Orientation sur la modernisation des applications   
Modèles d’architecture axés sur l’IPA pour la PaaS du nuage public

Version 1.1

Approuvée à la réunion du Conseil d’examen de l’architecture intégrée du gouvernement du Canada (CEAI GC) du 25 mars 2021

**Table des matières**

[Aperçu 2](#_Toc77159448)

[Pourquoi une architecture axée sur les IPA? 4](#_Toc77159449)

[Modèles élaborés à partir de la collaboration 5](#_Toc77159450)

[Références aux politiques 6](#_Toc77159451)

[Références de l’architecture de sécurité 7](#_Toc77159452)

[Points d’extrêmité IPA fournis avec la PaaS 8](#_Toc77159453)

[Modèles et anti-modèles d’architecture 9](#_Toc77159454)

[Anti-modèle 1a : Transferts par lots 9](#_Toc77159455)

[Modèle 1b : Interfaces du programmation d’applications (IPA) 10](#_Toc77159456)

[Anti-modèle 2a : Connexion directe client-service 11](#_Toc77159457)

[Modèle 2b : Passerelle IPA (proxy inverse) 12](#_Toc77159458)

[Anti-modèle 3a : Passerelle IPA et pare-feu réseau 15](#_Toc77159459)

[Modèle 3b : Passerelle IPA avec pare-feu d’application Web 16](#_Toc77159460)

[Anti-modèle 4a : Modèle d’exploitation par étape pour les services de plateforme IPA 18](#_Toc77159461)

[Modèle 4a : Modèle d’exploitation pour les services de plateforme IPA 19](#_Toc77159462)

[Harmonisation avec les scénarios de connectivité du GC 21](#_Toc77159463)

[Cas d’utilisation 22](#_Toc77159464)

[Cas d’utilisation 1 : SaaS vers application hébergée dans le nuage du GC 22](#_Toc77159465)

[Cas d’utilisation 2 : Application hébergée du centre de données du GC vers application hébergée dans le nuage du GC 23](#_Toc77159466)

[Architectures de solutions du fournisseur de nuage 24](#_Toc77159467)

[Amazon Web Services 24](#_Toc77159468)

[Microsoft 26](#_Toc77159469)

[Oracle 27](#_Toc77159470)

[Références 28](#_Toc77159471)

# Aperçu

En avril 2020, le gouvernement du Canada a mis à jour la Directive sur les services et le numérique afin d’y inclure des procédures obligatoires pour les interfaces de programmation d’applications (IPA). L’accent mis sur les IPA est naturel; une économie de plateforme est née de l’externalisation des méthodes d’application, de sorte que d’autres plateformes et l’automatisation puissent accéder à ces méthodes dans l’ensemble du protocole http/s omniprésent et largement pris en charge. Cela fournit aux développeurs des architectures puissantes favorisant la communication entre les services à l’aide des technologies normalisées.

Tout comme l’interface graphique utilisateur (GUI) est la méthode par laquelle les utilisateurs humains accèdent aux applications, les IPA sont la façon dont d’autres systèmes (services) accèdent aux applications. Les IPA rendent l’automatisation possible.

L’architecture des applications du GC est en train de changer. Traditionnellement, nos données sensibles et nos systèmes étaient déployés dans un périmètre qui, pour la plupart, appartenait au GC et à ses entrepreneurs et qui était exploité par eux. L’intégration du système se limitait souvent à un centre de données ou à l’ensemble du réseau du GC.



Figure 1 : Vue traditionnelle du déploiement d’applications lorsque des données sensibles sont conservées dans le périmètre du GC

L’architecture des applications du GC couvre de plus en plus Internet. L’introduction de services infonuagiques et de référentiels de données Web fait basculer le GC vers une architecture où les services échangent des données à l’aide du protocole https sur Internet avec des points d’extrémité d’IPA. La poussée vers les services numériques conduit le GC à adopter des architectures qui rapprochent ces services de l’emplacement où nos utilisateurs y ont accès; Internet.



Figure 2 : Les données sensibles du GC se trouvent sur des services Internet

Ce document d’orientation vise à fournir aux développeurs et aux opérations une vue des architectures qui peuvent être utilisées pour activer les IPA. L’accent est mis sur les technologies d’interconnexion de systèmes ouverts de la couche 7 et l’Internet. Une boîte à outils omniprésente de services et de capacités a été mise à disposition par les fournisseurs de services infonuagiques (ainsi que les fournisseurs informatiques traditionnels) qui permettent aux IPA d’orchestrer les flux opérationnels sans se soucier des parties profondes de la pile technologique. Les fournisseurs de services infonuagiques gèrent ces services et les offrent aux consommateurs comme un modèle de PaaS (plateforme comme service). Ces plateformes natives du nuage sécurisent non seulement nos données, mais en raison de leur évolutivité, ajoutent de la résilience et de la disponibilité à nos services tout en fournissant un modèle de service qui permet aux architectes et aux développeurs de se concentrer sur les choix de configuration et de rester abstraits des activités sous-jacentes d’ingénierie d’infrastructure.

# Pourquoi une architecture axée sur les IPA?

Une approche axée sur les IPA consiste à mettre l’accent sur la couche d’application pour intégrer les applications et les services dans les réseaux Internet et du GC.

Si nous prenons une interaction typique d’un citoyen avec un service en ligne du GC comme l’assurance-emploi au moyen d’un portail de Service Canada, un utilisateur accède au portail à l’aide d’un navigateur Web sur Internet. La connexion entre le navigateur client et le portail est sécurisée par une session https chiffrée et l’utilisateur est authentifié. Des renseignements sensibles sont accessibles et mis à jour sur Internet.

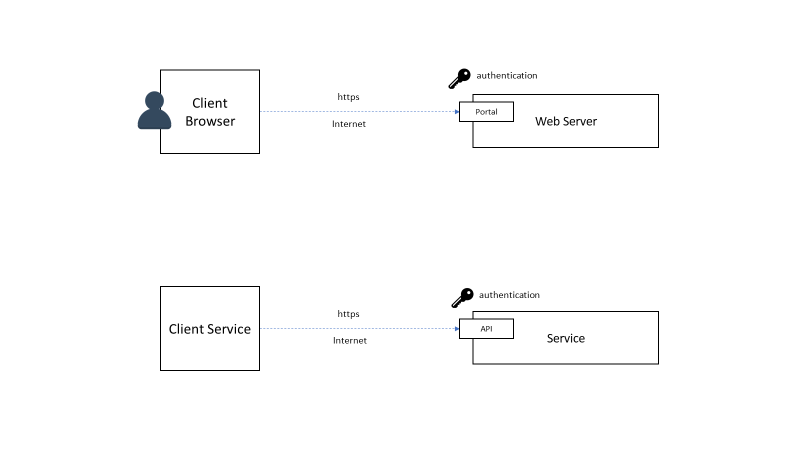


Figure 3 : Accès par l’utilisateur et mise à jour des données du GC sur Internet

Les IPA sont des points d’extrémité qui fournissent une expérience similaire pour l’accès et la mise à jour des renseignements dans l’application. Une application ou un service client remplace un utilisateur dans un navigateur Web. Au lieu d’accéder à une interface graphique au moyen d’un portail, un point d’extrémité d’IPA expose les fonctions d’accès et de mise à jour des données. C’est pourquoi une approche axée sur les IPA pour connecter les services infonuagiques sur Internet est l’approche préférée. Cette approche maintient la technologie nécessaire à l’échange de données entre les services de la couche d’application à l’aide de technologies omniprésentes comme l’Internet, le protocole https et les services de justificatifs d’identité.

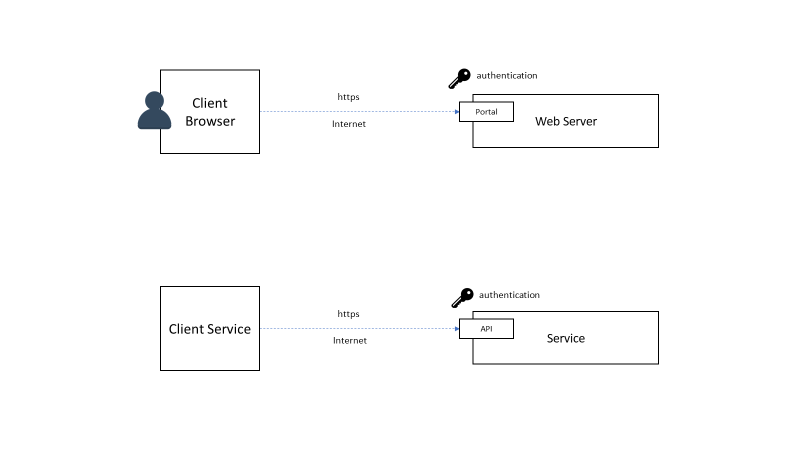


Figure 4 : Accès par le service ou l’application et mise à jour des données du GC sur Internet

# Modèles élaborés à partir de la collaboration

Le présent document a été élaboré en collaboration avec le Groupe de travail technique sur le nuage du GC en réponse à l’intérêt manifesté par ses membres pour l’établissement de pratiques exemplaires pour le déploiement des points d’extrémité d’IPA, et pour clarifier si des exigences politiques avaient une incidence sur la façon dont ces points d’extrémité sont déployés.

À la fin du printemps 2020, un premier projet a été créé par le Groupe de travail. Une ébauche du document a été affichée sur le forum de GCcollaboration du Groupe de travail. Au début de l’été, le document a été distribué aux fournisseurs de services infonuagiques admissibles à l’Entente-cadre sur les services infonuagiques de Services partagés Canada. On a invité ces fournisseurs ont été invités à fournir une présentation à une série de réunions du Groupe de travail technique sur le nuage à venir, au cours desquelles chaque fournisseur aurait une heure pour :

1. Formuler ses commentaires sur les modèles architecturaux pour toute correction et précision.
2. Fournir une architecture de solution à l’aide de leurs services qui s’harmonisent avec les modèles fournis dans ce document.

Oracle, Microsoft et AWS ont accepté l’invitation du Groupe de travail pour offrir une présentation. En fin septembre et octobre 2020, ces fournisseurs ont présenté leurs commentaires et leurs architectures de solution. On trouvera en annexe un résumé de ces architectures de solution. Ces architectures ne sont pas complètes et ne devraient pas être appliquées universellement pour chaque cas d’utilisation. Vous devriez plutôt consulter les documents des fournisseurs pour obtenir une couverture plus exhaustive du sujet.



En décembre 2020, le Réseau d’expertise sur le nuage et l’informatique a fourni et approuvé le présent document. En fin janvier 2021, la Communauté de pratique de l’architecture intégrée a approuvé le présent document. La publication définitive était en février 2021.

# Références aux politiques

Le gouvernement du Canada a publié des procédures obligatoires pour les interfaces de programmation d’applications (IPA). L’annexe B de la Directive sur les services et le numérique comprennent des [Procédures obligatoires sur les interfaces de programmation d’applications](https://www.tbs-sct.gc.ca/pol/doc-fra.aspx?id=32604). Ces procédures obligatoires mettent l’accent sur la façon dont les IPA doivent être élaborées et livrées.

|  |
| --- |
| *B.2.2.2 Élaborer les IPA en suivant le modèle Representational State Transfer (REST) (en anglais seulement) par défaut. REST est effectivement la norme pour l’intégration avec les services infonuagiques et est également la norme établie par la majorité des autres gouvernements ayant des programmes d’IPA bien établis.* |

# Références de l’architecture de sécurité

Le document [Modèles de conception de sécurité pour les systèmes d’information de SaaS](https://www.gcpedia.gc.ca/gcwiki/images/f/f4/GC_ESA_Security_Design_Patterns_for_SaaS-based_Solutions.pdf) inclut une superposition de sécurité pour les IPA. Le document met l’accent sur le SaaS (logiciel comme service), mais les parties du document qui portent sur les IPA peuvent être appliquées à tout modèle de service qui suit le même modèle. En effet, en limitant les interactions de service aux IPA, rend les services PaaS et IaaS, axés vers le public, identiques aux services IPA de SaaS. Remarque : La passerelle sécurisée dans le diagramme ci-dessous est la passerelle Internet organisationnelle hébergée dans le réseau du GC.

A screenshot of a cell phone

Description automatically generated

De plus, le document [Lignes directrices sur la sécurité des microservices et des conteneurs](https://github.com/canada-ca/platform-security_securite-de-plateforme/blob/master/en/5_Microservice_Security.md#api-security) fournit des exigences de sécurité pour la protection des points d’extrémité IPA. Certaines de ces mêmes mesures de protection se trouveront dans les modèles abordés dans le présent document, mais la ligne directrice fournit une liste consolidée et plus exhaustive.

# Points d’extrémité IPA fournis avec la PaaS

Le présent document porte sur les modèles axés sur les IPA à l’aide de la PaaS (plateforme comme service). La PaaS est le point de mire, car, comme le SaaS, les couches réseau ne sont pas gérées par le GC, mais par le fournisseur du nuage. C’est le fournisseur du nuage qui assure la gestion et la protection des couches réseau du service. Étant donné que le réseau, l’informatique et le stockage sous-jacents sont gérés par le fournisseur de services infonuagiques, le GC se concentre sur la protection des applications et, avec lui, les points d’extrémité des IPA.

Cela ne veut pas dire : cependant, l’IaaS ne tient pas compte de ces tendances. La PaaS peut servir à fournir une façade pour les applications déployées par IaaS. Lorsqu’il existe une façade PaaS, les modèles et les anti-modèles présentés dans le présent document s’appliquent toujours.

Figure 5 : la PaaS fournit une façade pour l’IaaS

Services infonuagiques

PaaS

IaaS

Réseau privé

Point d’extrémité d’API

Internet

# Modèles et anti-modèles d’architecture

Le présent document contient une collection de modèles et d’anti-modèles. Puisque les modèles peuvent favoriser une architecture optimale, les anti-modèles sont tout aussi utiles, car ils aident à éliminer certains choix architecturaux et à illustrer les faiblesses de ces choix.

Chaque modèle et chaque anti-modèle sont présentés avec des références des politiques et une architecture qui peut être appliquée à tout fournisseur de services infonuagiques qui possède les capacités de PaaS décrites dans le présent document. Les architectures de solution sont fournies spécifiquement à chaque fournisseur de services infonuagiques à la fin du document. Toutefois, ces architectures de solutions ne sont pas exhaustives. Le lecteur doit toujours consulter les références techniques du fournisseur de services infonuagiques pour obtenir une couverture plus exhaustive.

## Anti-modèle 1a : Transferts par lots

Dans cet anti-modèle, les renseignements sont regroupées en lot et transférées en un seul transfert asynchrone de transactions.



Figure 6 : Anti-modèle — transfert par lots

Pourquoi est-ce un anti-modèle?

Les transferts par lots ne fournissent pas de méthode normalisée pour accéder aux données dans les applications. Même s’ils ont fonctionnés pendant des décennies, ils ne sont pas optimisés pour un environnement axé sur l’IPA. Ils ne s’adaptent pas à une architecture Internet. L’autorisation et l’authentification ne sont souvent pas normalisées. Les processus d’extraction, de transformation et de chargement sont souvent nécessaires et ne fournissent pas de données en temps réel.

Pour ces raisons, les transferts par lots sont considérés comme un anti-modèle.

## Modèle 1b : Interfaces du programmation d’applications (IPA)



Figure 7 : Modèle — Interface de programmation d’applications

Les IPA fournissent une architecture moderne permettant d’accéder aux méthodes et aux données dans les applications, les services et les plateformes. Elles sont omniprésentes pour les services à l’échelle d’Internet. Les fournisseurs de nuage offrent une suite de services et d’architectures de plateforme pour prendre en charge une architecture d’IPA. Le gouvernement du Canada a publié des procédures obligatoires pour l’intégration des IPA. L’annexe B de la Directive sur les services et le numérique comprennent des [Procédures obligatoires sur les interfaces de programmation d’applications](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32604).

|  |
| --- |
| *B.2.2.2 Élaborer les IPA en suivant le modèle Representational State Transfer (REST) (en anglais seulement) par défaut. REST est effectivement la norme pour l’intégration avec les services infonuagiques et est également la norme établie par la majorité des autres gouvernements ayant des programmes d’IPA bien établis.* |

## Anti-modèle 2a : Connexion directe client-service

Dans ce cas, le client communique directement avec chaque service.



Figure 8 : Anti-modèle — direct entre le client et le service

Pourquoi est-ce un anti-modèle?

Dans ce cas, le client communique avec chaque service, de façon individuelle. Chaque service peut nécessiter une ou plusieurs des capacités suivantes : authentification, autorisation, facturation, etc. Dans l’anti-modèle ci-dessus, ces capacités communes ont été intégrées dans les services individuels. En tant que pratique exemplaire, ces capacités communes doivent être découplées de la logique opérationnelle. Ces capacités ne font pas partie de la logique opérationnelle exécutée par le service, mais sont plutôt nécessaires pour gérer les interactions entre le service et le client. Le client peut également être tenu d’accéder à plusieurs services avec plusieurs localisateurs de ressources uniformes (URL). La mise en place d’une couche de découplage entre le client et les services peut favoriser une souplesse accrue, comme l’ajout d’une compatibilité descendante à mesure que les versions de l’IPA changent.

## Modèle 2b : Passerelle IPA (proxy inverse)

Les capacités communes sont regroupées en un seul proxy inverse qui est une façade pour tous les services. Le client n’interagit pas directement avec chaque service, mais plutôt avec une passerelle IPA qui est un proxy inverse pour tous les services. Les fournisseurs de services infonuagiques offrent des fonctionnalités de passerelle IPA en tant que modèle de PAAS où l’infrastructure sous-jacente, y compris l’ordinateur, le stockage et le réseautage, est gérée par les fournisseurs de services infonuagiques. Le modèle ci-dessous suppose qu’une PaaS livre un modèle pour la passerelle IPA. La prestation en tant que modèle de service IaaS n’est pas recommandée, car elle exige un fardeau opérationnel plus important, notamment la gestion des correctifs, l’évolutivité et la sécurité des composants de l’infrastructure.

Extrait de l’Annexe B — Procédures obligatoires pour les interfaces de programmation d’applications :

|  |
| --- |
| *B.2.2.5 Appliquez les communications sécurisées en veillant à ce que les données de nature délicate ne soient jamais envoyées au moyen d’une connexion non sécuritaire ou non chiffrée, et dans la mesure du possible, les données non délicates devraient aussi être envoyées au moyen d’une connexion sécurisée. Activez la version TLS 1.2 ou les versions ultérieures, conformément aux lignes directrices du Centre de la sécurité des télécommunications (CST).*  *B.2.2.5.6 Utilisez des passerelles et des données de substitution plutôt que des listes blanches lorsque vous exposez des IPA à Internet.* *Utilisez une couche de passerelle sécurisée pour fournir un point de contrôle de sécurité au lieu de simplement envoyer une liste blanche d’adresses de protocole Internet (IP) entrant. La fonctionnalité de passerelle du magasin d’IPA peut servir. Lorsque vous utilisez des IPA externes, la route passe par des mandataires (sortie) au lieu d’utiliser une liste blanche d’adresses IP sur le pare-feu sortant.*  *B.2.2.5.4 Protégez l’accès aux IPA en mettant en œuvre un système de contrôle de l’accès qui empêche la mauvaise innovation des IPA, y compris les références non autorisées aux fonctions et aux données. Assurez-vous toujours de vous authentifier et d’avoir ou donner les autorisations nécessaires avant toute opération pour limiter l’accès aux IPA aux personnes et/ou aux systèmes autorisés. Utilisez des normes ouvertes, telles que OpenID Connect et Open Authorization 2.0 (OAuth 2.0) pour les IPA RESTful et le standard Security Assertion Markup Language 2.0 (SAML 2.0) pour les IPA SOAP. Assurez-vous que la clé/le code secret de l’IPA sont correctement protégés. Les IPA doivent être sécurisées à l’aide d’une clé IPA pour permettre le suivi de l’utilisation, mais aussi pour permettre d’identifier et de prévenir toute utilisation malveillante potentielle. Les IPA de données ouvertes doivent être sécurisées à l’aide d’une clé IPA pour permettre le suivi de l’utilisation, mais aussi pour permettre d’identifier et de prévenir toute utilisation malveillante potentielle.*  *B.2.2.5.9 Consignez et surveillez le rendement et l’activité en faisant le suivi de l’utilisation et de la surveillance des activités suspectes anormales y compris des tendances d’accès anormal comme les demandes après les heures normales, les demandes de données volumineuses, entre autres. Utilisez des normes d’enregistrement dans les journaux (p. ex., format d’événement commun) et intégrez les journaux de manière centralisée. Relevez les dépendances et surveillez les vulnérabilités, en particulier celles des temps d’exécution téléchargés qui fonctionnent comme composante de l’IPA. Les événements suspects doivent être transmis à la fonction ou à l’autorité compétente en matière d’opérations de sécurité, conformément aux politiques du gouvernement du Canada en matière de cybersécurité et au Plan de gestion des événements de cybersécurité du gouvernement du Canada.* |



Figure 9 : Modèle — Proxy inverse avec passerelle IPA

Les passerelles IPA offrent les fonctionnalités suivantes :

L’**authentification** est le contrôle de la tentative de connexion. Le client fournit des justificatifs d’identité qui sont vérifiés avant l’octroi de l’accès. Ces justificatifs d’identité peuvent être en texte clair (non recommandé) ou chiffrés. Les normes OAuth 2.0 et SAML sont suggérées dans les procédures obligatoires pour les IPA.

L’**autorisation** est l’octroi de l’accès au service. L’authentification vérifie que la connexion du client est autorisée; elle vérifie les services et les méthodes autorisés par le client.

L’**arrêt SSL** est le processus de conversion des renseignements chiffrés du client en texte clair aux fins de traitement.

**Routage** de la connexion client vers différents services en fonction de l’adresse URL fournie.

Par exemple, [https://domaine.com/paiement](https://domain.com/payment) acheminera les interactions client vers le service de paiement, alors que [http://domaine.com/panier](http://domain.com/cart) acheminera les interactions client vers le service panier. Ces services peuvent être déployés à l’aide d’architectures complètement différentes, mais pour le client ces complexités sont abstraites, car la passerelle IPA fournit le routage nécessaire.

**Regroupement** de plusieurs appels de service en un seul appel de service. Cela permet de réduire la quantité de bavardage entre le client et les services.

La **mise en cache** de méthodes dont on fait couramment appel peut réduire le traitement requis par les services administratifs tout en améliorant la réponse destinée aux clients. On peut régler l’expiration du cache pour forcer une actualisation du cache.

L’**équilibrage de charge** des demandes de service lorsque l’exécution d’un service ne se trouve pas dans une fenêtre indiquée peut être acheminé entre plusieurs instances de ce service. L’équilibrage de charge est également un moyen efficace d’effectuer des déploiements bleus/verts et des déploiements de contrôle de validité.

La **conversion de protocole** permet aux clients d’utiliser un protocole, par exemple HTTP v1 pour effectuer une requête, même si le service n’accepte que le protocole HTTP v2.

L’**analyse de la télémétrie** est une capacité essentielle pour surveiller une alerte en fonction des mesures de sécurité, financières et de rendement.

La **facturation** de l’utilisation de l’IPA ou l’attribution des coûts aux utilisateurs en fonction de l’utilisation est un modèle opérationnel courant.

## Anti-modèle 3a : Passerelle IPA et pare-feu réseau

Dans cet anti-modèle, tout le trafic est acheminé au moyen d’un pare-feu de nouvelle génération (déployé dans un environnement IaaS hébergé sur des machines virtuelles [MV]) avant d’être consommé par un point d’extrémité IPA sur la passerelle IPA.

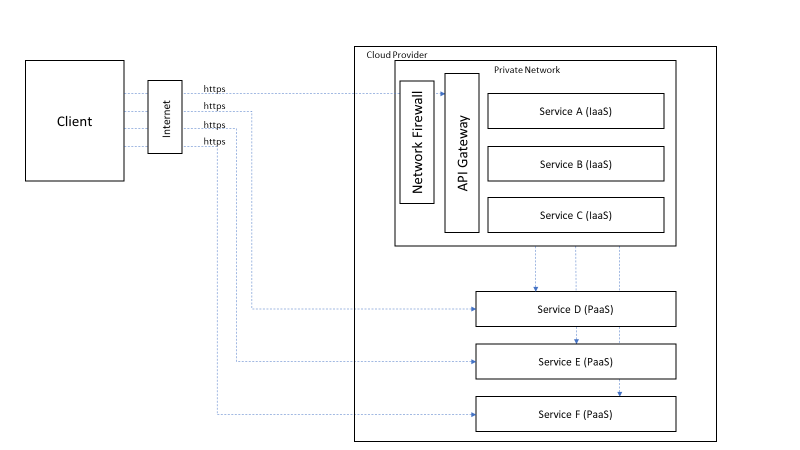


Figure 10 : Anti-modèle — Passerelle IPA avec pare-feu réseau

Pourquoi est-ce un anti-modèle?

Les pare-feu réseau sont conçus pour protéger les infrastructures comme les serveurs, mais pas nécessairement les applications ou les clients. Les pare-feu réseau se concentrent sur l’inspection du trafic des couches 3 et 4 OSI et ne connaissent pas les menaces propres au protocole HTTP/S et aux applications comme l’injection de code SQL et le script de site à site. Les pare-feu réseau prennent en charge de nombreux protocoles; toutefois pour les IPA, le seul protocole utilisé est HTTP/S. La protection DDoS se limite à la protection du réseau, pas nécessairement à la protection de la disponibilité de l’application. Les fonctionnalités d’un pare-feu de nouvelle génération sont redondantes avec les services fournis par un fournisseur de services infonuagiques lorsqu’une passerelle IPA PaaS est déployée. Le fournisseur de services infonuagiques protège les couches réseau de la plateforme.

Dans un environnement infonuagique, les pare-feu réseau sont déployés comme des MV dans un modèle de service IaaS. Ces MV sont contenues dans un sous-réseau privé et sont limitées à une région à moins que MV ne soient déployées sur plusieurs régions. Les pare-feu d’application Web et les passerelles IPA sont des PaaS et peuvent évoluer pour être presque illimités. Cela offre un niveau de résilience et de disponibilité supérieur à celui d’une architecture qui comprend des dispositifs de pare-feu. Dans un modèle PaaS, le fournisseur de services infonuagiques fournit des protections de sécurité nécessaires au niveau du réseau. L’objectif du GC est de protéger le point d’extrémité de l’IPA et de créer des applications qui tiennent compte de menaces courantes comme l’injection de code SQL.

## Modèle 3b : Passerelle IPA avec pare-feu d’application Web

L’ajout d’un pare-feu d’application Web offre des services à une disponibilité élevée tout en protégeant ces services et les clients contre les menaces courantes. Ce modèle s’appuie sur les capacités d’authentification et d’autorisation d’une passerelle IPA avec des mesures de protection supplémentaires pour les applications et les services pour lesquels la passerelle est un proxy inverse. Les fournisseurs de services infonuagiques offrent des fonctionnalités de pare-feu d’application Web en tant que modèle de PaaS où l’infrastructure sous-jacente, y compris l’ordinateur, le stockage et le réseautage, est gérée par les fournisseurs de services infonuagiques. Le modèle ci-dessous ne s’appliquerait pas lorsque les capacités de pare-feu d’application Web sont fournies en tant qu’IaaS, puisque la gestion de réseau privé virtuel sous-jacente incombe toujours au GC.

Extrait de l’Annexe B — Procédures obligatoires pour les interfaces de programmation d’applications :

|  |
| --- |
| *B.2.2.5.2 Concevez des IPA qui résistent aux attaques en veillant à ce que toutes les IPA soient conçues et mises en œuvre pour résister aux attaques communes d’lPA comme les dépassements de mémoire tampon et l’injection SQL. Traitez toutes les données soumises comme non fiables et validez-les avant de les traiter. Exploitez les schémas et les modèles de données pour assurer la validation correcte des données.* |

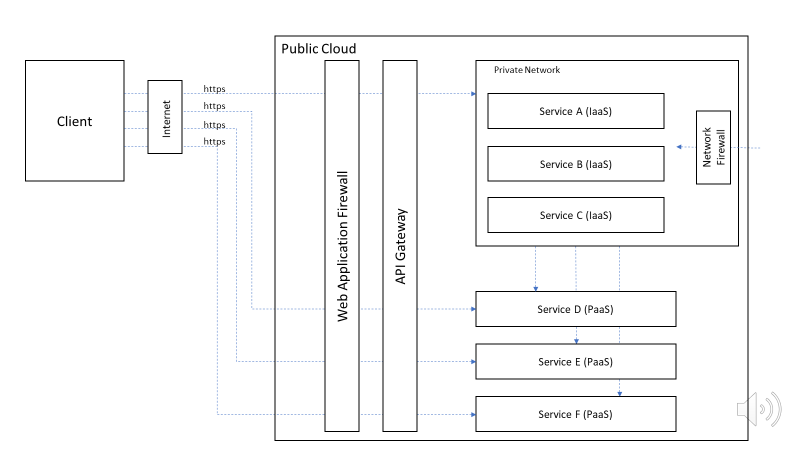


Figure 11 : Modèle — Services derrière un pare-feu d’application Web et une passerelle IPA

Fonctionnalités du pare-feu d’application Web comme axé sur la protection contre de nombreux risques parmi les [10 principaux risques de sécurité Web OWASP](https://owasp.org/www-project-top-ten/). Un pare-feu d’application Web peut augmenter les mesures de protection de la passerelle IPA en fournissant une méthode temporaire de résolution des défaillances constatées dans le code des applications. Par exemple, si une ancienne application est vulnérable aux injections de code SQL, on peut utiliser le pare-feu d’application Web pour fournir ces mesures de protection jusqu’à ce que l’ancien code des applications puisse être remanié. Par conséquent, un pare-feu d’application Web est plus efficace entre les mains d’un développeur qui connait le fonctionnement de l’application. Certains diraient qu’avec un test de code approprié, un pare-feu d’application Web n’est pas nécessaire, car les vulnérabilités seront trouvées et corrigées avec un test approprié. Les pare-feu d’application Web, lorsqu’ils sont livrés en tant que PaaS infonuagique, offrent aux développeurs les capacités suivantes :

* Protection contre les attaques par injection de code SQL.
* Protection contre les scripts de site à site.
* Protection contre les modifications de session ou de paramètre.
* Permet aux développeurs d’ajouter des inspections propres à une application
* Inspection du trafic chiffré SSL (HTTPS).
* Protection contre le déni de couche d’application et les attaques par déni de service distribué (DDoS).
* Fournit la validation du schéma XML
* Bloque le contenu XML malveillant

## Anti-modèle 4a : Modèle d’exploitation par étape pour les services de plateforme IPA

Il convient d’éviter les modèles opérationnels qui introduisent des barrières et le soutien de travail entre les équipes. Traditionnellement, l’équipe de la TI est organisée en cloisons fonctionnels axés sur la spécialisation, avec un soutien entre ces équipes pour déployer une solution complète. L’application de ce modèle traditionnel à la prestation d’IPA sur la passerelle IPA, le pare-feu d’application Web et les plateformes du réseau de diffusion de contenu ralentira le rythme de prestation, les processus complexes de gestion des services et la livraison intensive des personnes. Étant donné que ces capacités sont fournies par le biais de la PaaS, il n’y a pas lieu de s’inquiéter de l’expansion de ces capacités. Au lieu de cela, l’accent devrait être mis sur la gestion des configurations de ces capacités de plateforme.

On doit éviter un modèle de livraison par étape, en cascade.



## Modèle 4a : Modèle d’exploitation pour les services de plateforme IPA

Le modèle d’exploitation pour la fourniture de plateformes IPA est essentiel pour s’assurer que les développeurs peuvent fournir de nouvelles IPA et des changements avec rapidité sans compromettre la sécurité, la fiabilité ou la qualité.

Extrait des Procédures obligatoires pour les interfaces de programmation d’applications :

|  |
| --- |
| *D.2.2.1.2 Permettez au personnel d’offrir de meilleurs services en effectuant ce qui suit :*  *D.2.2.1.2.1 Veillez à ce que les outils, la formation et les processus nécessaires soient en place pour appuyer un processus robuste et souple d’élaboration et de gestion du cycle de vie des API.*  *D.2.2.1.2.2 Adoptez des pratiques d’intégration et de prestation continues (CI/CD) et de développement axé sur les essais (DAE) appuyées par des outils d’automatisation et des essais de sécurité intégrés.* *Cela constitue la base de l’adoption de DevOps à mesure que la maturité s’améliore.* |

Dans un environnement infonuagique, la passerelle IPA et le pare-feu d’application Web comme services de plateforme. La plateforme elle-même est gérée par le fournisseur de services infonuagiques. Les développeurs déploient des configurations sur la plateforme pour prendre en charge leurs applications, généralement au moyen d’un pipeline. Les opérations travaillent avec la gouvernance pour déployer les stratégies requises pour que tous les développeurs puissent les suivre ainsi que pour surveiller les scénarios à haut risque. Ces stratégies peuvent supprimer les options de configuration à haut risque. Voici des exemples de stratégiques qui pourraient être appliquées :

* Toutes les IPA doivent être enregistrées dans une passerelle IPA
* Toutes les passerelles IPA doivent être connectées à un pare-feu d’application Web
* Toutes les IPA nécessitent une authentification (peut-être une technologie d’authentification précise)
* Toutes les IPA doivent utiliser le protocole https
* Tous les pare-feu doivent inclure un ensemble de règles clés

La description ci-dessous ne doit pas être considérée comme des « exemples » de capacités communes pour chaque application, mais plutôt comme un ensemble commun de plateformes. Chaque application peut nécessiter une configuration unique de la plateforme adaptée à son but. En outre, les opérations peuvent mettre en œuvre une configuration de base commune sur toutes les plateformes.

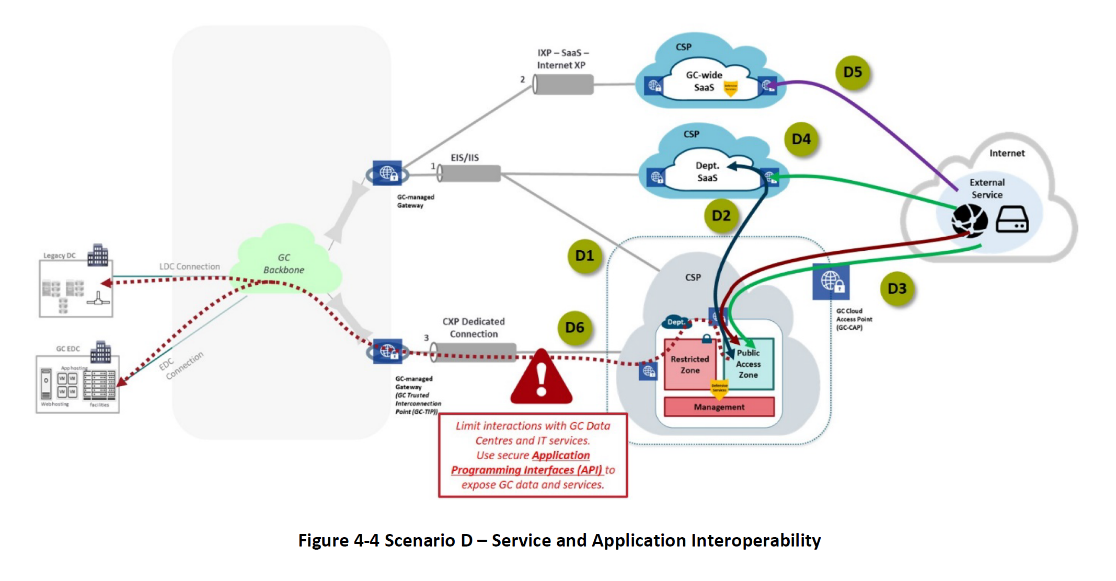


# Harmonisation avec les scénarios de connectivité du GC

Afin d’aider les ministères du GC à décrire leurs modèles de connectivité, la CEAI GC a approuvé un ensemble de [scénarios de connectivité](https://www.gcpedia.gc.ca/gcwiki/images/e/e7/GC_Secure_Cloud_Connectivity_Requirements.pdf). L’intégration d’applications ou de services informatiques hybrides (infonuagiques et sur place) relève du scénario D. Pour ceux qui orchestrent les interactions d’IPA sur Internet, entre les IPA publiques, mais sécurisées, sur place et celles dans le nuage, D1 s’applique lorsque tout le trafic traverse le Service Internet d’entreprise (SIE) du GC. Pour ceux qui orchestrent le même scénario sur CXP, le scénario D6 s’applique.

Le point d’accès au nuage (PAN) est élaboré pour les scénarios d’IaaS, car la PaaS est hors de la portée de l’initiative d’Activation et défense du nuage sécurisé (ADNS). Étant donné que les points d’extrémité IPA reposent sur des fonctionnalités de passerelle IPA comme le filtrage IP, mais plus important encore, l’identité pour authentifier et autoriser l’accès au point d’extrémité, le routage du trafic au moyen du PAN n’est pas nécessaire. À l’aide de modèles de déploiement PaaS, mettez la couche réseau de la passerelle IPA et du pare-feu d’application Web sous la gestion du fournisseur de services infonuagiques. Au moment de la rédaction du présent document, les services minimaux suivants sont recommandés :

* Contrôle d’accès
* Journalisation et surveillance
* Audit
* Services de cyberdéfense (CIN/CNH du CCCS)
* *Des services supplémentaires peuvent être requis selon le profil de risque (par exemple, si les flux Internet sont activés).*

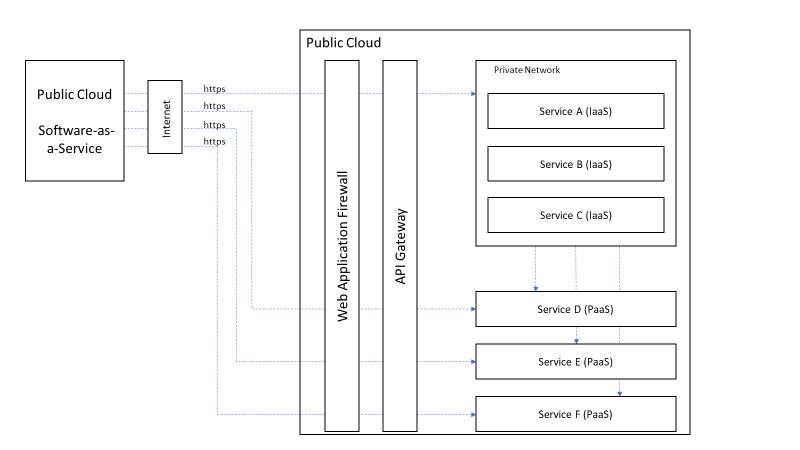


# Cas d’utilisation

## Cas d’utilisation 1 : SaaS vers application hébergée dans le nuage du GC

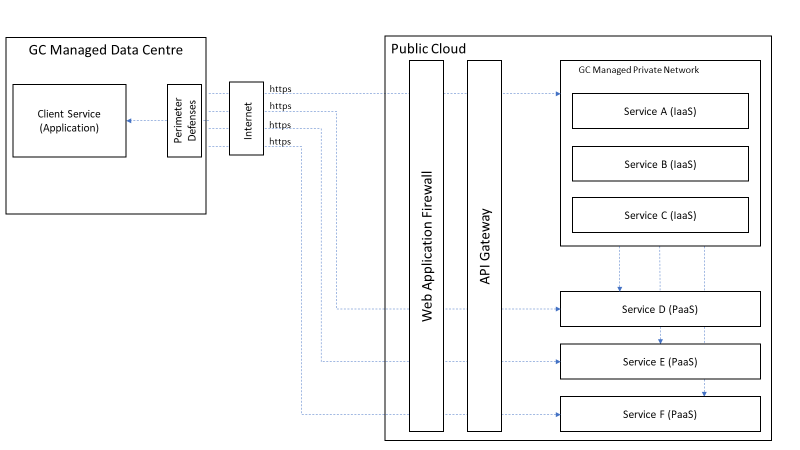
On peut employer des méthodes de SaaS dans le nuage public à l’extérieur au moyen des IPA. De même, le SaaS peut avoir besoin d’invoquer des IPA externes pour achever le traitement. Par exemple, dans un flux de travail, des renseignements provenant d’un autre système d’enregistrement peuvent être nécessaires pour achever le traitement.

Dans ce scénario, le SaaS invoque des méthodes pour plusieurs services hébergés par le GC dans un environnement infonuagique public. Ces services peuvent être fournis au moyen de solutions IaaS, par exemple des MV exécutant un produit LCPE, ou utilisant des services PaaS comme une application de microservices architecturée à l’aide d’une plateforme de fonction comme service.



## Cas d’utilisation 2 : Application hébergée du centre de données du GC vers application hébergée dans le nuage du GC

Dans ce scénario, une application hébergée dans un centre de données géré par le GC doit invoquer les méthodes d’une application ou d’un service hébergé dans un nuage public et vice versa. Il s’agit d’un cas d’utilisation informatique hybride où la seule connectivité entre les applications est fondée sur l’IPA sur le protocole https. Une passerelle IPA et un pare-feu d’application Web sont requis dans le centre de données et le nuage public.



# Architectures de solutions du fournisseur de nuage

## Amazon Web Services

L’équipe d’Amazon Web Services (AWS) a présenté son architecture générique pour les modèles d’architecture axés sur l’IPA. Elle a ensuite fourni un exemple de modèle et d’anti-modèle. AWS suggère le [livre blanc](https://d1.awsstatic.com/whitepapers/AWS_Serverless_Multi-Tier_Architectures.pdf) suivant pour expliquer plus en détail comment le service AWS peut activer les modèles axés sur l’IPA.

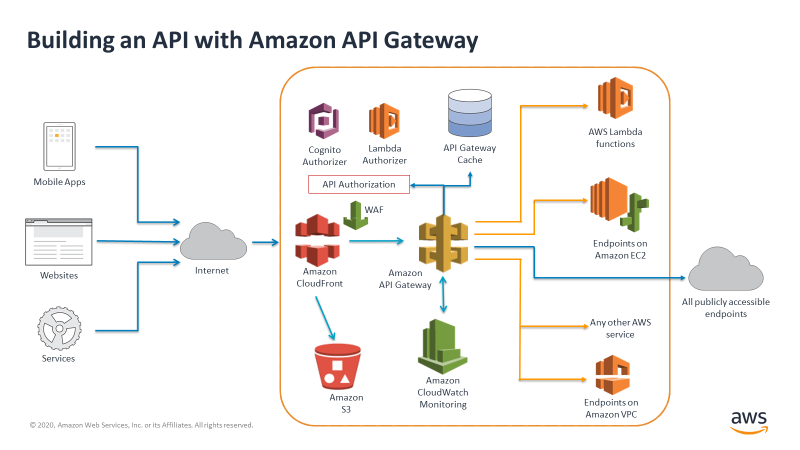


Figure 12 : Approche « générique » d’AWS pour les architectures axées sur l’IPA

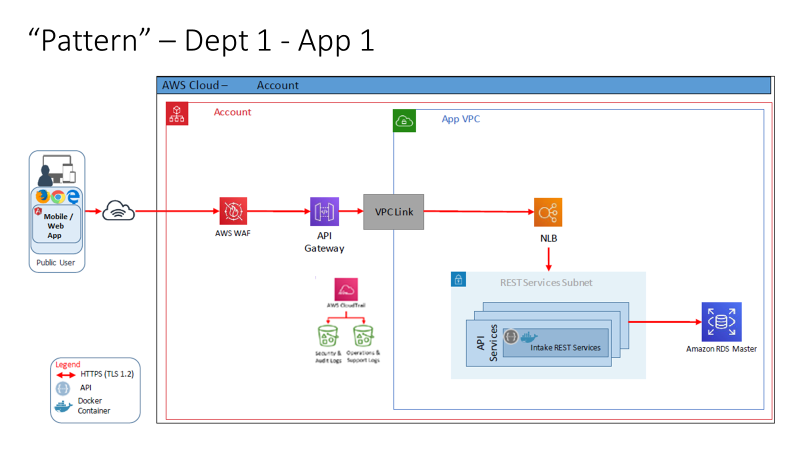


Figure 13 : Exemple d’AWS d’un modèle axé sur l’IPA

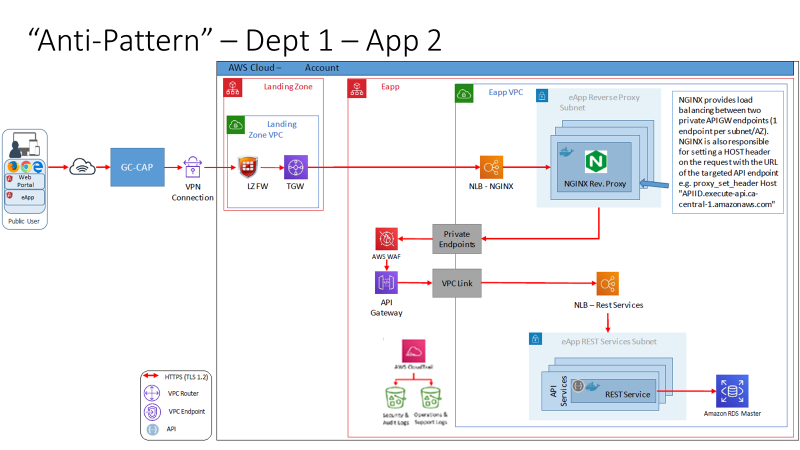
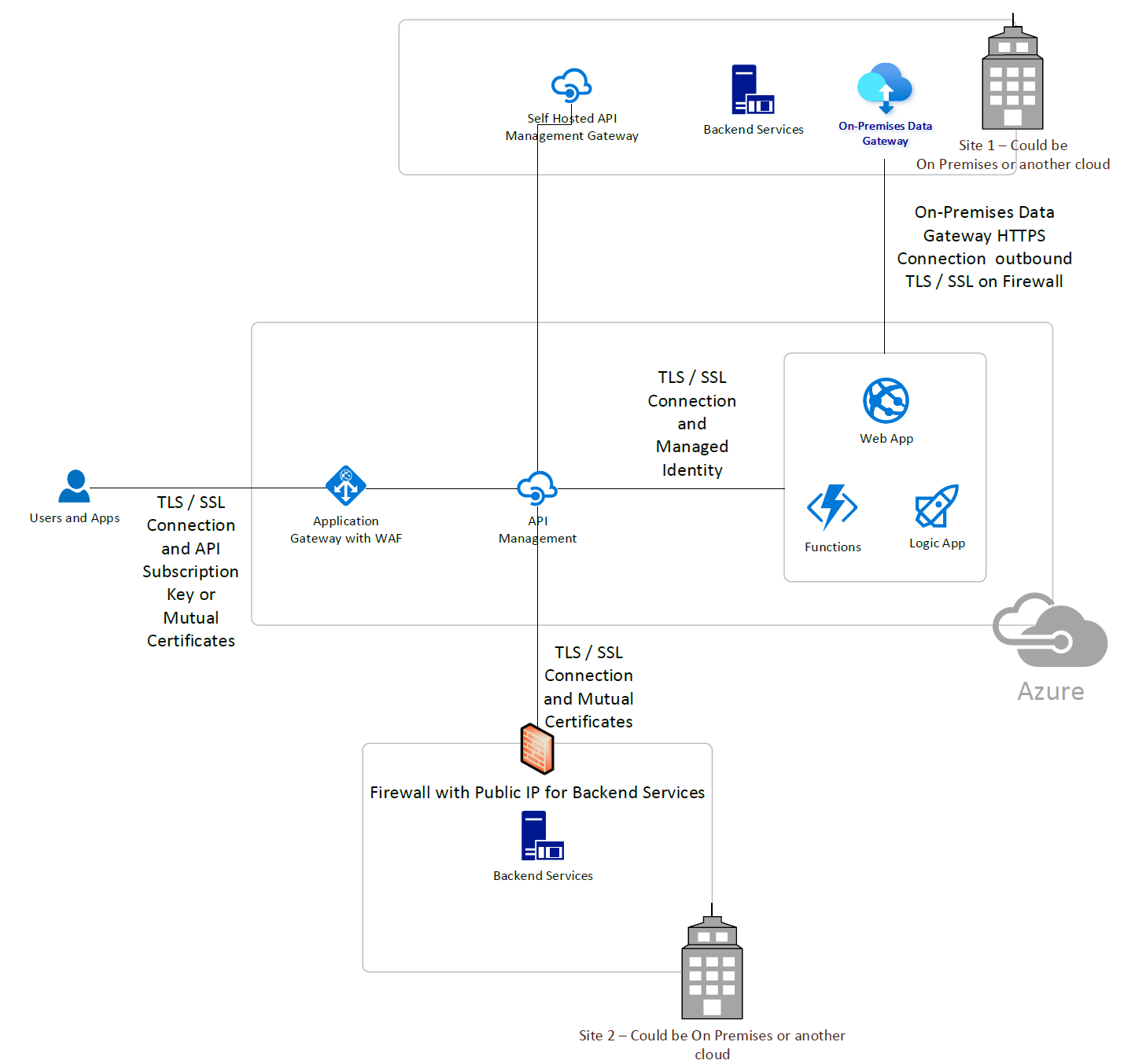


Figure 14 : Exemple d’AWS d’un anti-modèle en raison de la complexité et de la faible disponibilité

## Microsoft

Microsoft a proposé son architecture de solution pour les modèles axés sur l’IPA. Microsoft propose un produit à installer sur place appelé « Data Gateway » qui se connecte directement avec les applications Web. Par ailleurs, le modèle plus normalisé de déploiement d’une passerelle IPA sur place peut également être utilisé pour les modèles informatiques hybrides.



## Oracle

Oracle a présenté son architecture de solution générique pour les modèles axés sur l’IPA. Ils ont également créé un livre blanc [Oracle Cloud Infrastructure Serverless Multi-Tier Architectures](https://056gc-my.sharepoint.com/personal/slevac_tbs-sct_gc_ca/Documents/Oracle%20Cloud%20Infrastructure%20Serverless%20Multi-Tier%20Architectures) (https://bit.ly/2TmHhku).

Il existe également un laboratoire (https://bit.ly/3moNpoy) qui fournit un guide étape par étape sur la mise en œuvre de l’architecture décrite dans le document.

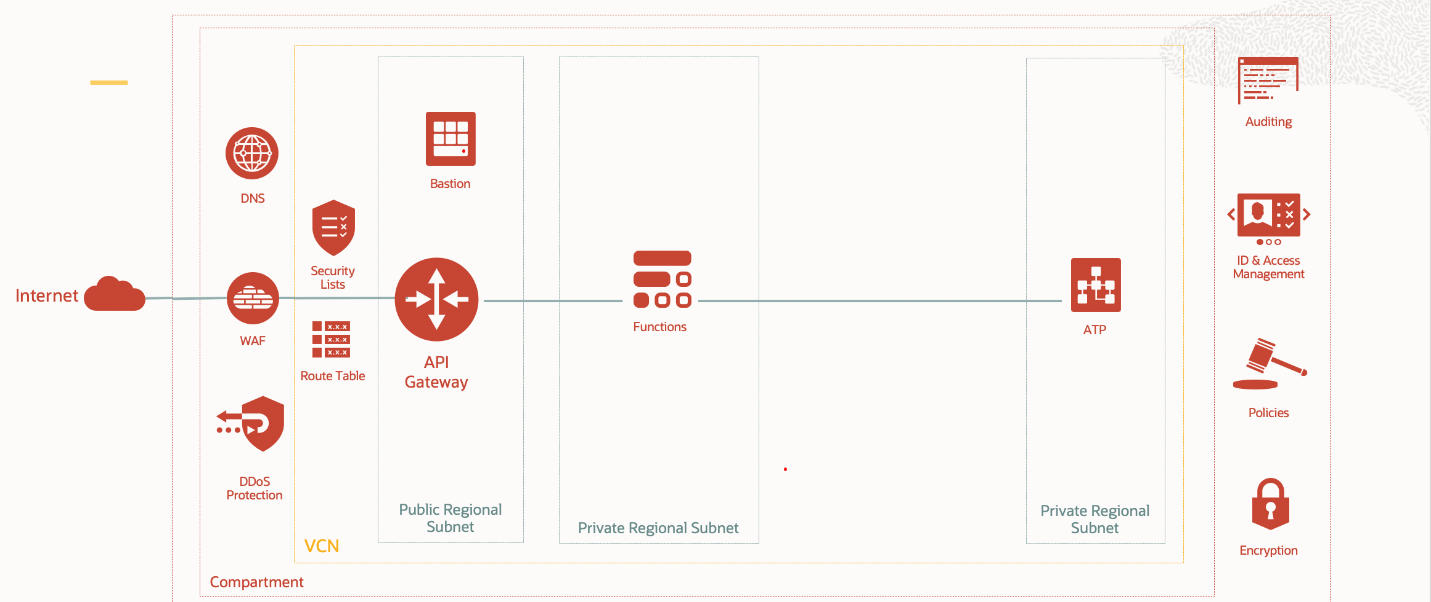


Figure 15 : Architecture de solution axée sur l’IPA d’Oracle OCI

# Références

[The API Gateway Pattern](https://manningbooks.medium.com/the-api-gateway-pattern-cd8af792084)

[Procédures obligatoires pour les interfaces de programmation d’applications](https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=15249&section=procedure&p=D)

[Exigences en matière de connectivité au nuage sécurisé du GC](https://www.gcpedia.gc.ca/gcwiki/images/e/e7/GC_Secure_Cloud_Connectivity_Requirements.pdf)

[Modèles de conception de sécurité pour les systèmes d’information de SaaS](https://www.gcpedia.gc.ca/gcwiki/images/f/f4/GC_ESA_Security_Design_Patterns_for_SaaS-based_Solutions.pdf)

[Lignes directrices sur la sécurité des microservices et des conteneurs](https://github.com/canada-ca/platform-security_securite-de-plateforme/blob/master/en/5_Microservice_Security.md#api-security)

Guide de modernisation des applications : [Création d’applications modernes à l’aide des services de plateforme](https://wiki.gccollab.ca/images/b/bc/01_Building_Modern_Applications_Using_Platform_Services_EN.pdf)