les conteneurs isolent le noyau du SE et les ressources matérielles. Ils disposent de la logique applicative, des configurations et des dépendances nécessaires pour permettre leur exécution.

Le diagramme ci-dessous (figure 1) illustre trois conteneurs, leurs dépendances et le plan de contrôle.

Figure 1 : Conteneurs



Les conteneurs servant à différentes fonctions doivent être répartis dans différentes ZAR en fonction de la classification et du niveau de sensibilité des données. Par exemple, les conteneurs qui hébergent une application et une base de données faisant partie intégrante d'une solution devraient être placés dans des ZAR différentes. Il est important de souligner que le présent guide ne permet pas d'assurer une sécurité à plusieurs niveaux. Un outil d'orchestration de conteneurs peut être utilisé pour gérer le déploiement des conteneurs et s'assurer que le principe de droit d'accès minimal est appliqué aux flux des trafics entrant et sortant entre les conteneurs. Considéré comme faisant partie du plan de contrôle infonuagique, cet outil sert également, en pareil cas, à renforcer les zones ayant été établies. Prière de consulter la figure 21 à l'annexe D pour une représentation de la relation entre les plans de contrôle et de données.

Le principe de droit d'accès minimal devrait être appliqué aux flux de trafic entre les conteneurs d'un même noyau, d'une même zone réseau et de zones différentes. Par défaut, une règle explicite interdisant tout trafic devrait être mise en place et

l'accès devrait être accordé en fonction des exceptions. Par exemple, les communications connues entre différents conteneurs formant un microservice devraient être autorisées.

Des zones devraient être établies pour restreindre l'accès aux conteneurs et au microservice en utilisant des contrôles d'accès granulaires. Les communications entre les conteneurs d'une même zone (ne faisant pas partie d'un même microservice) ou de zones différentes devraient être restreintes et n'autoriser que celles qui sont nécessaires. Prière de consulter la section 4.5 pour plus de détails sur le contrôle d'accès granulaire.

Il est important d'établir des zones pour les flux des trafics entrant et sortant. Il convient de limiter ces deux types de trafic en utilisant les mécanismes appropriés, comme des PIZ pour l'application des zones.

Voici trois (3) cas d'utilisation qui surviennent dans la segmentation et le zonage en conteneurs :

1. Les conteneurs devraient être segmentés en fonction de leur contexte de sécurité relatif pour veiller à ce qu'un noyau système particulier ne puisse exécuter que des conteneurs ayant le même niveau de sensibilité des données et les mêmes fonctionnalités. Par exemple, les conteneurs qui constituent un microservice unique peuvent partager les mêmes ressources de calcul, de réseau et de stockage.
2. Les conteneurs avec des fonctionnalités différentes, mais partageant un même contexte de sécurité ou une même classification de données, doivent être isolés. Dans un tel cas, les différents conteneurs devraient être regroupés dans la même zone et segmentés les uns des autres en leur allouant des ressources différentes. Par exemple, les applications publiques et internes devraient être placées dans des réseaux virtuels différents, et les communications entre les deux réseaux devraient s'effectuer à partir d'un petit nombre d'interfaces bien définies selon la stratégie de sécurité de votre organisation.
3. Vous devriez séparer les conteneurs ayant des classifications de données différentes dans des zones distinctes et utiliser des ressources de calcul, de réseau et de stockage différentes. Les conteneurs dont le niveau de classification des données est plus élevé devraient être placés dans des ZAR différentes avec des ressources différentes, comparativement aux conteneurs dont le niveau de classification des données est inférieur. Par exemple, vous pouvez utiliser un outil d'orchestration pour isoler des conteneurs dans des ensembles d'hôtes en fonction du niveau de sensibilité.

Dans la plupart des cas, vous pouvez définir des règles qui empêchent les charges de travail hautement sensibles de votre organisation de se trouver sur un hôte dont le niveau de sensibilité est inférieur. Il est possible de le faire en mettant en place des grappes distinctes et gérées individuellement pour chaque niveau de sensibilité. Vous pouvez également utiliser un outil d'orchestration pour « associer » un conteneur à un hôte, lorsque celui-ci est affecté à un hôte particulier. Il convient de savoir que l'« association » à un hôte fera en sorte de rendre le conteneur indisponible si l'hôte est aussi indisponible.

Les cas d'utilisation des conteneurs sont en constante évolution. Par exemple, le déploiement d'une base de données conteneurisée est un cas d'utilisation qui n'est pas encore tout à fait au point. Dans certains exemples particuliers, il s'agit toutefois d'une pratique acceptable. Par exemple, cette pratique peut être utilisée dans les environnements en nuage hors production, comme les environnements de tests et de développement. Dans tous les cas d'utilisation, il est nécessaire d'adopter des principes d'établissement de zones rigoureux, comme l'utilisation de conteneurs dans des ZAR de données.

4.4 Interface de programmation d'applications (API)

Le passage à un environnement en nuage et, plus particulièrement, à une architecture de microservices, fait en sorte que les microservices communiquent par l'intermédiaire d'interfaces de programmation d'applications (API pour *Application Programming Interface*) bien définies. La plupart, voire la totalité des composants logiciels des environnements en nuage offerts par les FSI sont basés sur des API. Ces dernières font partie des outils d'automatisation du nuage, comme les outils d'orchestration et les réseaux SDN. Vous pouvez utiliser des API pour exposer vos données et services organisationnels à des entités et à des utilisatrices et utilisateurs externes. De plus, l'accès aux API doit être sécurisé et restreint à des zones et à des charges de travail particulières.

Au sein d'un environnement en nuage, les API peuvent être déployées dans différentes zones du réseau, selon les exigences opérationnelles de votre organisation. Par exemple, des API peuvent être déployées comme services en périphérie dans la ZAP, le plan de contrôle infonuagique et le plan de données d'un environnement en nuage. Les API peuvent également être déployées dans la même zone que le microservice ou sur un réseau sur site. On peut avoir recours à des consoles Web et des outils natifs en nuage pour effectuer des appels d'API en vue de gérer les ressources de l'environnement en nuage et de soumettre des demandes à un microservice. Dans un centre de données traditionnel, les stations de travail sont parfois utilisées pour réaliser, entre autres choses, des tâches administratives sur des serveurs et des plateformes de gestion du matériel.

Vous trouverez ci-dessous quelques cas d'utilisation et de positionnement d'API visant à assurer la segmentation :

1. Les API peuvent servir à négocier les flux de trafic entre le plan de contrôle, le plan de données et l'application dorsale, comme une application patrimoniale ou une base de données en fin de vie. Dans un tel cas, l'API doit être placée dans le plan de données, aussi près que possible de la charge de travail. Prière de consulter la section 6.6, Modèle avec conteneur, pour plus de détails.
2. Les API peuvent servir à négocier les flux de trafic entre l'environnement en nuage et un réseau sur site ou la zone publique. L'API est placée dans la ZAP de l'environnement en nuage dans le cadre des services en périphérie. Il s'agit du seul point d'entrée des microservices pour toutes les demandes qui proviennent de sources externes. Prière de consulter la section 6.9, Modèle avec API, pour plus de détails.
3. Les API servent à réaliser les tâches de gestion dans le cadre du plan de contrôle. Par exemple, les utilisatrices et utilisateurs avec accès privilégié utilisent une API pour gérer les ressources de calcul, de réseau et de stockage. Prière de consulter la section 6.9.1, Modèle avec passerelle d'API, pour plus de détails.
4. Vous pouvez utiliser des API pour fournir une connectivité réseau au plan de données et une connectivité entre des composants différents sur ce plan. Par exemple, une API, en tant que mandataire, peut fournir la connectivité entre des microservices de la ZAR d'application et donner l'état opérationnel du plan de contrôle. Prière de consulter la section 6.6.2, Modèle ambassadeur, pour plus de détails.

En outre, les API peuvent être utilisées pour mettre en œuvre la stratégie de sécurité de l'organisation. Par exemple, l'API d'une stratégie de contrôle d'accès peut être utilisée afin de restreindre l'accès aux microservices. Dans un tel cas, l'API de la stratégie permet d'appliquer le contrôle d'accès aux flux des trafics entrant et sortant des microservices. Pour ce qui est du trafic entrant, l'API restreint les flux de trafic à l'intérieur du conteneur. Quant au trafic sortant, l'API est déployée en périphérie de l'environnement en nuage pour appliquer un contrôle d'accès en fonction des demandes de client. Prière de consulter la section 6.6, Modèle avec conteneur, pour plus de détails sur le contrôle d'accès du trafic entrant. On peut

également consulter la section 6.6.2, Modèle ambassadeur, et la section 6.9.1, Modèle avec passerelle d'API, pour plus de détails sur le contrôle d'accès du trafic sortant.

4.5 Contrôle de l'accès

L'accès aux microservices et aux API doit être restreint aux ressources, aux utilisatrices et aux utilisateurs autorisés au moyen de contrôles d'accès très précis. Les exemples de ces contrôles d'accès comprennent le recours à la segmentation, à l'authentification et à l'autorisation. Toutes les communications au sein d'une zone et entre les zones doivent être sécurisées au moyen du protocole TLS 1.2 ou une version plus récente, conformément aux directives du Centre pour la cybersécurité.

Pour sécuriser le trafic entrant entre les microservices, il convient d'utiliser l'authentification de l'entité homologue et l'authentification de demandes. L'authentification de l'entité homologue sert à assurer l'authentification entre services et à confirmer que le client a bien établi une connexion. Le client et le serveur doivent utiliser une certification TLS pour s'identifier entre eux. Ce faisant, il est également possible de protéger les communications entre les deux parties en assurant la confidentialité et l'intégrité des données. L'authentification de demandes vise à vérifier les justificatifs d'identité associés à la demande. On l'utilise lorsqu'une demande est soumise à partir du client sur le serveur au nom d'une utilisatrice finale ou d'un utilisateur final.

Toutes les demandes de service doivent être authentifiées et autorisées avant d'accorder un accès. Il convient d'utiliser des clés d'API et des normes ouvertes, comme Open Authorization 2.0 (OAuth 2.0), pour sécuriser les demandes de service. Les clés d'API devraient être stockées de manière sécurisée et leur accès devrait être restreint. Prière de consulter la *Normes du gouvernement du Canada sur les API* [9] du SCT pour plus de détails sur la façon de sécuriser les API et les services infonuagiques. Pour de plus amples renseignements, consultez l'ITSP.40.062, *Conseils sur la configuration sécurisée des protocoles réseau* [10].

5 Conseils sur la périphérie et le périmètre du nuage

L'environnement en nuage est en train de transformer la définition traditionnelle et le rôle joué par la périphérie de réseau ou le périmètre. Il est plus décentralisé et, par extension, sa périphérie est également plus décentralisée. Par exemple, l'environnement en nuage présente plusieurs points terminaux publics associés à différents services IaaS et PaaS du FSI. On retrouve généralement plusieurs points terminaux privés qui permettent d'utiliser les services infonuagiques dans un réseau virtuel, tout en continuant d'adhérer aux principes d'établissement de zones de réseau.

Pour cette raison, la sécurisation de la périphérie ou du périmètre d'un environnement en nuage peut poser plusieurs défis et il est d'autant plus important d'établir les zones pour ce qui est des flux des trafics entrant et sortant. Ces deux types de trafic devraient être limités au moyen de mécanismes appropriés, comme des PIZ, de manière à renforcer l'établissement des zones. En outre, il est possible de tirer avantage des outils d'orchestration de conteneurs et de la technologie de réseau virtuel pour assurer l'application des stratégies de sécurité d'un ministère pour les deux flux de trafic.

Selon la topologie de connectivité utilisée, le FSI gérera la périphérie du nuage. D'autres intermédiaires (section 6.4), comme les fournisseurs de services de sécurité gérés (FSSG), peuvent également offrir des services de sécurité ou des CASB afin d'étendre davantage la périphérie ou le périmètre.

5.1 Cas d'utilisation et conseils

Dans le nuage, l'environnement est un réseau virtuel en soi. La présente section examinera la façon de tirer avantage des topologies de connectivité et d'étendre un réseau virtuel en l'intégrant à d'autres réseaux virtuels. La section suivante abordera la façon d'utiliser les topologies de connectivité dans un réseau virtuel au moment d'établir les zones du nuage.

Vous trouverez ci-dessous quelques cas d'utilisation et conseils à ce sujet :

- **Cas d'utilisation :** Un autre réseau virtuel dans un même compte de niveau supérieur

  Conseils : En ce qui a trait à la connectivité réseau, il est possible d'intégrer deux réseaux virtuels appartenant au même compte de niveau supérieur de manière à tirer parti des services réseau du FSI, comme l'appairage de réseaux virtuels ou les passerelles réseau. Certains de ces services réseau proposent des fonctions de sécurité pour le filtrage du trafic réseau et le contrôle de l'accès.

  Dans la plupart des cas, ces services réseau ne respectent pas les fonctions et les exigences de sécurité d'un PIZ et devraient être renforcés par l'intégration d'un PIZ. Le PIZ doit être associé à une ZAP sur les deux réseaux virtuels pour les flux des trafics entrant et sortant.

  On conseille de faire appel au modèle de réseau en étoile où chaque réseau virtuel d'application se trouve dans un rayon. Le PIZ peut être mis en œuvre dans chaque réseau virtuel des rayons et le concentrateur peut reposer sur les exigences et les stratégies de sécurité de l'organisation. Prière de consulter la section 6.2, Modèle de réseau en étoile, et la figure 2 : Architecture conceptuelle, pour plus de détails sur le modèle de réseau en étoile.

- **Cas d'utilisation :** Un autre réseau virtuel dans un compte de niveau supérieur différent au sein d'une même région du nuage

Conseils : La plupart des FSI fournissent des services interrégionaux auxquels on peut avoir recours pour intégrer les réseaux virtuels qui se trouvent dans différents comptes de niveau supérieur. Par conséquent, les directives fournies dans le scénario précédent s'appliquent également à ce cas d'utilisation, notamment pour ce qui est de l'utilisation du modèle de réseau en étoile.

- **Cas d'utilisation :** Un autre réseau virtuel dans un compte de niveau supérieur différent au sein d'une région différente du nuage

  Conseils : La plupart des FSI fournissent des services intrarégionaux auxquels on peut avoir recours pour intégrer les réseaux virtuels qui se trouvent dans différents comptes de niveau supérieur de régions différentes. Par conséquent, les directives fournies dans le scénario précédent s'appliquent également à ce cas d'utilisation, notamment pour ce qui est de l'utilisation du modèle de réseau en étoile.

- **Cas d'utilisation :** Un autre réseau virtuel dans un compte de niveau supérieur différent relevant d'un autre FSI

  Conseils : Pour le moment, les FSI n'offrent aucune connectivité réseau aux autres FSI par l'intermédiaire de leur fond de panier. Il ne reste que deux options de réseau : utiliser un réseau avec ZP ou un réseau sur site.

  - Zone publique. Il est possible de faire appel à une connectivité directe, d'Internet à Internet, ou encore à un RPV site à site. Dans ces deux cas d'utilisation, la connexion devrait s'effectuer dans la ZAP. Vous pouvez tirer avantage des conseils formulés à la section 6.2, Modèle de réseau en étoile, et à la section 6.4, Topologie de connectivité intermédiaire, et interrompre la connectivité dans la ZAP du concentrateur qui fait office de PIZ.
  - Sur site. On suppose que l'organisation a établi une connexion réseau dédiée entre son réseau sur site et deux centres de données régionaux du FSI au moyen d'un fournisseur d'accès Internet (FAI). Cette connexion réseau dédiée doit avoir recours à des fonctions de sécurité, comme un RPV IPsec, le chiffrement OSI de couche 2 et le chiffrement TLS. Il s'agit d'un élément de référence. De plus amples recherches sur les protections supplémentaires à ajouter aux systèmes de niveau supérieur pourraient s'avérer nécessaires. Prière de consulter les conseils formulés à la section 6.3, Topologie de connectivité hybride. Si le même FAI est utilisé pour les deux FSI, il pourrait être possible d'acheminer le trafic réseau directement du FAI, sans avoir d'abord à passer par le site du premier FSI (du nuage au site), puis transmettre le trafic du réseau sur site vers le deuxième FSI (du site au nuage).

- **Cas d'utilisation :** Réseau sur site

  Conseils : On suppose que l'organisation a établi une connexion réseau dédiée entre son réseau sur site et deux centres de données régionaux du FSI au moyen d'un fournisseur d'accès Internet (FAI). Cette connexion réseau dédiée peut utiliser des fonctions de sécurité supplémentaires, comme IPsec, MACsec et le protocole TLS. Prière de consulter les conseils formulés à la section 6.3, Topologie de connectivité hybride.

6 Topologie de connectivité

La présente section traitera des modèles de conception infonuagique liés à la sélection et la mise en œuvre de zones auxquels on fera référence dans les sections subséquentes. Un modèle est une collection de solutions réutilisables et d'idées de conception misant sur l'utilisation des technologies pour résoudre des problèmes de conception de système courants. Il présente un flux de données de bout en bout entre les composants ou les zones d'un système.

Les modèles de conception sont utiles, puisqu'ils proposent des solutions établies à des problèmes de conception courants et sont généralement faciles à répéter. Ils sont organisés dans un format de référence normalisé et permettent d'assurer une cohérence en ce qui a trait à la conception et à la mise en œuvre des systèmes. Leur utilisation ne garantit pas que les problèmes de conception seront toujours résolus, car plusieurs facteurs peuvent entrer en ligne de compte, dont les exigences et les contraintes de sécurité des clients.

Les topologies de connectivité au nuage qui seront examinées dans la présente conviennent à tous les FSI. Les modèles couverts dans la présente section sont documentés, le cas échéant, de la façon suivante :

- Nom et brève description du modèle;
- Brève explication des difficultés pouvant être résolues au moyen de la mise en œuvre du modèle. Il peut s'agir d'une exigence;
- Visualisation de la structure du modèle, dont la solution de conception proposée par le modèle afin de résoudre le problème et de répondre aux exigences;
- Conseils sur la façon dont le modèle peut être appliqué, ce qui comprend les directives, les cas d'utilisation, les avantages et les inconvénients.

La présente section portera sur les modèles suivants :

- Modèle de réseau en étoile;
- Modèle hybride;
- Modèle intermédiaire;
- Modèle avec enclave de données;
- Modèle avec conteneur;
- Modèle avec adaptateur;
- Modèle avec API ou anti-API.

6.1 Présentation conceptuelle

Avant d'aborder les modèles individuels et d'y faire référence, il convient d'examiner les diagrammes ci-dessous, qui offre une présentation conceptuelle de certains des modèles importants et explique comment on peut les utiliser. Prière de consulter l'annexe B pour plus de détails.

Figure 2 : Architecture conceptuelle

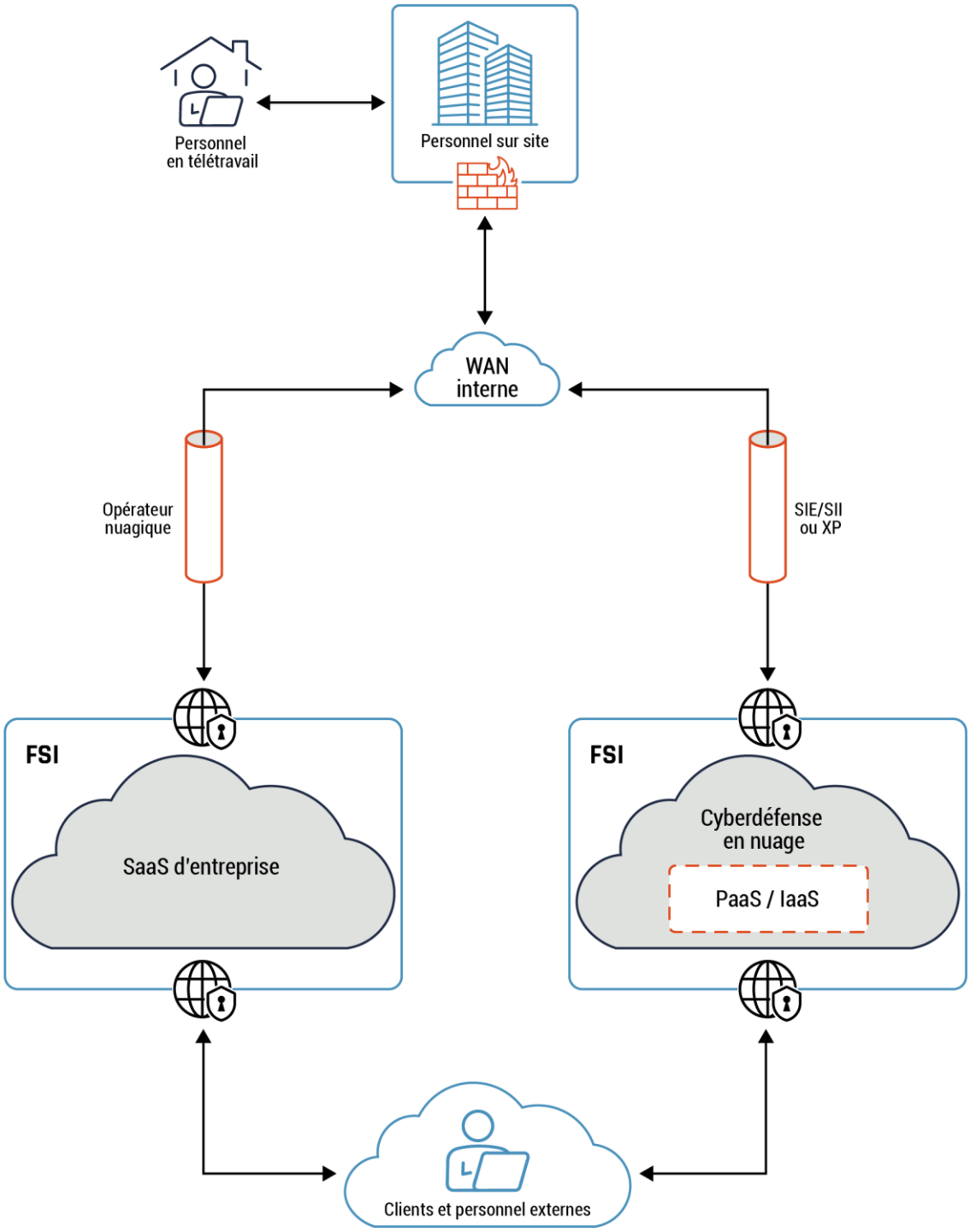
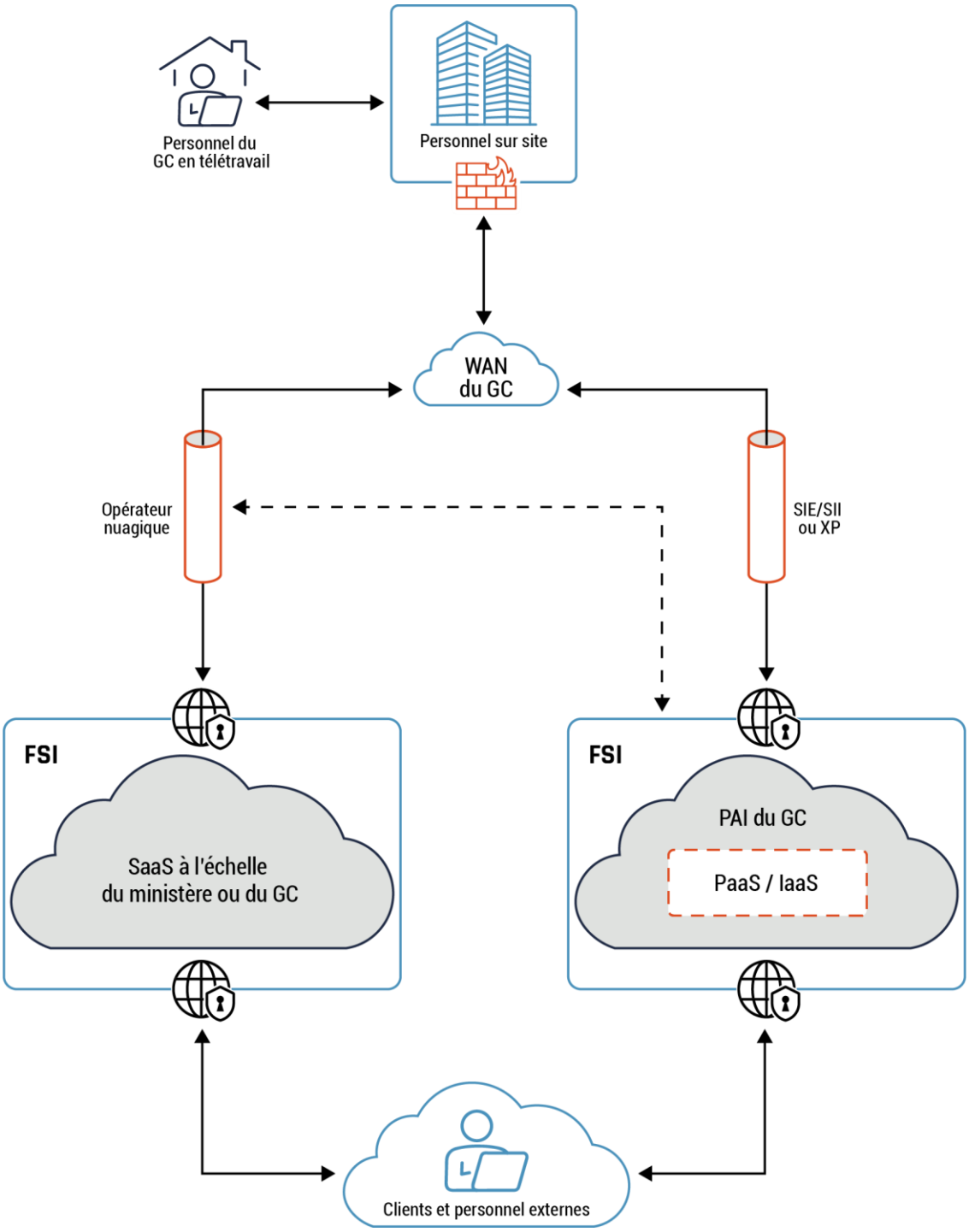


Figure 3 : Architecture conceptuelle dans



La vue de l'architecture conceptuelle offre une perspective de haut niveau de certaines topologies de connectivité clés les plus courantes, comme les réseaux hybrides, intermédiaires et en étoile. Le trafic entrant et sortant de l'environnement en nuage provient des nombreux points terminaux publics du FSI. Un modèle de réseau en étoile est au cœur de l'architecture du réseau et de l'établissement de ses zones. Le concentrateur héberge les services communs ou partagés, comme la surveillance, le routage et l'inspection. Ces services peuvent être consommés par différentes charges de travail hébergées

dans les rayons. De plus, le concentrateur agit à titre d'intermédiaire et inspecte tout le trafic entre la ZP, votre réseau sur site et votre environnement en nuage.

Les charges de travail du nuage de votre organisation sont déployées dans les rayons. Un rayon peut être segmenté en différentes zones, comme les niveaux s'appliquant au Web, aux applications et aux bases de données au sein des groupes de sécurité réseau (NSG) utilisés pour restreindre l'accès.

Vous trouverez ci-dessous quelques avantages découlant de l'utilisation d'un modèle de réseau en étoile :

- Vous pouvez isoler les charges de travail dans les différents rayons. Par exemple, les charges de travail présentant différentes classifications de données doivent se trouver dans des modèles différents et utiliser des ressources différentes.
- Il n'y a qu'un seul point pour le trafic entrant et sortant, le concentrateur, ce qui permet de réduire la surface d'attaque.

Voici ce que vous devez garder à l'esprit lors de la mise en œuvre d'un modèle de réseau en étoile dans votre environnement en nuage :

- Les environnements en nuages ont des implications en matière de coûts, en particulier si des frais sont imputables au trafic rayon-concentrateur-rayon. Par exemple, vous pourriez devoir payer des frais pour les flux des trafics entrant et sortant, notamment dans les cas d'utilisation à fort trafic. Votre organisation peut réduire les frais en faisant preuve d'une diligence raisonnable.

Le trafic peut provenir des installations sur site, où on retrouve un modèle hybride, ou de la ZP, où on retrouve un modèle intermédiaire. Il existe différentes formes d'intermédiaires, comme les FSSG et les CASB. Un bon exemple de FSSG est le service de connectivité hybride du GC. De plus, les services CASB peuvent être utilisés en tant que mandataire inverse pour l'application des stratégies, comme l'authentification, l'authentification unique, l'autorisation et le chiffrement. Prière de consulter le glossaire pour de plus amples renseignements sur les FSSG, les CASB et le service de connectivité hybride du GC.

Dans le contexte du gouvernement du Canada, le service de connectivité hybride du GC intègre un PIZ qui négocie tout le trafic réseau entre les installations sur site et la NACL du nuage. On peut également utiliser le PIZ pour négocier et inspecter tout le trafic réseau depuis la ZP. Certaines capacités du service de connectivité hybride du GC incluent des CASB, des NGFW, le déchiffrement TLS et des inspections approfondies des paquets.

Le modèle de réseau en étoile dans un environnement en nuage a été abordé à la section 5. La section 6 traitera des différents modèles retrouvés dans un réseau virtuel en étoile, comme les modèles avec enclave de données, avec conteneur et avec API.

6.2 Modèle de réseau en étoile

Points essentiels de ce modèle

Le modèle de réseau en étoile permet d'assurer une gestion efficace des exigences de communication et de sécurité courantes. Le concentrateur est une zone de sécurité de réseau qui contrôle et inspecte le trafic entrant ou sortant qui circule entre les zones suivantes : Internet, sur site et rayons. Par exemple, une passerelle RPV peut être déployée à titre de service commun pour fournir une connectivité sécurisée entre votre centre de données sur site et votre environnement en nuage au moyen de ce modèle. Prière de consulter la figure 4 – Topologie de connectivité du réseau en étoile pour plus de détails.

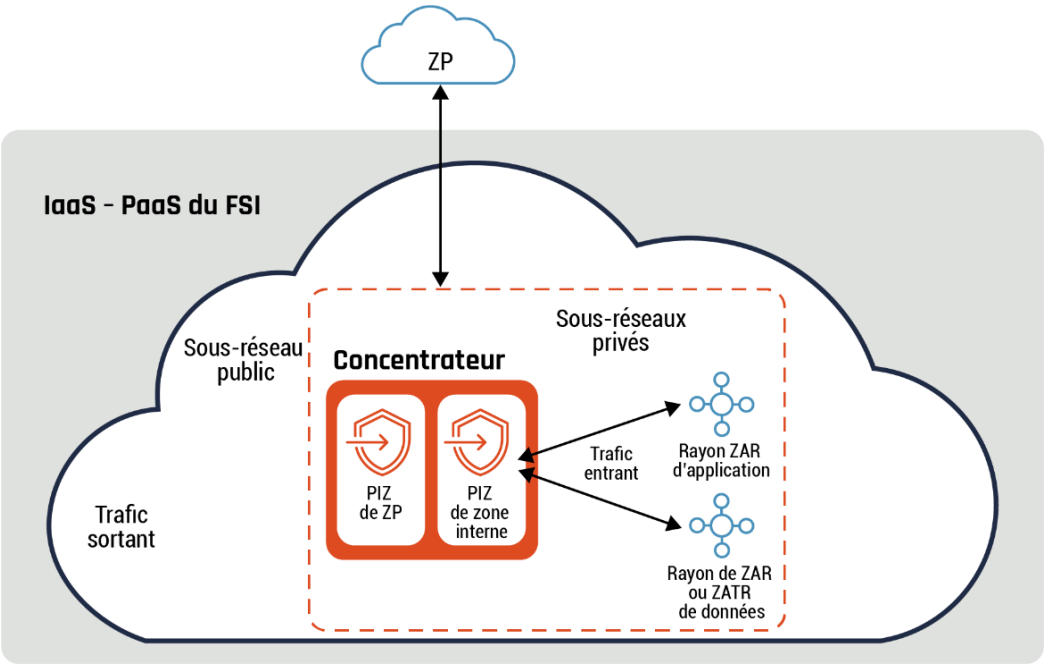
Remarque :

Par défaut, les flux de trafic sont autorisés entre les rayons. Ces flux de trafic dépendent de la stratégie de sécurité et du cadre de gestion des risques de votre organisation. Prière de consulter la section 4 – Conseils sur l'établissement de zones dans le nuage pour plus de détails sur certaines des mesures d'atténuation que l'on peut appliquer à ces flux de trafic.

Le modèle de réseau en étoile propose les avantages suivants à votre organisation :

- Réseau : On peut utiliser le concentrateur pour contrôler le trafic entrant et sortant, ce qui permet d'isoler votre réseau et de réduire la zone de souffle;
- Conformité :
    a. Un nouveau rayon hérite des contrôles et des exigences de sécurité de référence du concentrateur et de l'environnement dans son ensemble;
    b. La séparation des rayons est basée sur des exigences environnementales différentes, comme dans le cas des environnements de production et de non-production, ou de la séparation des secteurs d'activité;
- Extensibilité : Des rayons supplémentaires peuvent être ajoutés facilement, sans incidence sur les rayons actuels. Le FSI pourrait imposer des limites selon votre mise en œuvre, notamment pour l'appairage de réseaux virtuels ou la passerelle réseau.

Figure 4 : Topologie de connectivité du réseau en étoile



Remarque :

L'interface privée du PIZ de la zone interne et le sous-réseau privé du PIZ peuvent se trouver sur les mêmes flux des trafics entrant et sortant ou il peut s'agir d'interfaces privées et de sous-réseaux privés différents. Ce modèle s'applique également à tous les diagrammes présentés jusqu'à la fin du présent document, qui illustrent des flux des trafics entrant et sortant.

Comme l'indique le diagramme précédent, il existe une séparation logique entre les flux des trafics sortant et entrant. Le concentrateur joue ainsi une double fonction sans nécessiter une séparation entre les deux flux; il est composé d'un sous-réseau privé et d'un sous-réseau public. Les rayons sont hébergés sur des sous-réseaux privés.

Conseils

Le PIZ de la ZP devrait être utilisé pour filtrer les paquets selon les caractéristiques définies par votre organisation et ne devrait avoir recours qu'aux services nécessaires pour communiquer avec la ZP. Le ou les PIZ de la zone interne du concentrateur peuvent faire office de PIZ pour les rayons s'ils respectent toutes les fonctions de sécurité et les exigences présentées à l'annexe A. Par exemple, votre organisation peut déployer un pare-feu infonuagique en mode natif, l'appliance NGFW d'une tierce partie ou un équilibreur de charge dans le concentrateur et y intégrer un module de gestion unifiée des menaces (UTM pour *Unified Threat Management*) pour le trafic sortant entre la ZP et le concentrateur.

Dans le cas du trafic entrant, le concentrateur peut servir de PIZ si les rayons ne comportent aucun PIZ. Si un PIZ est intégré à chaque rayon, le concentrateur peut fournir des capacités de routage réseau, dont le contrôle d'accès. Dans un tel cas, toutes les ressources du concentrateur portent la même classification de données et sont gérées concurremment.

Prière de consulter les modèles hybride et intermédiaire pour obtenir des renseignements supplémentaires sur l'intégration de ces modèles.

Vous trouverez ci-dessous trois cas d'utilisations liés au trafic entrant dans un modèle de réseau en étoile selon la stratégie de sécurité et le cadre de gestion des risques de votre organisation :

1. Les rayons d'un même concentrateur peuvent communiquer entre eux par l'intermédiaire du PIZ du concentrateur, ainsi qu'au moyen d'autres contrôles d'accès plus détaillés, ce qui peut servir à restreindre les flux de trafic, le cas échéant. Par exemple, une utilisatrice ou un utilisateur interne a accès à un portail Web qui extrait des données à propos d'un client à partir de sources différentes. Le client possède un compte personnel et un compte d'entreprise, et les données d'applications sont accessibles à partir de différentes interfaces sur des rayons différents. Chaque application a une connectivité directe aux autres applications aux fins de mise à jour, comme la modification du nom d'un client. Prière de consulter la figure 20, Exemples de passerelles d'API, de services API et de conteneurs pour plus de détails;
2. Selon les exigences de sécurité de votre organisation, il ne doit y avoir aucune connectivité directe entre les rayons. Tout le trafic qui transite entre les rayons passe par le concentrateur. Par exemple, les rayons hébergent les charges de travail des environnements de test, de développement, de préproduction et de production de votre organisation. Prière de consulter la figure 17, Exemple de modèle de réseau en étoile à l'annexe C pour plus de détails;
3. Selon les exigences de sécurité de votre organisation, on doit retrouver une connectivité directe et non directe entre les rayons. Par exemple, un des rayons héberge la zone de travail de votre organisation, tandis que les autres hébergent les charges de travail des environnements de test, de développement, de préproduction et de production. Les environnements de production et de préproduction présentent des configurations matérielles et logicielles similaires, à part le fait que le premier soit entièrement redondant (tous les composants sont déployés en paires). La ZT dispose d'une connectivité directe aux quatre environnements et héberge les postes de travail virtuels. Il n'y a toutefois aucune connectivité directe entre les quatre environnements.

   Par exemple, une demande d'assistance est soumise relativement à un bogue rencontré par une utilisatrice ou un utilisateur dans l'environnement de production et est affecté à une développeuse ou un développeur. Le développeur confirmera le bogue en utilisant un ordinateur virtuel dans la ZT pour accéder à l'environnement de production. Il utilisera ensuite l'environnement de préproduction pour déboguer le problème soulevé dans la demande en ouvrant une session d'utilisateur dans la ZT. Prière de consulter la figure 19, Troisième exemple de modèle de réseau en étoile à l'annexe C pour plus de détails.

6.3 Modèle hybride

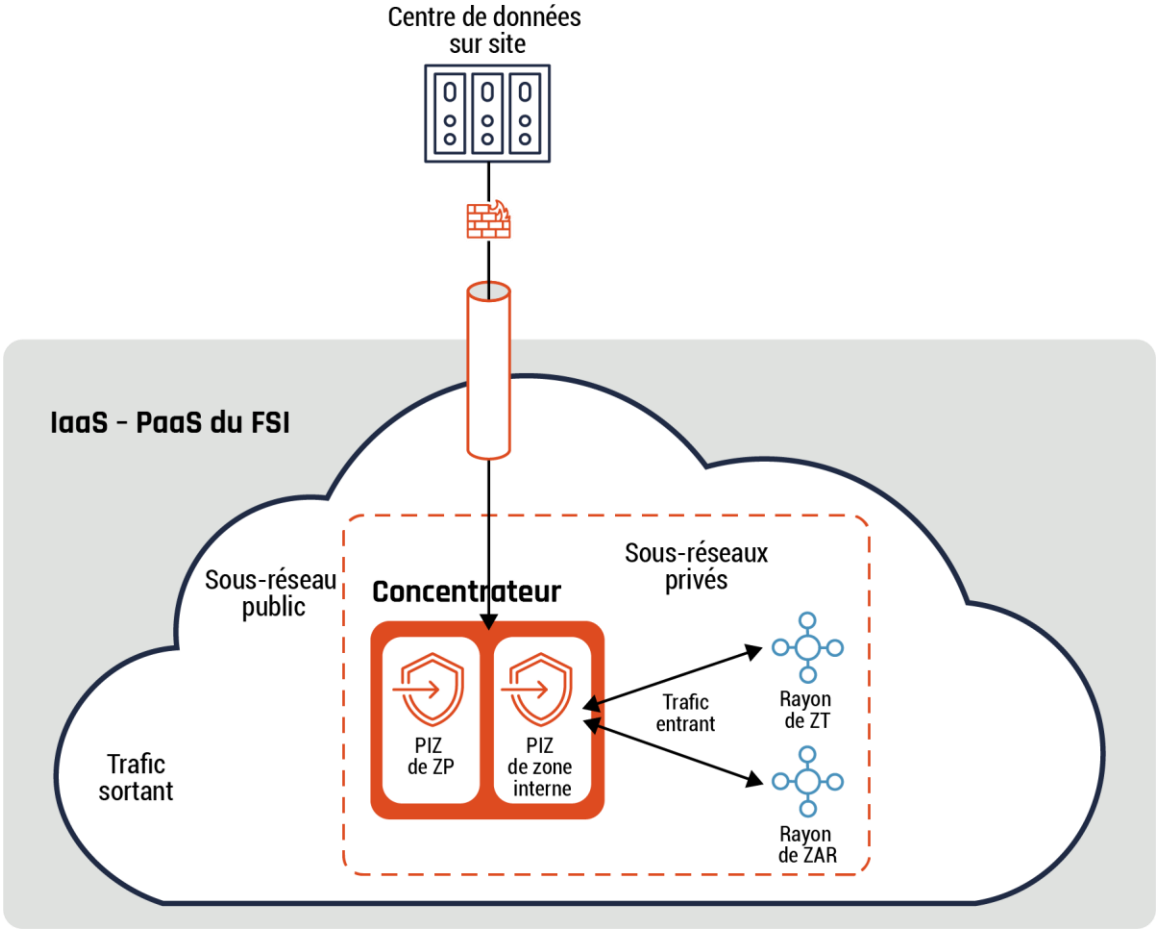
Points essentiels de ce modèle

Le modèle hybride est un modèle de conception réseau permettant de gérer efficacement les exigences de sécurité et les communications entre un concentrateur infonuagique, les charges de travail d'un centre de données sur site et les utilisatrices et utilisateurs. Les systèmes, comme les API, et les utilisatrices ou utilisateurs peuvent accéder aux services nécessaires à partir du réseau sur site de votre organisation ou depuis l'environnement en nuage.

Le modèle hybride propose les avantages suivants à votre organisation :

- Réseau : Permet d'assurer une connectivité réseau entre le centre de données sur site de votre organisation et l'environnement en nuage;
- Conformité : Le trafic réseau passera par un réseau privé dédié;
- Extensibilité : Une bande passante dédiée supplémentaire peut être mise en place en collaboration avec votre FSI et un fournisseur d'accès Internet (FAI) intermédiaire pour ce qui est des communications.

Figure 5 : Topologie de connectivité hybride



Dans le diagramme précédent, une connectivité réseau directe est établie entre le centre de données sur site de votre organisation et l'environnement en nuage.

Tout le trafic qui transite entre le centre de données sur site de votre organisation et l'environnement en nuage doit passer par le PIZ. De plus, le PIZ comprend un mandataire inverse permettant de négocier et de vérifier tout le trafic qui transite entre la ZP et vos charges de travail (hébergées dans votre centre de données sur site et l'environnement en nuage). Selon la stratégie de sécurité de votre organisation, le trafic de la ZP peut être restreint de manière à limiter l'accès aux charges de travail de votre environnement en nuage.

Conseils

Le concentrateur peut faire office de PIZ s'il répond à toutes les fonctions de sécurité et aux exigences mentionnées à l'annexe A. Par exemple, vous pouvez déployer un pare-feu infonuagique en mode natif ou l'appliance NGFW d'une tierce partie dans le concentrateur et y intégrer un module d'UTM pour le trafic réseau sortant entre le concentrateur et le centre de données sur site. Si un PIZ a été mis en œuvre sur un compte de rayon, le concentrateur peut également fournir des capacités de routage réseau, dont le contrôle d'accès.

Le trafic qui transite entre le réseau sur site et le concentrateur devrait être protégé par le protocole IPsec, selon les configurations décrites à l'ITSP.40.062 [10], ou le protocole MACsec, selon les configurations d'algorithmes de chiffrement décrites à l'ITSP.40.111 [11]. À mesure que la sensibilité des données augmente, il peut être nécessaire de faire appel à des capacités supplémentaires comme, par exemple, deux tunnels RPV et des liens dédiés à partir d'un même fournisseur ou de fournisseurs différents. Les deux tunnels RPV servent au chiffrement des données, ce qui offre une meilleure protection et une redondance accrue.

6.4 Modèle intermédiaire

Points essentiels de ce modèle

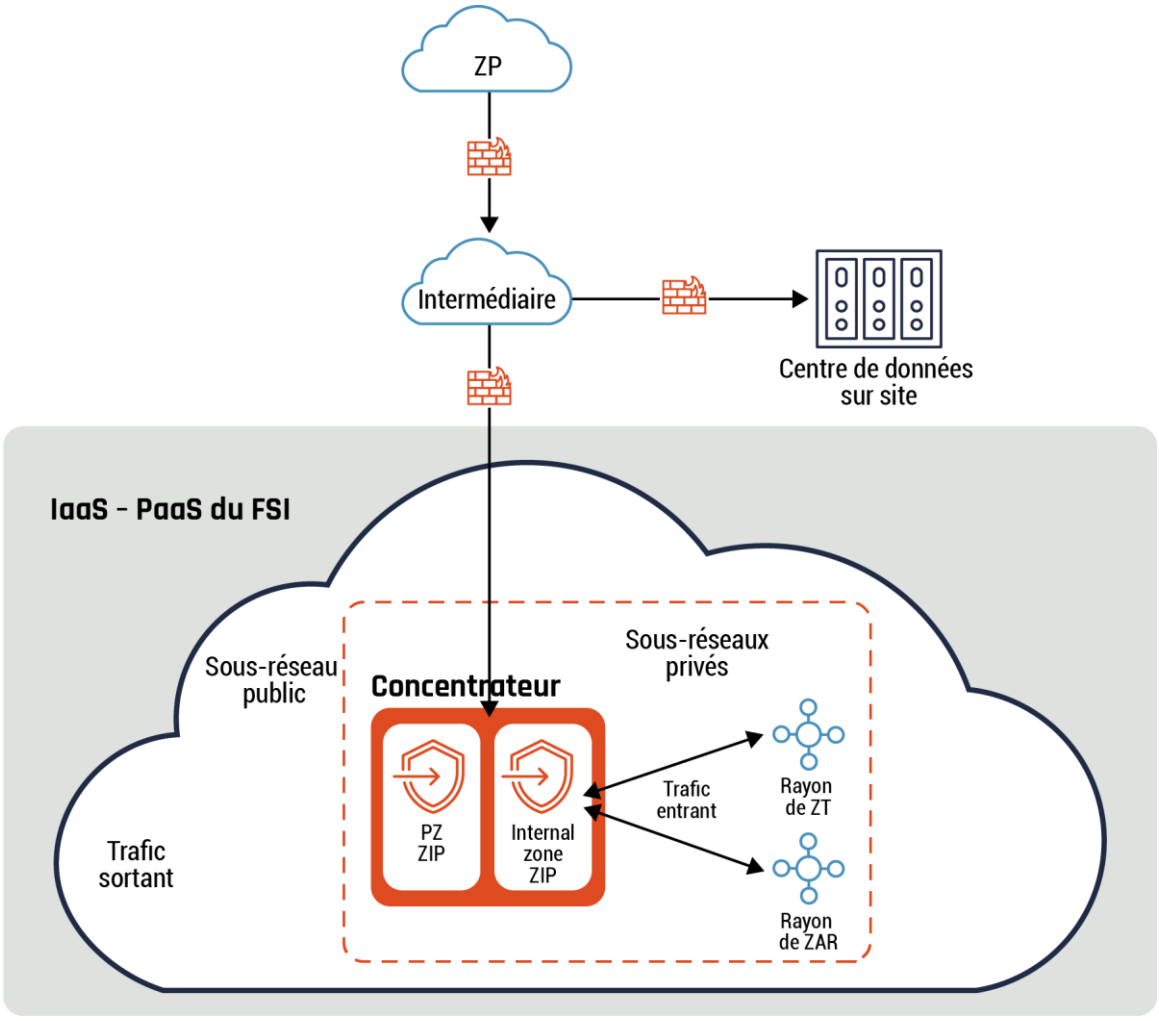
Le modèle intermédiaire est une modèle de conception réseau permettant de gérer efficacement les exigences de sécurité et les communications entre un concentrateur et une ZP, comme Internet ou le concentrateur et le centre de données de votre organisation.

Le modèle intermédiaire peut être mis en œuvre par votre organisation ou un fournisseur tiers. La mise en œuvre peut être effectuée dans l'environnement virtuel du FSI, sur site ou au niveau du FAI de manière à faire partie de la connectivité réseau dédiée privée du FSI.

Le modèle intermédiaire propose les avantages suivants à votre organisation :

- Réseau : Tout le trafic réseau en provenance ou en direction de la ZP doit transiter par un intermédiaire, ce qui permet d'améliorer la gestion de la connectivité réseau avec la ZP;
- Conformité :
    a. Le trafic réseau transite par un PIZ dédié qui répond à toutes les fonctions de sécurité et à toutes les exigences d'un PIZ. Le concentrateur peut ne pas offrir toutes les fonctionnalités d'un PIZ, mais celles manquantes sont prises en charge par le composant intermédiaire. Par exemple, les services courants qui sont consommés par les rayons, comme le NGFW, le système de détection d'intrusion (SDI) et le système d'adressage par domaines (DNS) sont hébergés par le concentrateur. Les services qui doivent être isolés conformément aux exigences de sécurité, comme les services de surveillance et de conformité, sont hébergés sur le composant intermédiaire;
    b. Dans un contexte gouvernemental, ou dans le cas d'une grande entreprise comportant plusieurs secteurs d'activités, l'ensemble du trafic provenant des différents secteurs d'activités passe par le composant intermédiaire. Dans une telle situation, le composant intermédiaire fait office de concentrateur centralisé pour tous les autres concentrateurs des secteurs d'activités;
- Extensibilité : Une bande passante dédiée supplémentaire peut être mise en place en collaboration avec le FSI et un FAI intermédiaire pour ce qui est des communications.

Figure 6 : Topologie de connectivité intermédiaire



Conseils :

Le composant intermédiaire peut fournir les capacités d'un PIZ s'il répond à toutes les fonctions de sécurité et aux exigences mentionnées à l'annexe A. Par exemple, vous pouvez déployer un pare-feu infonuagique en mode natif ou l'appliance NGFW d'une tierce partie dans le composant intermédiaire et y intégrer un module d'UTM pour le trafic sortant entre le composant intermédiaire et le concentrateur.

Une cas d'utilisation courant pourrait prendre la forme d'une organisation qui envoie tout le trafic vers l'environnement en nuage par l'intermédiaire d'un CASB faisant office d'intermédiaire de manière à centraliser la configuration. L'organisation a recours au CASB pour consolider tous les accès vers l'environnement en nuage.

6.5 Modèle avec enclave de données

Points essentiels de ce modèle

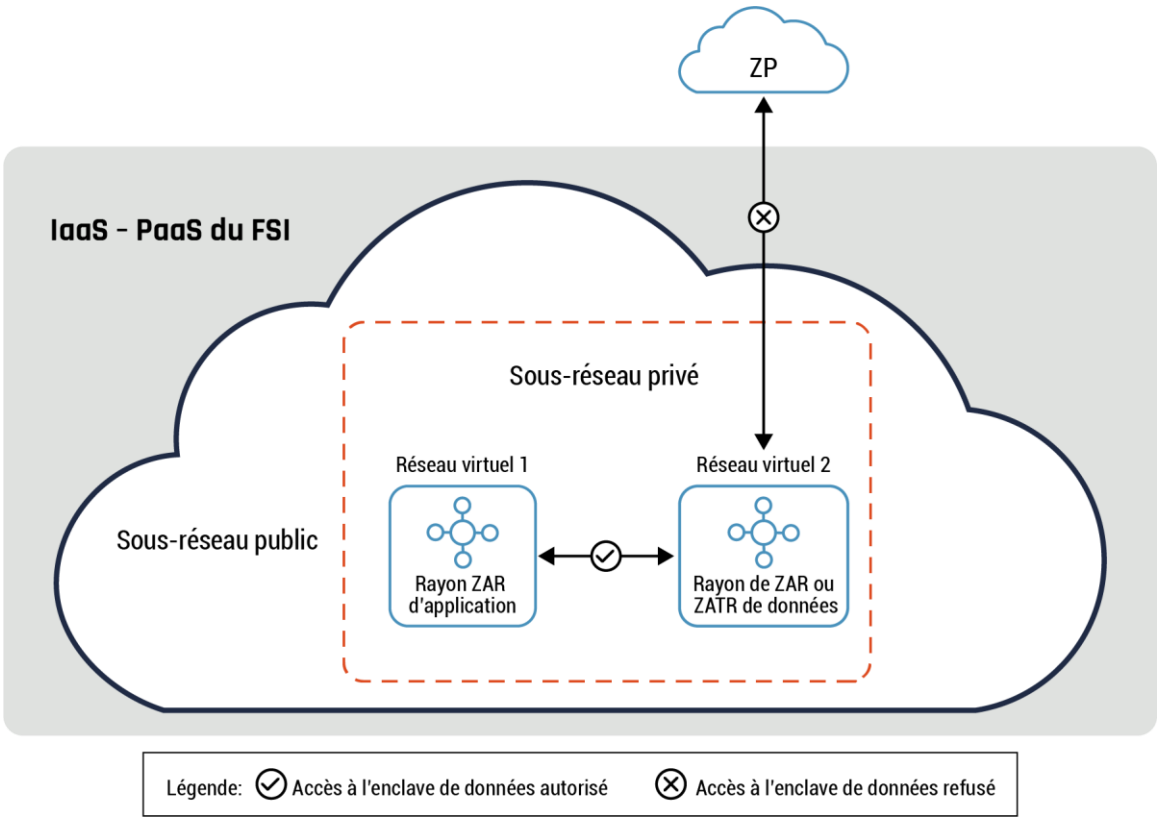
La sécurité des données, et plus particulière l'exfiltration des données, est une des principales préoccupations des organisations. Pour aborder la sécurité des données de façon optimale, il convient de faire appel à un mécanisme de défense en profondeur multicouche auquel il est possible d'intégrer des stratégies de sécurité, la gouvernance, la GIdA, la

sécurité des applications et la gestion des interventions en cas d'incident. Le modèle avec enclave de données fait partie de la couche de sécurité d'application à utiliser dans une ZAR ou une ZATR.

Le modèle avec enclave pour ZAR ou ZATR comportant des données propose les avantages suivants à votre organisation :

- Sécurité du périmètre :
    a. Permet de mettre en place des contrôles du périmètre très précis. On peut atténuer les risques d'exfiltration en isolant les services multilocataires, ce qui fera en sorte d'éviter que des données soient copiées vers des sources non autorisées à l'extérieur du périmètre;
    b. Périmètre de sécurité : On peut contrôler les services des FSI qui sont accessibles à partir d'un réseau virtuel;
- Contrôle de l'accès : Il convient de s'assurer que les données sensibles ne sont accessibles qu'à partir des réseaux virtuels autorisés. Ce modèle offre une couche de sécurité supplémentaire en refusant l'accès aux réseaux non autorisés, et ce, même si les stratégies de GIdA régissant les données sont mal configurées;
- Sensibilité au contexte : On peut restreindre une ressource ou un accès d'utilisateur à des adresses IP autorisées, à des identités particulières et à des dispositifs clients approuvés.

Figure 7 : Topologie de connectivité avec enclave de données



Dans le diagramme précédent, les deux réseaux virtuels peuvent appartenir à un même FSI ou à des FSI différents sans connectivité directe entre eux, à l'exception du sous-réseau public (réseau virtuel 2). Les connexions directes à la ZAR de données ou au sous-réseau de la ZATR ne sont pas permises, sauf par l'intermédiaire du sous-réseau privé. Ce sous-réseau

héberge les API du service infonuagique restreint. De plus, la ZAR de données ou le sous-réseau de la ZATR ne lance aucune demande de service et ne fournit aucune réponse directe à une demande de service, à moins que ça ne soit par l'intermédiaire du sous-réseau privé.

Conseils

Une enclave de données devrait être mise en œuvre dans un réseau virtuel ou un environnement conteneurisé lorsqu'il s'agit d'une ZAR ou d'une ZATR de données. Prière de consulter l'annexe C, figure 18, Deuxième exemple de modèle de réseau en étoile pour plus de détails.

Bien que les NACL et les NSG puissent offrir un certain niveau de protection et être utilisées avec des capacités de sécurité additionnelles, comme l'accès tenant compte du contexte, il pourrait être nécessaire de mettre en place d'autres contrôles d'accès plus précis. Les restrictions relatives aux API du service infonuagique sont un bon exemple de ces contrôles d'accès nécessaires. Prière de consulter la figure 18 – Deuxième exemple de modèle de réseau en étoile et la figure 19 – Troisième exemple de modèle de réseau en étoile à l'annexe C pour plus de détails sur la façon dont on peut utiliser les NSG pour restreindre l'accès entre des zones de sécurité au sein d'un rayon.

Prière de consulter la section 6.6, Modèles avec conteneur, pour de plus amples renseignements sur la façon d'intégrer l'enclave des données à ces modèles.

6.6 Modèles avec conteneur

La présente section traitera de deux modèles : le modèle side-car et le modèle ambassadeur.

Points essentiels de ces modèles

Ces deux modèles avec conteneur sont utiles pour votre organisation pour les raisons suivantes :

1. renforcement de l'isolation des conteneurs;
2. restriction des flux du trafic intraconteneur dans différentes zones de l'environnement en nuage;
3. restriction des flux du trafic interconteneur entre l'environnement en nuage et le réseau sur site ou la ZP.

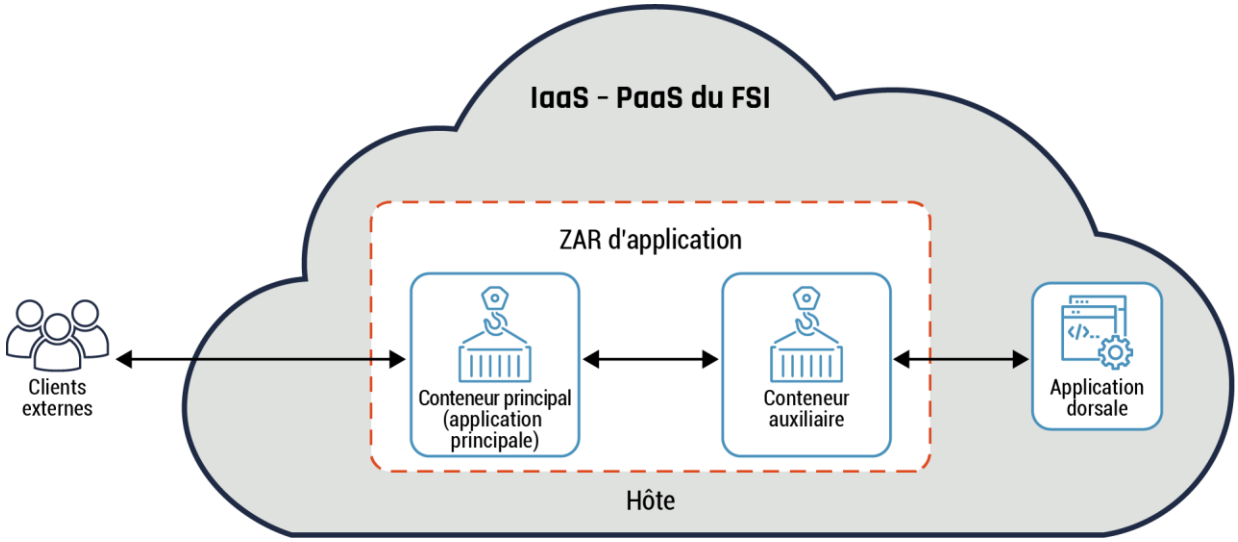
6.6.1 Modèle side-car

Le modèle side-car se compose de deux conteneurs permettant d'assurer l'isolation et la segmentation des processus : le conteneur auxiliaire et le conteneur principal. Le conteneur auxiliaire vise à réduire la complexité du conteneur principal. Les deux conteneurs sont co-situés dans le même noyau du SE et le conteneur auxiliaire connaît le même sort que le conteneur principal (par exemple, au démarrage et à l'arrêt). Le conteneur auxiliaire offre des fonctions courantes, comme la journalisation, la configuration et la synchronisation des fichiers. Ces fonctions sont consommées par d'autres conteneurs.

Ce modèle peut servir à traiter la connectivité des données entre le conteneur principal et les autres conteneurs qui composent le microservice ou les autres composants de la solution. Un exemple d'utilisation de ce modèle est un serveur Web (conteneur principal) offrant du contenu à des clients externes. Le conteneur principal demande au conteneur auxiliaire d'extraire le contenu demandé à partir de la base de données dorsale. Le conteneur auxiliaire extrait le contenu demandé et le renvoie au serveur Web. Le serveur achemine à son tour le contenu extrait au client externe. Prière de consulter la figure 8 ci-dessous pour plus de détails sur le modèle side-car.

Le modèle side-car appartient au plan de données.

Figure 8 : Modèle side-car



Conseils

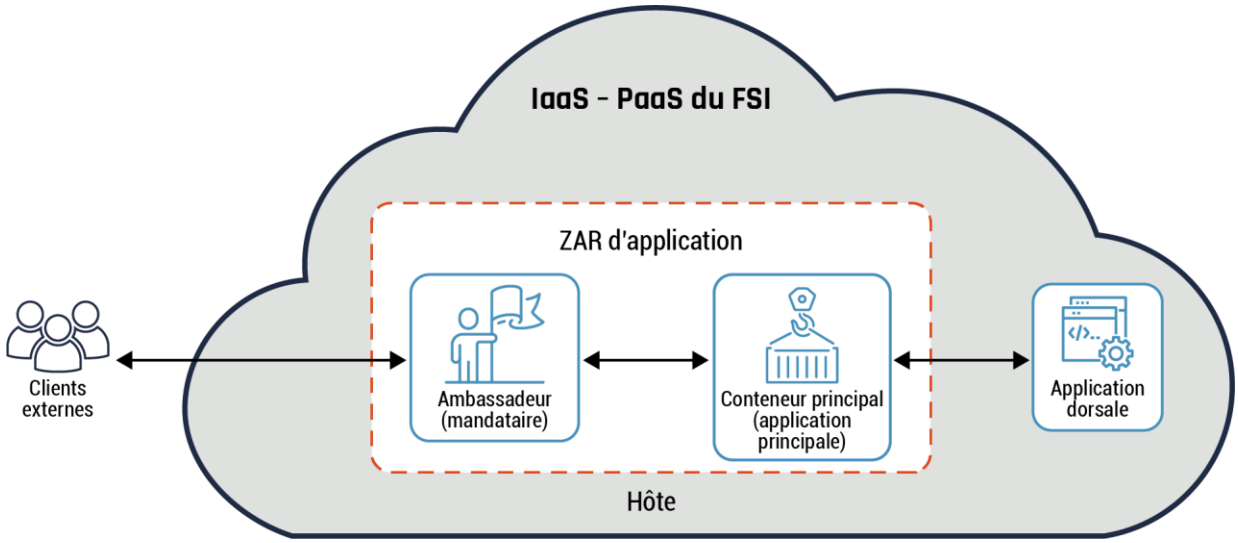
Le modèle side-car peut être mis en œuvre dans l'environnement conteneurisé d'une ZAR d'applications ou de données. L'isolation des processus provient du fait que le conteneur auxiliaire traite à la fois les flux des trafics entrant et sortant pour le conteneur principal dans l'environnement en nuage. Ce modèle est généralement mis en œuvre pour chaque conteneur principal et les conteneurs auxiliaires communiquent entre eux. Le tout est normalement géré au moyen d'un outil d'orchestration de conteneurs faisant partie du plan de contrôle du nuage. Prière de consulter la section 6 et l'annexe D pour plus de détails sur l'outil d'orchestration de conteneurs et le plan de contrôle du nuage.

6.6.2 Modèle ambassadeur

Le modèle ambassadeur permet de gérer la connectivité des données entre le conteneur principal et les composants externes. Le modèle se compose de deux conteneurs co-situés dans le même noyau du SE : un conteneur principal et un conteneur ambassadeur. Le conteneur ambassadeur fait office de mandataire et propose une vue simplifiée du conteneur principal. Il assiste le conteneur principal pour les communications avec les autres zones dans l'environnement en nuage, sur le réseau sur site ou dans la ZP. Ce modèle appartient au plan de données.

Le conteneur ambassadeur peut servir à traiter les tâches de connectivité de client courantes, comme la surveillance, la journalisation, le routage et les requêtes sur la base de données. En règle générale, on utilise ce modèle pour interfacer avec les applications patrimoniales ou en fin de vie.

Figure 9 : Modèle ambassadeur



Dans le diagramme précédent, le conteneur principal est une application Web. Le conteneur ambassadeur traite toutes les demandes de service du conteneur principal et fait office de mandataire de base de données pour les bases de données externes.

Conseils

Le modèle ambassadeur devrait être mis en œuvre dans l'environnement conteneurisé d'une ZAR d'applications ou de données. L'isolation des processus est réalisée au moyen d'un mandataire traitant les flux de trafic pour le conteneur principal. Ce modèle est généralement mis en œuvre lorsque le conteneur principal doit être indépendant de la langue, prendre en charge des applications patrimoniales ou prendre en charge de nombreuses applications et bibliothèques. Cette mise en œuvre peut fournir du soutien aux services dont l'exposition aux menaces est importante. Dans un tel cas, on recommande que des mesures d'atténuation des risques appropriées soient déployées. Prière de consulter la section 4, Conseils sur l'établissement de zones dans le nuage pour plus de détails sur les mesures d'atténuation à utiliser.

6.7 Modèle avec adaptateur

Points essentiels de ce modèle

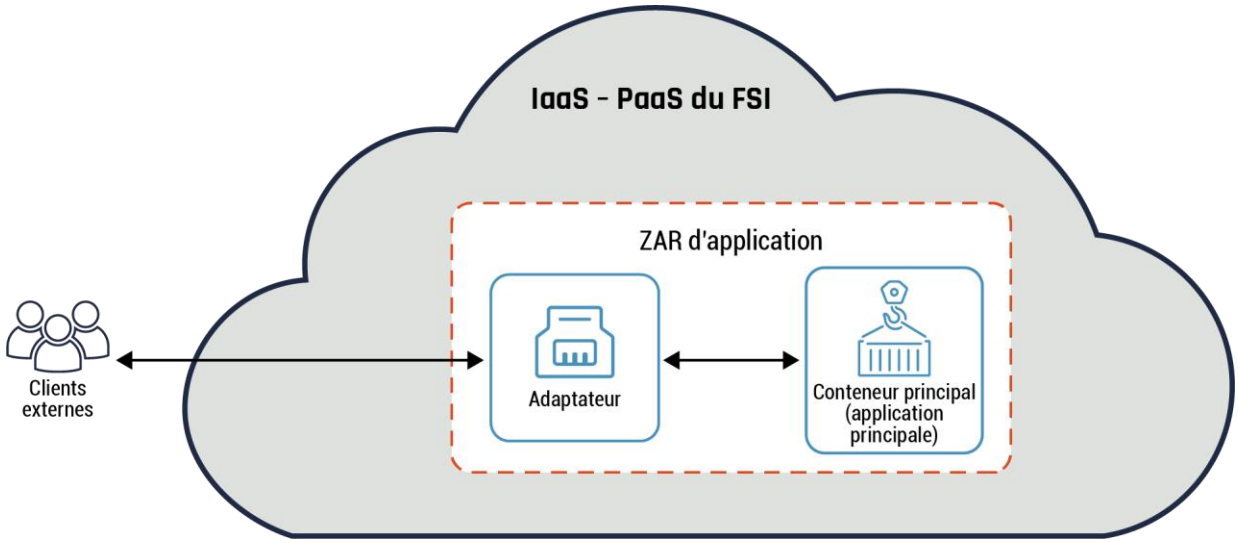
Le modèle avec adaptateur permet de fournir une vue normalisée de l'application aux entités externes. Ce modèle se compose de deux conteneurs : un conteneur principal et un conteneur adaptateur. Le conteneur principal intègre l'application principale, tandis que le conteneur adaptateur traite toutes les demandes de service entre le conteneur principal et les applications externes. Le conteneur adaptateur traite les tâches courantes, comme l'extraction des mesures relatives à l'état opérationnel des composants du plan de données (par exemple, le conteneur principal et la mise en forme des données). Prière de consulter la figure 10 ci-dessous pour plus de détails.

Le modèle avec adaptateur propose les avantages suivants à votre organisation :

- Segmentation des applications externes et de la ZAR d'application ou de données;
- Isolation des processus du conteneur principal par la restriction des accès;

- Restriction du trafic sortant entre le conteneur principal et les applications externes.

Figure 10 : Modèle avec adaptateur



Conseils

Le modèle avec adaptateur devrait être mis en œuvre dans un réseau virtuel ou un environnement conteneurisé. Il est généralement mis en œuvre lorsqu'il est nécessaire de connecter deux composants incompatibles, comme un conteneur principal et un logiciel tiers. Le conteneur adaptateur fournit une interface au moyen de laquelle les deux composants peuvent envoyer des requêtes et recevoir des réponses particulières.

Le conteneur adaptateur peut également servir à traiter des formats de données incompatibles.

Par exemple, le client envoie une requête ne faisant pas appel au protocole HTTP à un microservice qui n'accepte que des requêtes HTTP, version 2. Le conteneur adaptateur procédera à la conversion de protocole afin de permettre la communication entre le client et le microservice. Dans un tel cas, le conteneur adaptateur fait office de passerelle d'API reliant deux composants ou deux fonctions de nature différente. Prière de consulter la section 6.9.1, Modèle avec API – passerelle d'API, pour plus de détails.

6.8 Modèle et antimodèle avec API

La présente section portera sur deux modèles avec API : le modèle avec API et l'antimodèle avec API. On abordera également deux types de modèles avec API : les points terminaux d'API et deux exemples distincts de passerelle d'API. Ces modèles fournit les fonctionnalités nécessaires pour permettre à un client d'accéder à un service et à un service de renvoyer une réponse. Il est à noter qu'il incombe à votre organisation d'assurer la sécurité et la surveillance des API déployées.

Remarque :
Prière de consulter le document Modèles d'architecture axés sur l'IPA pour la PaaS du nuage public [12] du SCT pour plus de détails sur les modèles et antimodèles avec API.

6.9 Modèle avec API : point terminal d'API

Points essentiels de ce modèle

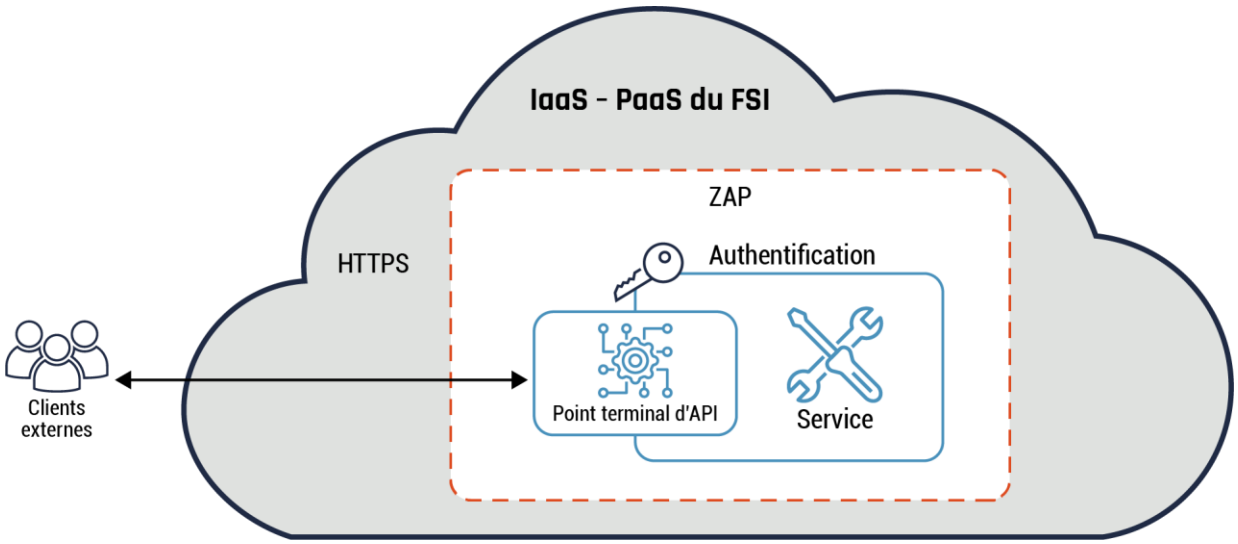
Un microservice doit fournir un ensemble disparate de fonctions à différents clients, comme des appareils mobiles et des stations de travail. Certaines demandes de clients exigent plus de fonctions et de ressources, comparativement à d'autres demandes. Il peut en résulter une surcharge pour le microservice. De plus, un client pourrait devoir soumettre plusieurs demandes avant de pouvoir récupérer toutes les données requises.

La solution consiste à permettre à un point terminal d'API (ou API, pour simplifier) de traiter toutes les demandes de service entre les différents types de clients et le microservice (application principale). Ce modèle, dans sa forme la plus simple, exige que l'on insère une API entre le client et le microservice. L'API peut avoir une ou plusieurs fonctions intégrées. Prière de consulter le diagramme du modèle avec point terminal d'API ci-dessous pour plus de détails.

Le modèle avec point terminal d'API propose les avantages suivants à votre organisation :

- Réduction de la surcharge du microservice – Le microservice permet à l'API de traiter toutes les connectivités de données avec le client. Il offre ses fonctionnalités de base aux clients et décharge toutes les fonctions auxiliaires à l'API;
- Isolation des processus – Il n'y a aucun accès direct au microservice, sauf au moyen de l'API. Il est, de ce fait, isolé;
- Découplage des services courants et de la logique applicative du microservice – Par exemple, les services communs, comme l'authentification, l'autorisation et la facturation, qui sont nécessaires à la gestion des interactions entre le service et le client et qui ne font pas partie de la logique applicative du microservice;
- Contrôle de l'accès – L'API peut servir à appliquer les stratégies de sécurité organisationnelles, comme les fonctions d'authentification et d'autorisation;
- Protection contre les menaces – Permet une protection contre les attaques, comme les injections SQL, les exploits d'analyseur XML (Extensible Markup Language) et les attaques par déni de service (DoS pour *Denial of Service*).

Figure 11 : Modèle avec API



Dans le diagramme ci-dessus, le point terminal d'API peut servir à exposer les fonctions d'accès et de mise à jour des données accessibles au service client. Cette API est accessible depuis la ZP au moyen du protocole HTTPS et offre des services d'identité, comme l'authentification.

Conseils

Le point terminal d'API peut être placé dans la ZAP et servir à réaliser des fonctions en périphérie pour le microservice, comme la passerelle RPV, le routage et la surveillance. L'API peut être utilisée dans des scénarios uniformisés, comme offrir une fonction particulière. Par exemple, l'API peut servir au déchiffrement TLS d'une demande de service.

6.9.1 Modèle avec API : passerelle d'API

La passerelle d'API est un modèle plus complexe que le modèle d'API. On peut y avoir recours pour traiter les cas d'utilisation qui nécessitent un ensemble varié de fonctions, comme l'autorisation, l'authentification, le routage, la surveillance et la facturation. De façon similaire à une API, une passerelle d'API fait office d'intermédiaire entre le client et le microservice. La passerelle d'API peut également servir de mandataire inverse. Prière de consulter la figure 11, Modèle avec API, ci-dessus pour plus de détails.

La passerelle d'API permet de résoudre des problèmes similaires à un modèle d'API. Elle permet également de résoudre les problèmes suivants :

1. Transformation de demande et de réponse. Par exemple, une passerelle d'API peut modifier la demande entrante et y ajouter des paramètres de chemin d'accès avant de la transmettre au microservice. De plus, la passerelle peut modifier la réponse du microservice avant de la transmettre au client, comme le ferait une passerelle, et y ajouter un message d'erreur plus générique en cas d'erreur plutôt que le message de débogage détaillé du microservice.
2. Contrôle du trafic. Une passerelle d'API peut servir à gérer le trafic vers le microservice, comme l'équilibrage de charge.

Deux mises en œuvre de passerelle d'API seront prises en considération dans la présente : la mise en œuvre monolithique et la mise en œuvre spécialisée. Certains cas d'utilisation exigent le déploiement de différentes API dans la passerelle d'API. Par exemple, une entreprise offre une application à partir d'une ZP à laquelle on peut accéder au moyen d'appareils mobiles, d'ordinateurs et d'applications utilisant des API (connexions de système à système). Dans un tel scénario, il est plus efficace d'utiliser une API spécialisée constituée de trois API que d'avoir recours à une passerelle d'API monolithique.

Voici certains problèmes traités par les passerelles d'API **spécialisées** :

- Scénarios uniformisés pour les passerelles d'API monolithiques – Il est plus difficile de procéder à la maintenance informatique d'une passerelle d'API monolithique, car celle-ci présente de nombreuses fonctionnalités différentes pour les divers ensembles de services offerts. Par exemple, il est beaucoup plus facile de mettre à jour une API unique dans une API spécialisée que de mettre à jour une API monolithique;
- Efficacité et performance de l'API – Chaque API de la passerelle d'API spécialisée fournit une fonctionnalité particulière. En revanche, une passerelle d'API monolithique n'est pas optimisée à des fins d'efficacité et de performance.

Figure 12 : Modèle avec passerelle d'API monolithique

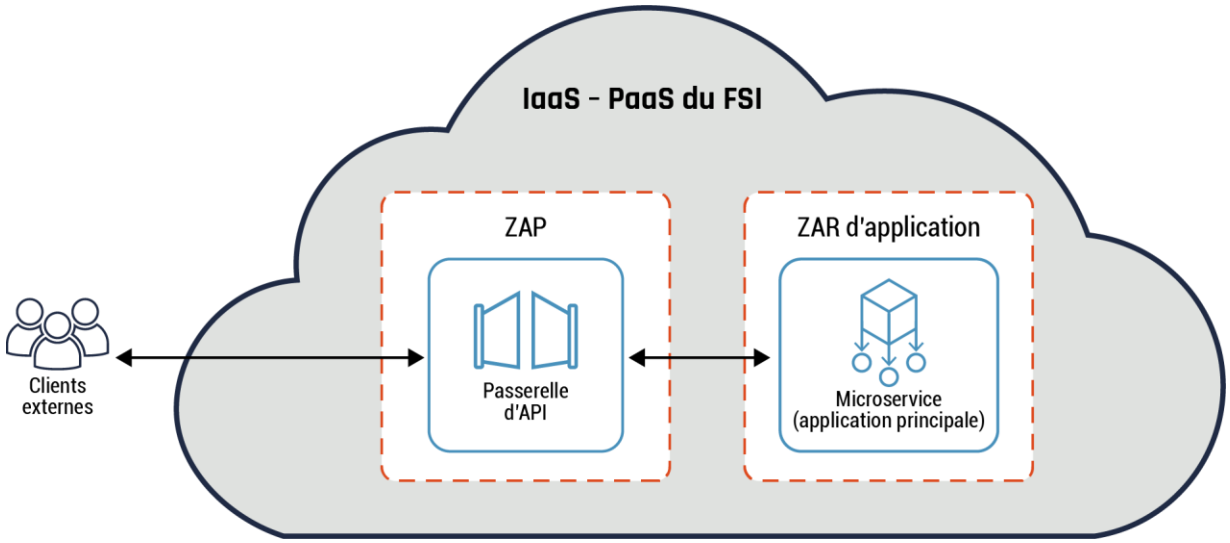
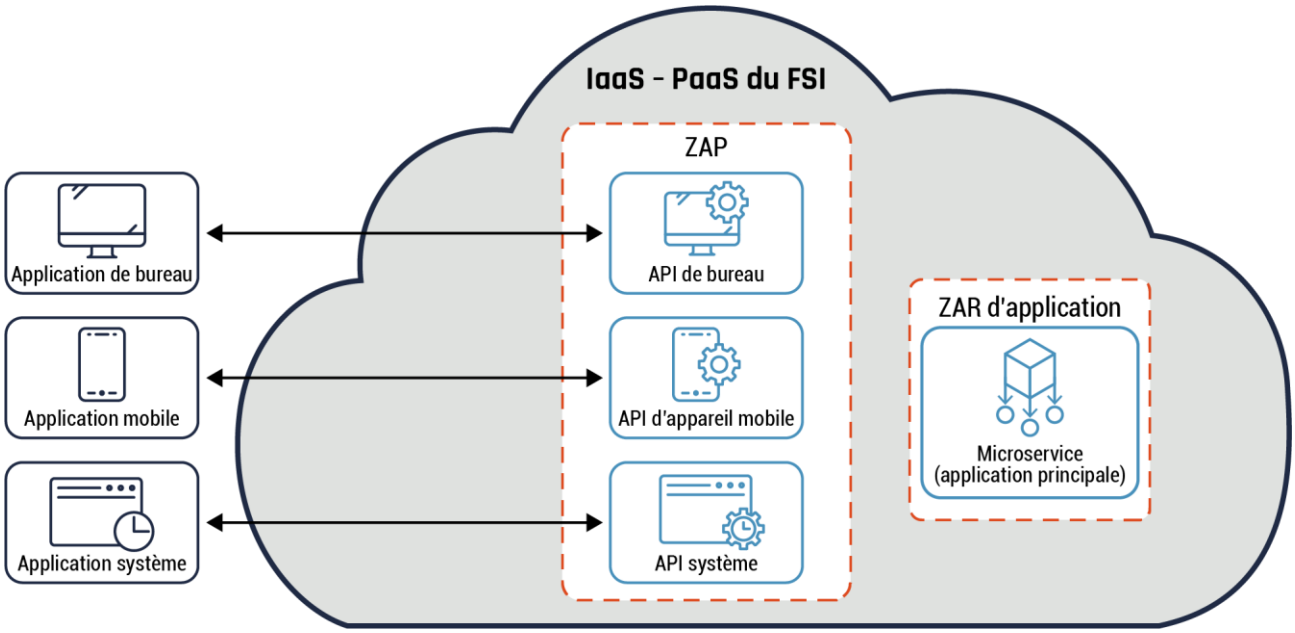


Figure 13 : Modèle avec passerelle d'API spécialisée



Conseils

Contrairement à un point terminal d'API, les passerelles d'API monolithiques et spécialisées peuvent être placées dans la ZAP et être utilisées pour exécuter des fonctions en périphérie, comme la vérification du trafic sortant pour le microservice. Par exemple, une passerelle d'API peut servir à exposer de façon sélective les microservices en tant qu'API aux applications client, à vérifier toutes les demandes entrantes, ainsi qu'à les authentifier ou à les autoriser.

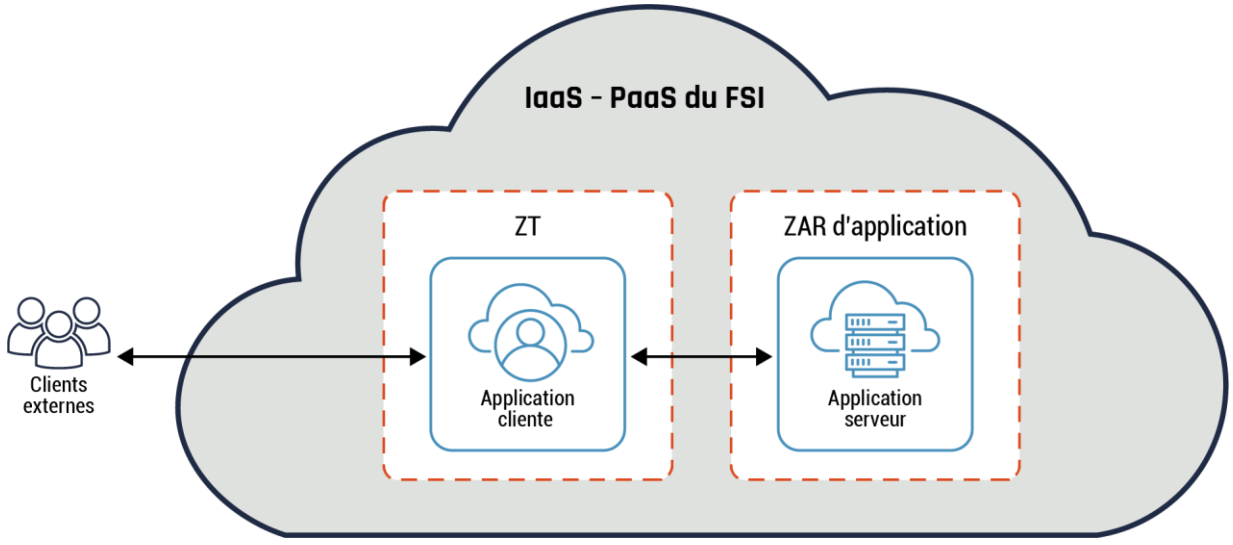
On peut également utiliser une passerelle d'API monolithique afin de déployer une fonctionnalité de RPV pour fournir une connectivité sécurisée entre votre centre de données sur site et votre environnement en nuage, entre autres services. Une passerelle d'API spécialisée peut servir à traiter les cas d'utilisation qui nécessitent un ensemble diversifié de fonctions, comme permettre à différents types d'utilisateurs et à d'autres entités (par exemple, des appareils) d'accéder au microservice.

6.9.2 Antimodèle avec API

Points essentiels de ce modèle

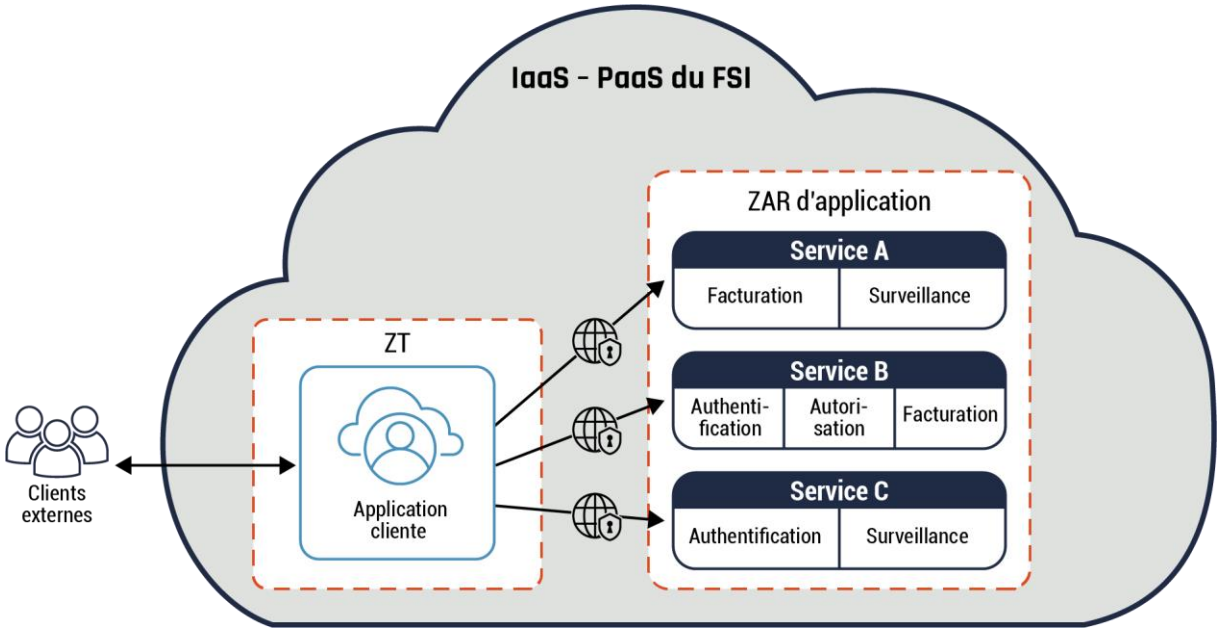
Votre organisation peut décider d'utiliser un antimodèle avec API dans des cas limités exigeant une connectivité plus directe entre le client et le microservice. Par exemple, ce cas d'utilisation peut convenir dans une architecture client-serveur, comme une connectivité de données entre une application client et une application serveur. Les deux composants sont déployés dans un environnement en nuage. Le serveur est déployé dans la ZAR d'application, alors que le client réside sur un point terminal ou un ordinateur virtuel mis en place dans la ZT. On peut envisager de faire appel à un antimodèle avec API comme solution temporaire à certains problèmes. Ce modèle peut, par exemple, résoudre les problèmes de latence entre le client et le microservice, car en raison de sa conception simple, il n'est pas nécessaire de déployer un aussi grand nombre de composants ou d'appareils. Il permet également d'apparier les composants logiciels. **Il est important de noter que, lorsque cela s'avère possible, il est préférable d'utiliser un modèle avec API, plutôt qu'un antimodèle avec API.** Pour plus de détails, prière de consulter la figure 14, Antimodèle avec API (exemple 1), et la figure 15, Antimodèle avec API (exemple 2), ci-dessous.

Figure 14 : Antimodèle avec API (exemple 1)



L'exemple ci-dessus illustre une connectivité directe entre le client et le serveur (microservice). Les données sont regroupées en lot et transférées au moyen de l'utilitaire SCP. L'adoption de ce type de déploiement comme solution d'entreprise pose certains défis. On recommande de déployer une solution basée sur les API pour fournir des données en temps quasi réel. Par exemple, les services communs, comme l'authentification, l'autorisation et la facturation, font rarement l'objet d'une normalisation et doivent être intégrés à des services individuels au moyen de ce type de modèle.

Figure 15 : Antimodèle avec API (exemple 2)



Dans l'exemple ci-dessus, le client communique avec chaque service individuellement. Chaque service peut exiger qu'on y intègre des services communs, comme des services organisationnels et de sécurité. On peut également demander au client d'accéder aux services individuels en utilisant des localisateurs de ressources uniformes (URL pour *Unique Resource Locator*) différents.

Conseils

Le client et le microservice sont placés dans des zones réseau différentes. Par exemple, le microservice est placé dans la ZAR de données et le client dans la ZT.

On peut avoir recours à des NACL et à des NSG afin de restreindre l'accès aux composants utilisant l'antimodèle avec API. Il convient de tirer avantage des capacités de sécurité supplémentaires, comme la sensibilité au contexte et un contrôle de l'accès plus précis, pour restreindre davantage le client et le microservice. Dans la mesure du possible, il est préférable d'utiliser un modèle avec API approprié, plutôt qu'un antimodèle avec API.

7 Contenu complémentaire

7.1 Liste des acronymes, des abréviations et des sigles

Acronyme, abréviation ou sigle	Définition
API	Interface de programmation d'applications (*Application Programming Interface*)
CASB	Agent de sécurité d'accès au nuage (*Cloud Access Security Broker*)
CCC	Centre de la sécurité des télécommunications
CST	Centre canadien pour la cybersécurité
DDoS	Attaque par déni de service distribué (*Distributed Denial of Service*)
DNS	Service de noms de domaine (*Domain Name Service*)
DoS	Déni de service (*Denial of Service*)
FAI	Fournisseur d'échange infonuagique (*Cloud Exchange Provider*)
FIPS	*Federal Information Processing Standards*
FSI	Fournisseur de services infonuagiques
FSSG	Fournisseur de services de sécurité gérés
FTP	Protocole de transfert de fichiers (*File Transfer Protocol*)
GC	Gouvernement du Canada
HTTP	Protocole de transfert hypertexte (*Hypertext Transfer Protocol*)
HTTPS	Protocole de transfert hypertexte sécurisé (*Hypertext Transfer Protocol Secure*)
IaaS	Infrastructure-service (*Infrastructure as a Service*)
IaC	Infrastructure en tant que code (*Infrastructure as Code*)
IPsec	Protocole IPsec (*Internet Protocol Security*)
ITSG	Conseils en matière de sécurité des technologies de l'information (*Information Technology Security Guidance*)
ITSP	Conseils en matière de sécurité des technologies de l'information pour les praticiens (*Information Technology Security Guidance for Practitioners*)
NACL	Liste de contrôle d'accès réseau (*Network Access Control List*)
NGFW	Pare-feu de prochaine génération (*Next-Generation Firewall*)
NIST	National Institute of Standards and Technology
NSG	Groupe de sécurité réseau (*Network Security Group*)
OSI	Interconnexion de systèmes ouverts (modèle) (*Open Systems Interconnection*)
PaaS	Plateforme-service (*Platform as a Service*)

Acronyme, abréviation ou sigle	Définition
PASSI	Processus d'application de la sécurité dans les systèmes d'information
PIZ	Point d'interface de zone
RPV	Réseau privé virtuel
SaaS	Logiciel-service (*Software as a Service*)
SCT	Secrétariat du Conseil du Trésor du Canada
SDI	Système de détection d'intrusion
SDN	Réseau à définition logicielle (*Software-Defined Network*)
SQL	Langage SQL (*Structured Query Language*)
STI	Sécurité des technologies de l'information
TI	Technologies de l'information
TLS	Protocole de sécurité de la couche transport (*Transport Layer Security*)
UTM	Gestion unifiée des menaces (*Unified Threat Management*)
VM	Machine virtuelle (*Virtual Machine*)
WAF	Pare-feu d'applications Web (*Web Application Firewall*)
WAN	Réseau étendu (*Wide Area Network*)
XML	Langage XML (*Extensible Markup Language*)
ZAP	Zone d'accès public
ZP	Zone publique

7.2 Glossaire

Acronyme, abréviation ou sigle	Définition
Agent de sécurité d'accès au nuage (CASB)	Point d'application de politiques de sécurité infonuagique disposé entre les clients des services infonuagiques et le FSI afin de combiner et d'insérer des stratégies de sécurité organisationnelles au moment d'accéder aux ressources infonuagiques. Les CASB peuvent servir à consolider plusieurs types d'applications de stratégies de sécurité. Parmi les exemples de stratégies de sécurité mises en place, on retrouve l'authentification, l'authentification unique, l'autorisation, la mise en correspondance des justificatifs d'identité, le profilage de dispositifs, le chiffrement, la segmentation en unités, la journalisation, les alertes et la détection et prévention de maliciels.
Antimodèle	Toute solution répétée (mais inefficace) à un problème commun.
Attaque par déni de service (DoS)	Attaque consistant à prévenir l'accès autorisé à une ressource du système ou à retarder les opérations et les fonctions du système.

Acronyme, abréviation ou sigle	Définition
Attaque par déni de service distribué (DDoS)	Attaque dans le cadre de laquelle plusieurs systèmes, généralement compromis, sont utilisés pour cibler un système particulier et causer un déni de service. Les victimes d'une attaque par DDoS sont à la fois le système d'extrémité ciblé et tous les systèmes utilisés de façon malveillante dans le cadre de l'attaque distribuée.
Authentification	Processus de vérification de l'identité déclarée par ou pour une entité de système.
Autorisation	Droits d'accès accordés à une utilisatrice ou un utilisateur, à un programme ou à un processus.
Autorité de zone de sécurité de réseau	La ou les personnes qui sont responsables de la mise en place et de la gestion de la sécurité de la zone de sécurité de réseau et qui doivent rendre des comptes à cet égard.
Chiffrement de bout en bout	Service de confidentialité reposant sur le chiffrement de données à l'intérieur ou au niveau du système d'extrémité source, le déchiffrement correspondant ne se produisant qu'à l'intérieur, ou à la destination.
Concentrateur	Réseau virtuel situé au centre des rayons qui permet de gérer le trafic sortant et d'héberger les services communs utilisés par les rayons. On peut utiliser un concentrateur pour gérer le trafic entrant conformément aux stratégies de sécurité ou au cadre de gestion des risques de l'organisation.
Contrôle de l'accès	Service servant à contrôler l'accès aux applications et aux services autorisés.
Détection des intrusions	Service de sécurité qui surveille et analyse les événements réseau ou système afin de détecter toute tentative d'accès non autorisé aux ressources du système ou du réseau et d'émettre des alertes à cet égard en temps réel ou presque.
Extranet restreint	Extension contrôlée du réseau privé d'une organisation permettant d'échanger de l'information et des ressources avec des organisations jouissant d'un degré de confiance élevé. Un tel extranet d'accès restreint peut se terminer dans une zone de sécurité contrôlée par l'organisation (contrairement à l'extranet générique, qui doit se terminer dans une ZAP). Les deux parties de confiance devraient convenir de la gestion et du contrôle de l'interface au préalable.
Fournisseur de services de sécurité gérés	Fournit des services externes de surveillance et de gestion pour la sécurité des appareils et des systèmes, que ce soit à partir de ses propres installations ou à partir d'autres fournisseurs de centre de données. Les services courants offerts incluent un pare-feu géré, la détection des intrusions, un RPV, l'analyse des vulnérabilités et des services d'antivirus. Les FSSG ont recours à des centres d'opérations de sécurité à disponibilité élevée afin de fournir des services en tout temps dans le but de réduire le personnel de sécurité qu'une entreprise devrait autrement embaucher, former et conserver afin d'assurer une posture de sécurité acceptable.
Fournisseur de services infonuagiques	Entreprise offrant des composants de l'informatique en nuage, typiquement des IaaS, des SaaS ou des PaaS, à d'autres entreprises.
Frontière	Partie du périmètre d'une zone ou d'un réseau, qui sert de point de connexion entre deux zones ou réseaux.
Gestion unifiée des menaces	Pare-feu de réseau offrant dans un seul produit différentes fonctions, comme le filtrage des courriels, la protection contre les programmes malveillants, la détection ou la prévention des intrusions et le filtrage du contenu Web, en plus des fonctions traditionnelles d'un pare-feu.
Hôte	Ordinateur connecté à un sous-réseau ou à un interréseau de communications, qui peut utiliser des services réseau pour échanger des données avec d'autres systèmes connectés au même sous-réseau ou interréseau.
Infrastructure en tant que code	Infrastructure permettant d'automatiser la gestion de la configuration des environnements en nuage et des ressources connexes. Elle veille à ce que la configuration de l'environnement soit reproductible et traçable.

Acronyme, abréviation ou sigle	Définition
Infrastructure-service	La cliente ou le client a la capacité de fournir le traitement, le stockage, les réseaux et les autres ressources informatiques de base, dans la mesure où il peut déployer et exécuter des logiciels arbitraires, y compris des systèmes d'exploitation et des applications. Le client n'a pas à gérer ni à contrôler l'infrastructure infonuagique, mais peut contrôler les activités liées aux systèmes d'exploitation, au stockage et aux applications déployées; il peut également disposer d'un contrôle limité sur certains composants réseau (par exemple, les pare-feu hôtes).
Inspection dynamique	L'inspection dynamique intercepte les paquets au niveau de la couche réseau (comme dans les filtres de paquets), mais les données dérivées de toutes les couches de communication sont consultées et analysées pour renforcer la sécurité (plutôt que les couches 4 à 7 dans le cas des passerelles de la couche application). Elle accroît encore davantage le niveau de sécurité en intégrant les attributs de la couche liaison de données et de la couche application et des informations contextuelles consignées et mises à jour de façon dynamique. On obtient ainsi un référentiel de renseignements permettant d'évaluer les tentatives de communication ultérieures.
Intégrité de l'origine des données	Assurance fournie par l'expéditeur que le message reçu n'a pas été modifié et qu'il était complet avant la transmission.
Interface	Frontière où transitent les communications entre deux systèmes. Il peut s'agir d'un connecteur matériel utilisé pour la connexion à d'autres dispositifs ou d'une convention permettant d'établir des communications entre deux systèmes logiciels. Il existe souvent entre les deux systèmes un composant intermédiaire servant à connecter leurs interfaces.
Internet	Réseau informatique mondial unique constitué d'un ensemble de réseaux commerciaux, gouvernementaux, éducatifs et autres qui partagent l'ensemble de protocoles spécifiés par le Conseil IAB (Internet Architecture Board) et l'espace de noms et d'adresses géré par la Société pour l'attribution des noms de domaines et numéros sur Internet.
Logiciel-service	La cliente ou le client a la capacité d'utiliser les applications du fournisseur qui sont exécutées sur l'infrastructure infonuagique. Ces applications sont accessibles à partir de divers dispositifs clients par l'intermédiaire d'une interface client léger comme un navigateur Web (p. ex. services de courrier Web) ou d'une interface de programmation. Le client n'a pas à gérer ni à contrôler l'infrastructure infonuagique sous-jacente, dont le réseau, les serveurs, les systèmes d'exploitation, le stockage ou même les capacités d'application, à l'exception, peut-être, des paramètres de configuration d'application propres à l'utilisateur.
Maliciel	Mot-valise formé de « malveillant » et de « logiciel ». Module logiciel (p. ex. bombe logique, intentionnellement inséré ou intégré dans un système informatique avec le dessein de causer des dommages.
Microservice	Ensemble de conteneurs travaillant de pair pour former une application.
Nœud	Dispositif adressable connecté à un réseau informatique. S'il s'agit d'un ordinateur, on l'appelle plus souvent un « hôte ». Le terme nœud comprend également les dispositifs, comme les routeurs et les imprimantes, qui ne sont pas, à proprement parler, des « hôtes ».
Nuage	L'informatique en nuage (ou l'infonuagique) est un modèle convivial d'accès Web sur demande à un répertoire partagé de ressources informatiques configurables (p. ex. réseaux, serveurs, stockage, applications et services). Mis en œuvre en un tournemain, ce modèle exige une gestion minimale et peu d'interaction avec le fournisseur du service.
Pare-feu	Passerelle créant entre deux réseaux une frontière qui sert à isoler, à filtrer et à protéger les ressources des systèmes locaux des connexions externes, par le contrôle du volume et des types de trafic autorisés à passer d'un réseau à l'autre.

Acronyme, abréviation ou sigle	Définition
Passerelle	Système intermédiaire servant d'interface entre deux réseaux informatiques.
Périmètre	Ligne de connexion imaginaire entourant un ensemble de composants de réseau, qui sert à décrire les limites externes d'un réseau.
Périmètre de sécurité	Frontière d'un domaine où s'applique une stratégie de sécurité ou une architecture de sécurité : par exemple la limite de l'espace dans lequel les services de sécurité protègent les ressources du système.
PIZ connecté à la zone de gestion (PIZ connecté à la ZG)	PIZ déployé sur le chemin d'accès de communication entre les zones de gestion et la voie de communication qui gère le trafic de gestion. Le PIZ connecté à la ZG est associé à la fonctionnalité de gestion de système.
PIZ de chemins de données	Point d'interface déployé sur la voie de communication entre les zones qui traitent le trafic opérationnel (par opposition au trafic de gestion). Le trafic opérationnel est associé aux fonctionnalités d'utilisateur.
Plan de contrôle	Sert à gérer les ressources dans un environnement en nuage au moyen d'outils, comme un outil d'orchestration de conteneurs et un réseau SDN.
Plan de données	Traite le trafic opérationnel (d'utilisateur). Il s'agit de l'endroit où résident les ressources gérées par le plan de contrôle.
Plateforme-service	La cliente ou le client a la capacité de déployer dans l'infrastructure infonuagique des applications créées par le client ou acquises et créées au moyen de langages de programmation, de bibliothèques, de services et d'outils pris en charge par le fournisseur. Le client n'a pas à gérer ni à contrôler l'infrastructure infonuagique sous-jacente, y compris le réseau, les serveurs, les systèmes d'exploitation et le stockage. Il a toutefois le contrôle des applications déployées et, possiblement, des paramètres de configuration de l'environnement qui héberge l'application.
Point d'interface de zone	Interface et point de connexion entre deux zones de sécurité de réseau à travers laquelle le trafic est acheminé.
Protocole	Ensemble de règles (c.-à-d. formats et procédures) permettant de mettre en œuvre et de contrôler certains types d'association (p. ex., les communications) entre les systèmes. Une suite ordonnée d'étapes informatiques ou de télécommunications qui sont exécutées par deux ou plusieurs entités système pour réaliser un objectif commun.
Rayon	Réseau virtuel hébergeant des charges de travail en nuage qui se connecte à un concentrateur au moyen d'un appairage de réseaux virtuels ou d'une passerelle réseau.
Réseau à définition logicielle	Approche à la gestion de réseau permettant d'assurer une configuration dynamique et efficace du point de vue de la programmation afin d'améliorer les performances et les activités de surveillance.
Réseau privé virtuel	Service utilisé pour établir des connexions privées entre une entité externe et votre organisation pour l'authentification, l'autorisation, la confidentialité des transmissions et l'intégrité.
Réseau virtuel	Réseau informatique logique (c'est-à-dire artificiel ou simulé), à usage restreint, construit à partir des ressources d'un réseau physique (c'est-à-dire réel) relativement public (comme une ZP), en faisant appel au chiffrement (au niveau des hôtes ou des passerelles) et en mettant sous tunnel des liaisons du réseau virtuel à travers le réseau réel. Dans le vocabulaire général, ce terme désigne souvent un réseau qui émule un réseau privé, même s'il passe par les infrastructures et les lignes du réseau public.
Réseau virtuel sécurisé (RVS)	Réseau virtuel utilisant la cryptographie (p. ex. le protocole IPsec) contrairement aux RPV dont la sécurité est simplement fondée sur l'isolement logique (p. ex. des communications MPLS ou un réseau local Ethernet virtuel).

Acronyme, abréviation ou sigle	Définition
Services de connectivité hybride du GC	Service fournissant des connexions sécurisées entre les centres de données d'entreprise du GC et les FSI par l'intermédiaire de liens de connectivité privée. Il assure une connectivité entre les utilisateurs ou les applications sur site et les applications sur le nuage.
Services de mandataire	Fonction d'interréseau de service d'application pouvant être incorporée à un pare-feu, et qui crée, pour le client, une duplication des services disponibles sur d'autres serveurs. Pour le client, le mandataire semble être le serveur lui-même, alors que pour le serveur, il se comporte comme le client. (Lorsqu'il est incorporé à un pare-feu, un service mandataire est souvent appelé « passerelle d'applications »).
Sous-réseau	Portion d'un réseau, pouvant constituer un segment physique distinct, qui partage une adresse réseau avec d'autres portions du réseau, dont il se distingue par son numéro de sous-réseau.
Structure infonuagique	Serveur, connexions à haute vitesse et commutateurs qui composent une infrastructure ou un cadre infonuagique.
Système de frontière interne	Passerelle qui relie deux interréseaux ou plus dans une zone de sécurité de réseau.
Tunnels doubles	Liens de chiffrement multiples, comme des tunnels de RPV, utilisés par les données se dirigeant vers la même destination par l'entremise d'interfaces différentes. Les tunnels servent à fournir une protection accrue. Les liens dédiés peuvent provenir du même fournisseur ou de différents fournisseurs.
Vérification de l'intégrité des données	Vérification par le destinataire que le message reçu n'a pas été modifié en transit et qu'il provient de l'expéditeur initial.
Vulnérabilité	Lacune ou faiblesse dans les efforts de protection d'un réseau, d'un système ou d'un bien de TI.
Zone d'accès public	Partie d'un réseau située entre deux composants d'application de stratégie du réseau (typiquement entre la ZP et les réseaux internes) et permettant à l'organisation d'héberger ses propres services Internet sans risquer d'accorder un accès non autorisé à son réseau privé.
Zone de sécurité de réseau	Environnement de réseau clairement délimité relevant d'une autorité de zone de sécurité de réseau et caractérisé par un niveau standard de vulnérabilité aux menaces. On distingue les types de zones d'après les exigences de sécurité s'appliquant aux interfaces, au contrôle du trafic, à la protection des données, au contrôle de la configuration de l'hôte et au contrôle de la configuration du réseau.

7.3 Références

Numéro	Référence
1	Centre canadien pour la cybersécurité. ITSM.50.062, *Gestion des risques liés à la sécurité infonuagique*.
2	Centre canadien pour la cybersécurité. ITSP.80.022, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau*, janvier 2021.
3	Centre canadien pour la cybersécurité. ITSG-38, *Établissement des zones de sécurité dans un réseau – Considérations de conception relatives au positionnement des services dans les zones*, mai 2009.

Numéro	Référence
4	Centre canadien pour la cybersécurité. ITSG-33, *La gestion des risques liés à la sécurité des TI : Une méthode axée sur le cycle de vie*, décembre 2014.
5	Secrétariat du Conseil du Trésor *Politique sur les services et le numérique*, 1er avril 2020.
6	Secrétariat du Conseil du Trésor *Politique sur la sécurité du gouvernement*, 1er juillet 2019.
7	Secrétariat du Conseil du Trésor *Directive sur la gestion de la sécurité*, 1er juillet 2019.
8	Secrétariat du Conseil du Trésor *Orientation relative à la résidence des données électroniques*, 13 mars 2018.
9	Secrétariat du Conseil du Trésor *Normes du gouvernement du Canada sur les API*, 1er juillet 2020
10	Centre canadien pour la cybersécurité. ITSP.40.062, *Conseils sur la configuration sécurisée des protocoles réseau*, octobre 2020.
11	Centre canadien pour la cybersécurité. ITSP.40.111, *Algorithmes cryptographiques pour l'information NON CLASSIFIÉ, PROTÉGÉ A et PROTÉGÉ B*, septembre 2022.
12	Secrétariat du Conseil du Trésor Modèles d'architecture axés sur l'IPA pour la PaaS du nuage public, version 1.1, février 2021.

Annexe A : Exigences de sécurité et PIZ en nuage

Le document ITSP.80.022, *Exigences de base en matière de sécurité pour les zones de sécurité de réseau – Annexe F : Point d'interface de zone*, contient un ensemble d'objectifs regroupés en fonction des activités de contrôle du trafic, de l'intégrité et de la disponibilité du réseau, et de la protection des données. Une série d'exigences de base en matière de sécurité sont définies pour le PIZ à partir de ces objectifs de sécurité.

Le tableau ci-dessous illustre la mise en correspondance des objectifs et exigences de sécurité tirés de l'ITSP.80.022 avec les constructions du PIZ en nuage définies précédemment. Il est recommandé de consulter l'ITSP.80.022 pour connaître la définition détaillée associée au numéro d'exigence et au contrôle de sécurité connexe de l'ITSG-33. Il est important pour votre organisation de bien comprendre les situations où il convient de mettre en place un PIZ particulier en fonction des exigences de sécurité de ce qui est protégé et de la stratégie de sécurité organisationnelle.

Tableau 3 : Mise en correspondance des exigences de base et des PIZ en nuage

Numéro de l'exigence dans l'ITSP.80.022	Liste de contrôle d'accès réseau	Groupe de sécurité réseau	Pare-feu de prochaine génération	Commentaire
Interface réseau				
ZIP-NI-100	Oui	Oui	Oui	Tous les chemins d'accès réseau doivent transiter par un PIZ.
ZIP-NI-101	Oui	Oui	Oui	Nombre limité de PIZ.
ZIP-NI-105	Oui	Oui	Oui	Collecte de donnée prise en charge par des journaux du flux réseau.
Contrôle du trafic				
ZIP-TC-101	Oui	Oui	Oui	Séparation du trafic de gestion du reste du trafic des autres réseaux (la séparation peut être physique ou logique).
ZIP-TC-102	Oui	Oui	Oui	En cas d'urgence ou de menace accrue, peut répondre rapidement à des niveaux de sécurité rehaussés.
ZIP-TC-103	Oui	Oui	Oui	Dans un centre de données traditionnel, un PIZ peut servir à fournir une authentification entre deux zones de réseau et aux communications entre les services de ces zones. Un PIZ sert à fournir une autorisation de connexion au niveau de la couche transport (modèle Open Systems Interconnection, couche 4) entre deux zones dans un environnement en nuage et pour les communications entre les services de ces zones. Certains FSI fournissent cette capacité.
ZIP-TC-105	Oui	Oui	Oui	Principe de droit d'accès minimal pour le trafic.
ZIP-TC-106	Oui	Oui	Oui	Une classe de service est fournie.

ZIP-TC-107	Oui	Oui	Oui	Modèle d'adressage pouvant détecter et diagnostiquer le trafic malveillant.
ZIP-TC-110	Oui	Oui	Oui	Principe de droit d'accès minimal pour le contrôle de l'accès.
ZIP-TC-111	Non	Oui	Oui	Les NACL sont sans état.
ZIP-TC-112	Non	Non	Oui	Les NACL/NSG sont pris en charge par les journaux du flux réseau. Les alertes sont activées par d'autres services infonuagiques.
ZIP-TC-113	Non	Non	Oui	Le filtrage de contenu des NACL/NSG n'est pas disponible dans la ZP.
ZIP-TC-120	s.o.	s.o.	s.o.	ANS avec le fournisseur de services pour l'infrastructure commune.
ZIP-TC-122	Oui	Oui	Oui	Trafic malformé rejeté.
ZIP-TC-123	Oui	Oui	Oui	Les NACL/NSG fonctionnent au niveau des couches 3 et 4 de l'OSI. Les NGFW fonctionnent au niveau de la couche 3 et des couches supérieures.
ZIP-TC-124	Oui	Oui	Oui	Capacité de filtrage du trafic entre la ZP et la ZAP.
ZIP-TC-125	Oui	Oui	Oui	Principe de droit d'accès minimal pour les adresses source et de destination.
Configuration réseau				
ZIP-NC-100	Oui	Oui	Oui	Les NACL/NSG sont pris en charge par les journaux d'audit du nuage.
ZIP-NC-103	Oui	Oui	Oui	La topologie de réseau peut être périodiquement vérifiée. Par exemple, une solution d'infrastructure en tant que code peut être utilisée afin de s'assurer que la topologie de réseau de l'environnement en nuage respecte la configuration de référence.
ZIP-NC-104	Oui	Oui	Oui	La configuration réseau peut être vérifiée pour les connexions non autorisées.
ZIP-NC-105	Oui	Oui	Oui	Les NACL/NSG sont pris en charge par le RBAC et la stratégie. L'accès au plan de contrôle est protégé par ces fonctionnalités, qui sont intégrées
ZIP-NC-109	Oui	Oui	Oui	Seuls les administrateurs authentifiés et autorisés peuvent gérer les nœuds du PIZ
ZIP-NC-110	Oui	Oui	Oui	Les modifications peuvent être approuvées avant leur mise en œuvre
Configuration d'hôte				
ZIP-HC-100	Non	Non	Non	La configuration de l'hôte dépasse la portée de cette publication sur l'établissement de zones infonuagiques.
ZIP-HC-101	Non	Non	Non	La configuration de l'hôte dépasse la portée de cette publication sur l'établissement de zones infonuagiques.

ZIP-HC-103	Non	Non	Non	La configuration de l'hôte dépasse la portée de cette publication sur l'établissement de zones infonuagiques.
ZIP-HC-104	Non	Non	Non	La configuration de l'hôte dépasse la portée de cette publication sur l'établissement de zones infonuagiques.
ZIP-HC-105	Non	Non	Non	La configuration de l'hôte dépasse la portée de cette publication sur l'établissement de zones infonuagiques.
ZIP-HC-106	Non	Non	Non	La configuration de l'hôte dépasse la portée de cette publication sur l'établissement de zones infonuagiques.
ZIP-HC-111	Non	Non	Non	La configuration de l'hôte dépasse la portée de cette publication sur l'établissement de zones infonuagiques.
ZIP-HC-112	Non	Non	Non	La configuration de l'hôte dépasse la portée de cette publication sur l'établissement de zones infonuagiques.
Protection des données				
ZIP-DP-101	Oui	Oui	Oui	Un PIZ peut prendre en charge les connexions du trafic de données chiffrées entre les zones. Prière de consulter l'ITSP.50.106, *Guide sur le chiffrement des services infonuagiques,* du Centre pour la cybersécurité pour plus de détails sur les conseils de chiffrement s'appliquant au nuage.
ZIP-DP-103	Oui	Oui	Oui	La catégorisation de la sécurité du PIZ et les résultats du PASSI pourraient exiger la mise en place de mesures de protection des données. Les services de protection des données peuvent être appliqués soit à la couche réseau, soit aux couches supérieures, selon les besoins de la mise en œuvre. Les NACL/NSG fonctionnent au niveau des couches 3 et 4 de l'OSI, alors que le NGFW peut fonctionner au niveau de la couche 3 et des couches supérieures de l'OSI.
ZIP-DP-104	Non	Non	Oui	Les NACL/NSG ne valident pas le chiffrement FIPS-140-2 et les signatures numériques.

Annexe B : Accès aux charges de travail du nuage et cas d'utilisation

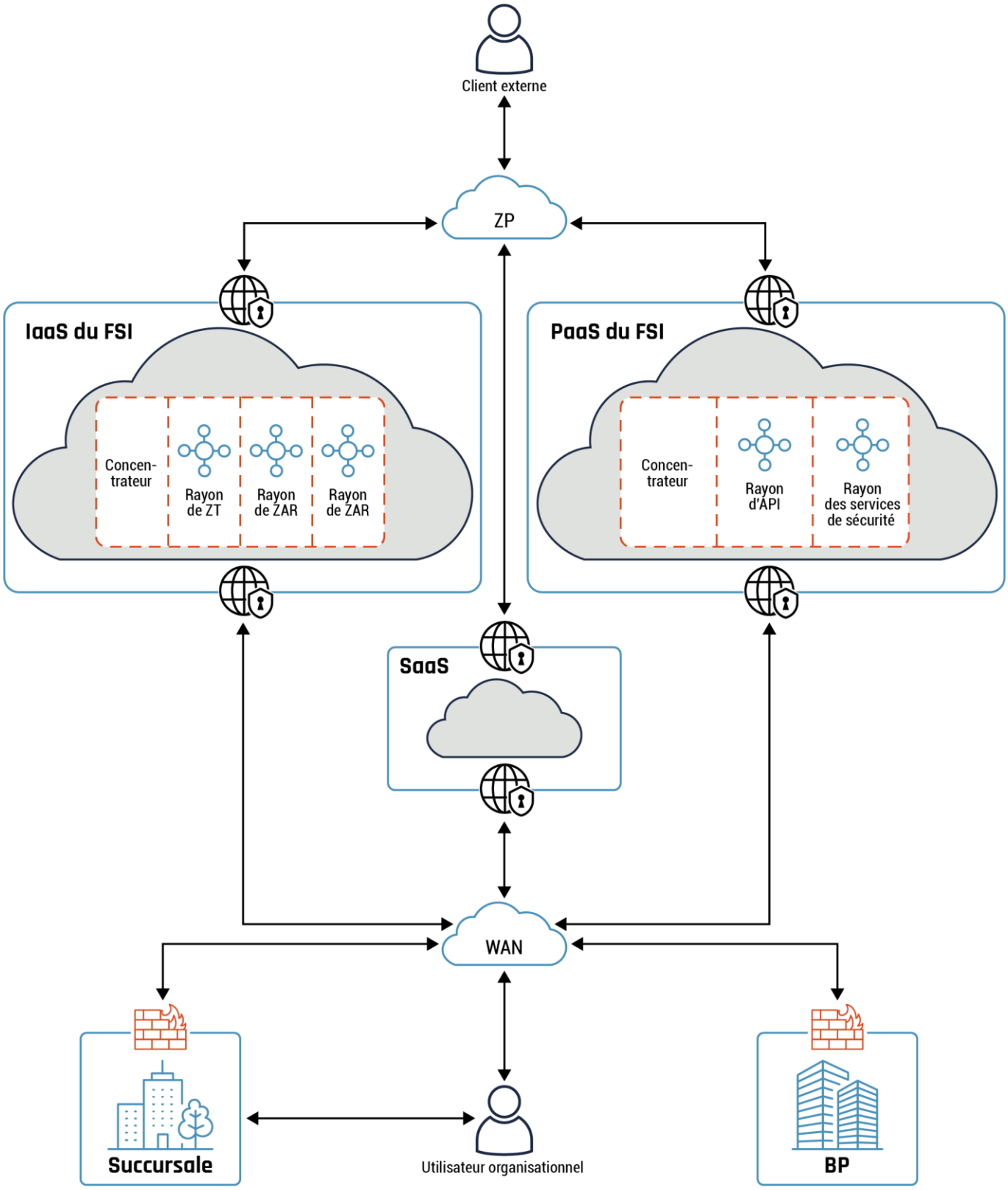
La présente section propose plus de détails sur les concepts évoqués à la section 4, comme le modèle de réseau en étoile. Elle fournit également quelques cas d'utilisation courants liés à l'accès aux charges de travail en nuage hébergées dans les IaaS et les PaaS du FSI selon le modèle de réseau en étoile.

Le diagramme ci-dessous présente ce qui suit :

- une utilisatrice ou un utilisateur de l'organisation accédant au réseau sur site par l'intermédiaire d'un RPV;
- une utilisatrice ou un utilisateur de l'organisation, l'administratrice ou l'administrateur de système et l'API interne accédant aux charges de travail du nuage à partir d'un réseau sur site;
- une utilisatrice ou un utilisateur externe et les API externes accédant aux charges de travail du nuage depuis la ZP.

Les charges de travail du nuage peuvent également accéder aux charges de travail du réseau sur site afin de terminer les demandes de services de l'utilisatrice ou l'utilisateur externe et de l'API. Prière de consulter le tableau 4, Accès aux charges de travail du nuage et cas d'utilisation, pour plus de détails sur les cinq cas d'utilisation illustrés dans le diagramme.

Figure 16 : Accès aux charges de travail du nuage et cas d'utilisation



Les deux connexions dédiées du CXP vers les services IaaS et PaaS de FSI établies à partir du réseau étendu peuvent provenir du même fournisseur ou de fournisseurs différents. Le CASB peut servir de mandataire inverse et appliquer la stratégie de sécurité de votre organisation, comme l'authentification, l'autorisation et l'authentification unique. De plus, il est possible d'utiliser une connexion dédiée du CXP pour se connecter à un FSI (non illustré dans le diagramme ci-dessus) en fonction de la stratégie de sécurité de votre organisation.

Tableau 4 : Accès aux charges de travail du nuage et cas d'utilisation

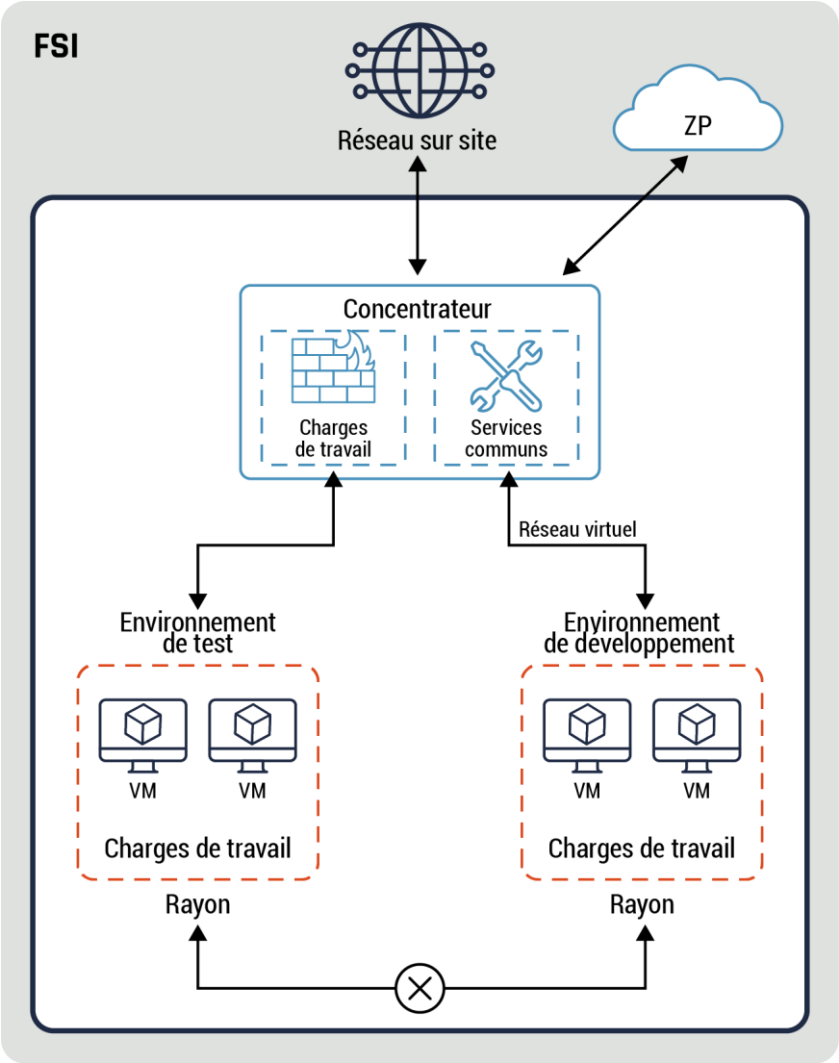
Référence	Cas d'utilisation
A1	Un utilisateur de l'organisation accède au réseau sur site par l'intermédiaire d'un RPV à partir de la ZP. L'utilisateur, après avoir été authentifié et autorisé, peut accéder aux charges de travail du nuage IaaS et PaaS à partir du réseau sur site. Le même flux de trafic s'applique aux autres utilisatrices et utilisateurs situés sur le réseau sur site des deux succursales du bureau principal en ce qui a trait à l'accès aux charges de travail du nuage basées sur les privilèges accordés par votre organisation. Tous les flux de trafic sont sécurisés.
A2	L'administrateur de système accède aux environnements en nuages IaaS et PaaS à partir du réseau sur site pour réaliser des tâches de gestion.
A3	Une utilisatrice externe accède aux charges de travail du nuage IaaS et PaaS à partir de la ZP. À l'occasion, les charges de travail du nuage accéderont aux charges de travail sur site hébergées depuis une succursale ou le bureau principal afin de répondre à des demandes de service (selon les exigences opérationnelles relatives aux charges de travail du nuage ou les stratégies de sécurité de votre organisation). Cela est illustré par la ligne bleue pointillée allant des composants IaaS et PaaS jusqu'au WAN, puis vers le bureau principal et les deux succursales.
A4	L'interface API interne accède aux charges de travail du nuage à partir du réseau sur site. Elle est utilisée pour accéder aux services et aux données de l'organisation. Tous les flux de trafic de l'interface API sont sécurisés.
A5	L'interface API externe accède aux charges de travail du nuage à partir de la ZP. Elle est utilisée pour accéder aux services et aux données de l'organisation. À l'occasion, les charges de travail du nuage se connecteront aux charges de travail sur site hébergées depuis une succursale ou le bureau principal afin de répondre à des demandes de service (selon les exigences opérationnelles des charges de travail du nuage ou des stratégies de sécurité de votre organisation). Cela est illustré par la ligne verte pointillée allant des composants IaaS et PaaS jusqu'au WAN, puis vers le bureau principal et les deux succursales.

Annexe C : Exemples de modèle de réseau en étoile

La présente section donne quelques exemples du modèle de réseau en étoile qu'il est possible de mettre en œuvre dans l'environnement en nuage de votre organisation. Ces modèles sont répertoriés selon un ordre de complexité croissant.

Le modèle de réseau en étoile se compose de deux rayons distincts où sont hébergés vos environnements de test et de développement. Il n'y a aucune connectivité directe entre les deux rayons (environnements), sauf par l'intermédiaire du concentrateur. Le concentrateur héberge les services communs et offre une connectivité externe vers le réseau sur site et la ZP.

Figure 17 : Un exemple de modèle de réseau en étoile

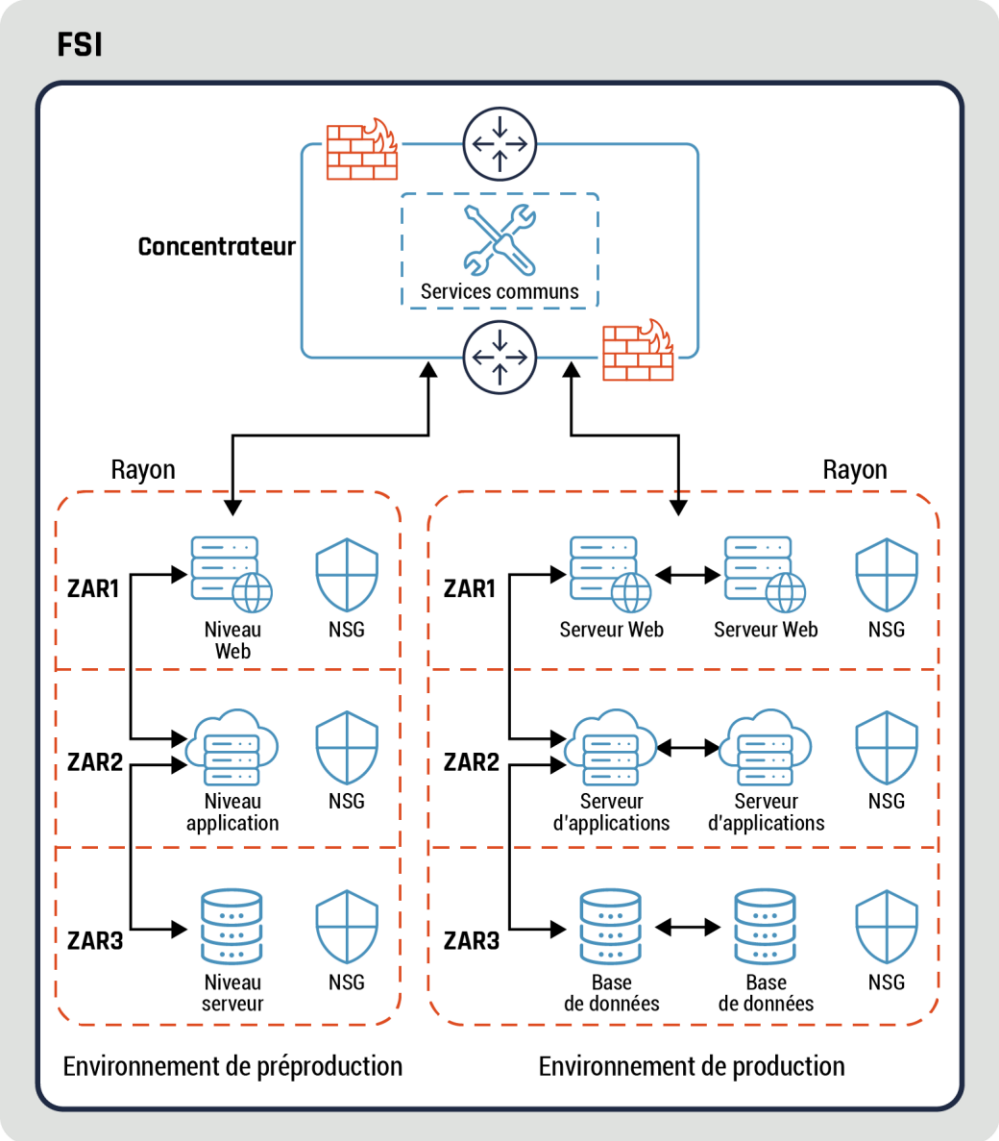


Le prochain exemple consiste en un modèle de réseau en étoile hébergeant un environnement de préproduction et un environnement de production. Les deux environnements sont similaires, à l'exception que le premier est entièrement redondant. Un NSG permet de restreindre l'accès entre les différentes zones de sécurité au sein de chaque rayon. Comme dans l'exemple précédent, il n'y a aucune connectivité directe entre les deux rayons, sauf par l'intermédiaire du

concentrateur. Le concentrateur offre une connectivité externe vers la ZP et le réseau local en fonction des exigences de sécurité de votre organisation. On retrouve des niveaux Web, d'application et de base de données dans chaque rayon.

Des restrictions sont également appliquées au trafic entre les trois niveaux au moyen du NSG. Le niveau de base de données n'est accessible qu'à partir du niveau d'application, alors qu'il existe une connectivité directe entre les niveaux Web et d'application. Une mise en œuvre au niveau de la base de données est un exemple robuste de modèle avec enclave de données.

Figure 18 : Deuxième exemple de modèle de réseau en étoile

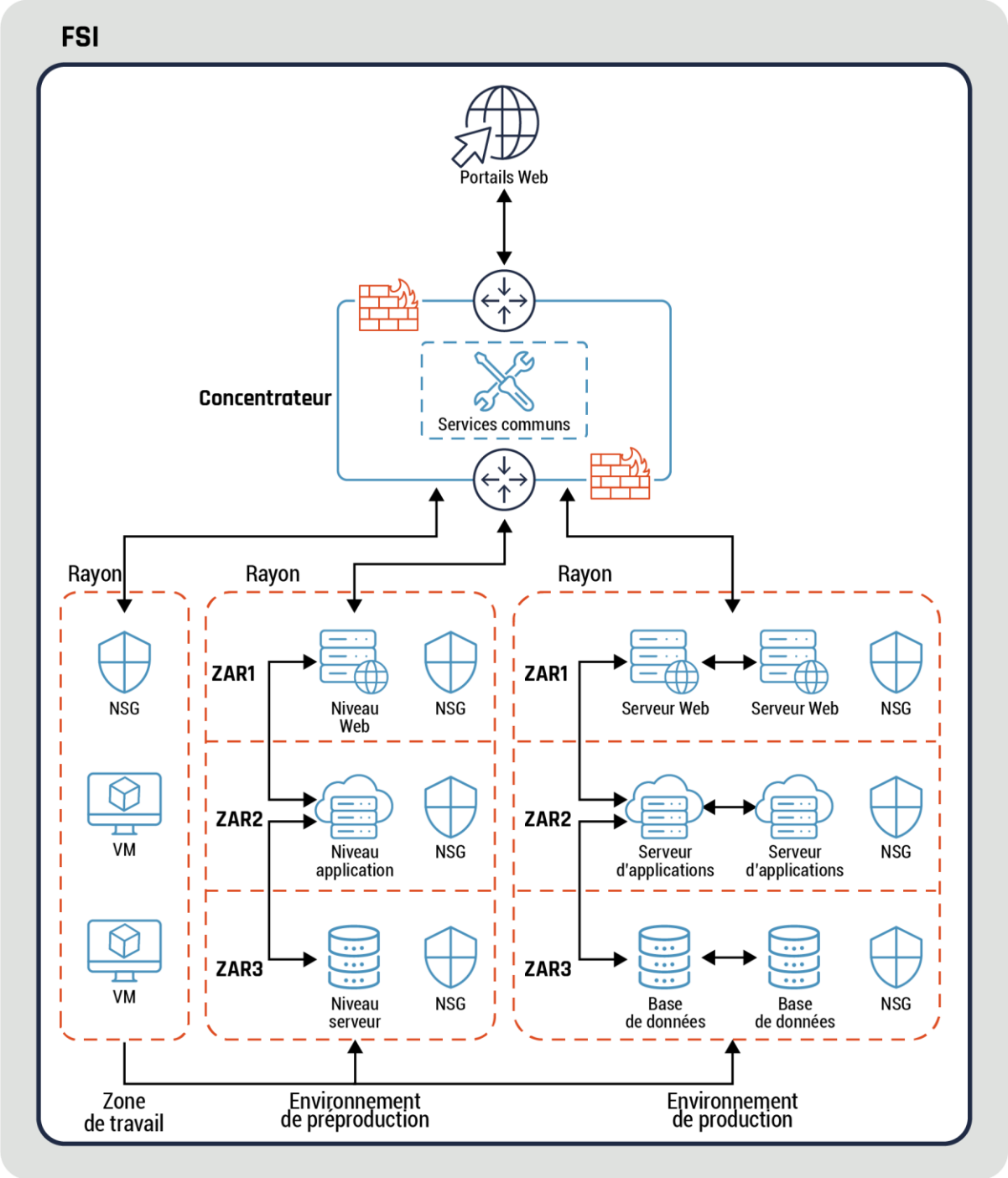


Le modèle de réseau en étoile suivant se compose de trois rayons, d'une zone de travail, d'un environnement de production et d'un environnement de préproduction. Le modèle est similaire à l'exemple précédent, à l'exception de la ZT, qui offre une connectivité directe aux deux environnements. Il n'y a aucune connectivité directe entre les deux environnements

(préproduction et production). La ZT héberge des ordinateurs virtuels qu'il est possible de mettre en place de façon dynamique (sur demande) ou statique selon les besoins opérationnels de votre organisation.

Le concentrateur offre une connectivité externe vers la ZP et le réseau local en fonction des exigences de sécurité de votre organisation.

Figure 19 : Troisième exemple de modèle de réseau en étoile

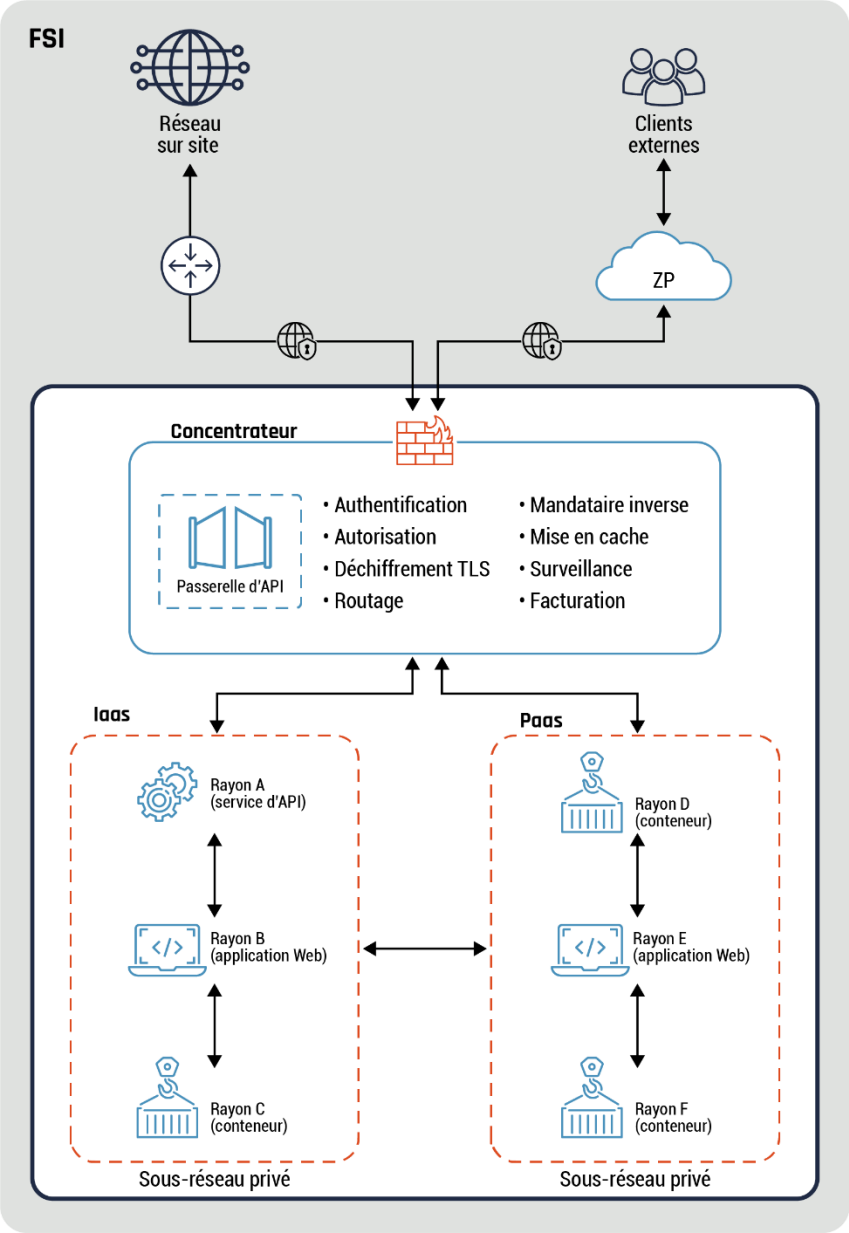


Annexe D : Passerelles d'API, services d'API et conteneurs

Le diagramme de la présente section (figure 20 ci-dessous) offre un exemple de passerelle d'API et de différents types de services déployés, comme des services de conteneurs, d'application et d'API. Ces services sont déployés sur deux sous-réseaux privés d'IaaS et de PaaS. Les services offerts par les composants d'IaaS et de PaaS peuvent communiquer entre eux. On retrouve également une connectivité entre les composantes d'IaaS et de PaaS.

Un pare-feu, comme un WAF, et une passerelle d'API sont déployés sur un concentrateur qui offre une connectivité externe vers la ZP et le réseau sur site. On peut utiliser le WAF pour filtrer le trafic malveillant qui transite vers les services des deux rayons. La passerelle d'API fait office de mandataire inverse et peut offrir des services, comme l'authentification et l'autorisation.

Figure 20 : Exemple de passerelles d'API, de services API et de conteneurs



Le diagramme ci-dessous illustre la différence entre le placement du plan de contrôle et du plan de données. Comme mentionné plus tôt, l'outil d'orchestration de conteneurs fait partie du plan de contrôle. Les deux conteneurs ou applications font partie du plan de données. Tous le flux de trafic entre le plan de contrôle et les applications du plan de données transitent par les mandataires. Les flux de trafic entre les deux applications sont sécurisés. Par ailleurs, tous les flux de trafic entre le plan de contrôle, le plan de données et les applications sont sécurisés.

Figure 21 : Relation entre les plans de contrôle et de données