
SCHÉMA DE SÉCURITÉ DU CLOUD 2.0

# ARCHITECTURES ET SOLUTIONS

# Table des matières

# Introduction

Dans la Présentation du schéma de sécurité du Cloud 2.0, nous avons abordé les concepts de base (modèle de responsabilité partagée, zéro confiance) ainsi que les défis avancés que doit relever une architecture moderne de sécurité du Cloud. Ces défis comprennent l'extension des surfaces d'attaque, la réduction de la visibilité, les charges de travail dynamiques et éphémères, les processus de DevOps automatisés, les privilèges excessifs et les multiples environnements dans le Cloud.

Nous avons ensuite décrit les principes architecturaux de la sécurité dans le Cloud qui sont essentiels pour relever efficacement ces défis. Ces principes comprennent :

- Protection avancée contre les menaces au niveau du périmètre du réseau
- Sécurisation d'autres vecteurs d'attaque tels que les identités, les contrôles et les données
- Sécurité dès la conception : concevoir l'architecture de manière à ce que la sécurité soit un composant de l'environnement même, en plus des contrôles s'appuyant sur des configurations
- Segmentation pour minimiser les surfaces d'attaque et réduire le rayon d'action des infections
- Agilité, automatisation, élasticité sans compromettre la sécurité
- Absence de frontières, indépendamment des spécificités des Clouds

Dans ce second livre blanc, nous abordons les architectures et les solutions du schéma de sécurité du Cloud 2.0.

Nous présentons tout d'abord les solutions de sécurité de Check Point pour le Cloud, CloudGuard IaaS, CloudGuard Dome9 et CloudGuard Log.ic, qui peuvent être utilisées pour des déploiements sécurisés dans le Cloud. Nous précisons ensuite comment ces solutions répondent aux défis de la sécurité du Cloud, et les principes architecturaux introduits dans le premier livre blanc.

# CloudGuard IaaS : Prévention avancée des menaces et sécurité réseau dans le Cloud

Check Point CloudGuard IaaS (CGI) fournit une prévention avancée des menaces pour les applications et les données dans les Clouds privés, publics et hybrides. CGI est essentiellement similaire aux passerelles de sécurité de Check Point pour les appareils physiques, mais la solution est adaptée et configurée spécifiquement pour les déploiements dans les Clouds et les Datacenters logiciels. Les principales fonctionnalités et les principaux avantages de l'utilisation de CloudGuard IaaS sont les suivants :

- **Prévention multicouche de haut niveau contre les menaces pesant sur les infrastructures dynamiques et élastiques dans le Cloud :** Protège les services et les applications dans le Cloud contre les accès non autorisés et les attaques de déni de service, fournit une connectivité sécurisée aux ressources dans le Cloud, applique une authentification à deux facteurs pour l'accès mobile, empêche les fuites de données et protège contre les logiciels malveillants et les attaques zero-day.
- **Absence de frontières :** Fonctionne avec de nombreux prestataires de services de Cloud public (AWS, Azure, GCP, etc.) et de prestataires de solutions pour Datacenters logiciels (VMware NSX, Microsoft Hyper-V, Openstack, Cisco ACI, Nuage Networks, etc.)
- **Déploiement rapide :** Disponible sur les principales places de marché de Cloud public, et prenant en charge les modèles de tarification PAYG (coût à mesure de l'évolution) ou BYOL (utilisation de ses propres licences), le déploiement et la configuration des passerelles CloudGuard ne prennent que quelques minutes. Des modèles et des workflows propres aux prestataires et autorisés par le département informatique peuvent être utilisés pour assurer une homogénéité avec l'écosystème de sécurité de l'entreprise.
- **Agilité grâce à des politiques dynamiques et automatisées :** S'intégrant avec les principales solutions d'administration des Clouds publics, CloudGuard IaaS garantit la mise à jour en temps réel de tous les éléments définis dans le Cloud, tels que le marquage des actifs, les objets et les groupes de sécurité. Les politiques de sécurité sont alors automatiquement ajustées aux changements se produisant dans le Cloud. De cette façon, les équipes de développement et les équipes métiers peuvent provisionner et consommer des ressources dans le Cloud sans compromettre la sécurité de l'entreprise.
- **Administration centralisée des infrastructures dans le Cloud et sur site :** Application d'une politique de sécurité cohérente à partir d'une console d'administration unique, visualisation des événements de sécurité dans des environnements complexes et corrélation des événements avec les applications et les politiques.
- **Journaux et rapports consolidés :** Visibilité de bout en bout et investigations améliorées grâce à des journaux et des rapports consolidés pour les Clouds hybrides.

# Présentation du modèle en étoile

Lors de la conception d'un environnement sécurisé dans le Cloud avec CloudGuard IaaS, il est fortement recommandé d'utiliser le modèle en étoile qui a été introduit dans le schéma 1.0. Afin de mettre en œuvre les principes architecturaux de sécurité du Cloud déjà décrits, l'environnement est implémenté dans ce modèle sous forme de système de connexions ressemblant à une roue de vélo, dans lequel tous les rayons sont reliés à un courtier central (nœud) et la totalité du trafic vers et depuis les rayons passe par un courtier. Le schéma peut être conçu pour un seul ou plusieurs nœuds, comme le montre la Figure 1.

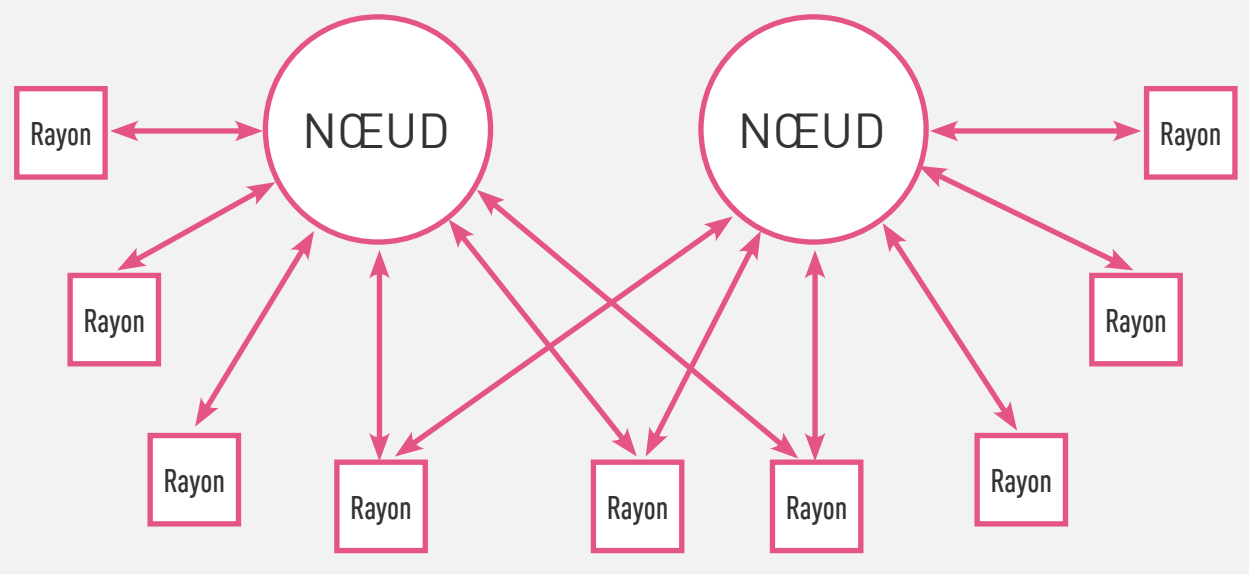


**Figure 1 : Modèle en étoile (à plusieurs nœuds)**

## Les rayons

Un rayon est un environnement réseau isolé contenant un ensemble d'un ou plusieurs sous-réseaux à partir desquels des charges de travail peuvent être installées et exécutées. Un cas d'utilisation courant est celui de plusieurs serveurs virtuels, qui constituent ensemble une pile applicative (c.-à-d. web, application et base de données). Un autre cas d'utilisation est un rayon qui agit comme extension d'un réseau existant sur site, tel qu'un ensemble de serveurs d'assurance qualité à des fins de test ou un ensemble de serveurs de traitement de données qui utilisent le provisionnement à la demande du Cloud pour réduire les coûts et améliorer l'agilité.

Les rayons sont très polyvalents et nous avons vu des clients les utiliser dans leur environnement pour un large éventail de cas d'utilisation. Le dénominateur commun de ces cas d'utilisation est toutefois que les rayons sont les entités dans lesquelles se déroulent les activités dans le Cloud.

## Les nœuds

La Figure 2 ci-dessous illustre une conception à deux nœuds, qui est plus flexible et permet la séparation systématique des types de communications dans l'environnement. L'un des nœuds est destiné au trafic entrant en provenance d'Internet, tandis que l'autre est destiné au trafic latéral entre les rayons, au trafic entrant et sortant du réseau de l'entreprise, et au trafic sortant vers Internet ou d'autres environnements dans le Cloud.

Comme pour les rayons, ce que nous décrivons ici ne sont que les cas d'utilisation les plus courants. En réalité, chaque client met en place ses plates-formes en fonction de ses besoins et de ses exigences spécifiques. Dans les livres blancs de cette série qui décrivent la manière dont le modèle est déployé sur des plates-formes spécifiques de prestataires de Cloud, nous présentons les principales conceptions et alternatives.

## Trafic dans l'environnement

Dans la conception à deux nœuds illustrée dans la Figure 2 ci-dessous, les nœuds sont la seule façon d'entrer et de sortir de l'environnement, et la seule façon de se déplacer à l'intérieur et entre les rayons. Les rayons ne sont pas directement reliés entre eux et ne sont accessibles que par l'intermédiaire d'un des nœuds.

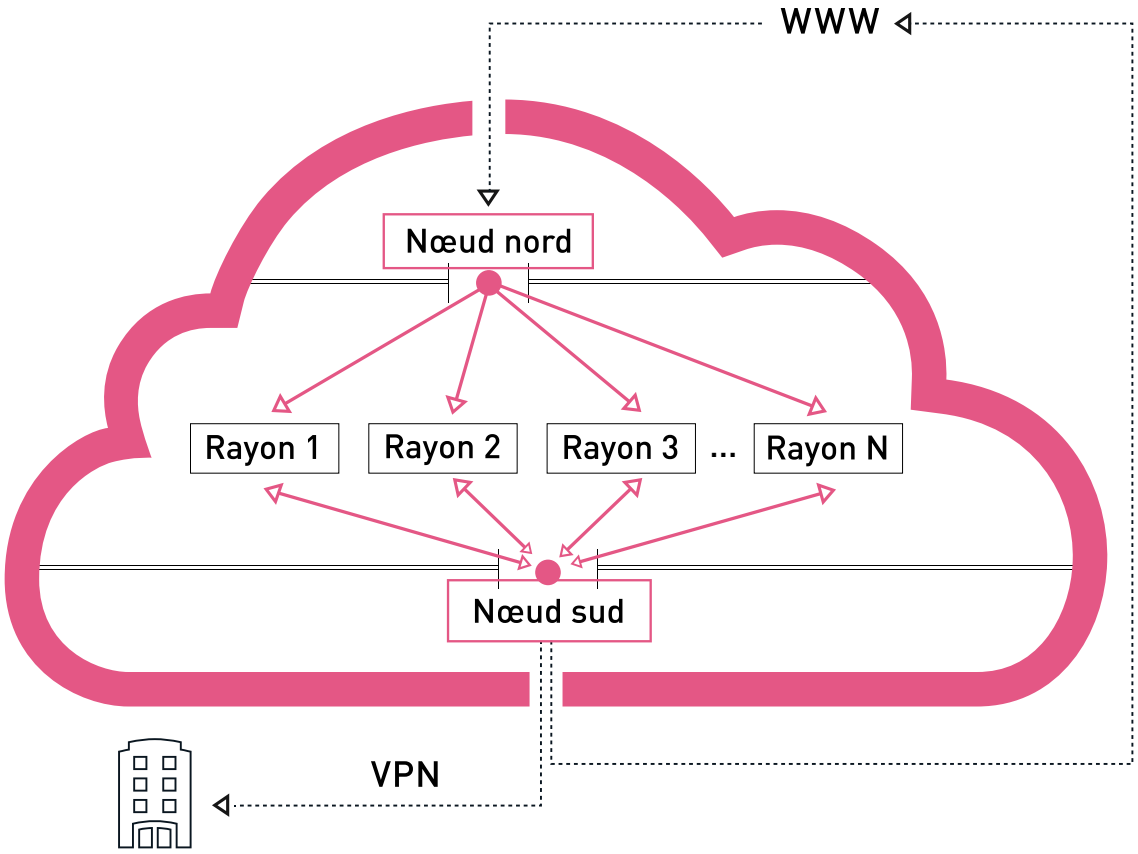


**Figure 2 : La totalité du trafic est acheminée par les nœuds. Le nœud nord est destiné au trafic entrant et le nœud sud au trafic en provenance et à destination du réseau de l'entreprise, au trafic vers internet et à l'accès est-ouest entre les rayons. Chaque rayon comprend des machines virtuelles dans le Cloud avec des niveaux de sécurité et d'accès variables.**

# CloudGuard Dome9 : Orchestration et conformité du Cloud

Faisant désormais partie de la famille des produits CloudGuard, CloudGuard Dome9 est une plate-forme SaaS sous forme d'API qui s'intègre nativement aux clusters AWS, Microsoft Azure, GCP et Kubernetes déployés en tout lieu. CloudGuard Dome9 est une solution d'administration de la posture de sécurité dans le Cloud (CSPM) pour l'orchestration de politiques multi-Cloud. CloudGuard Dome9 utilise les contrôles natifs du Cloud pour mettre en œuvre des politiques de conformité dans chaque Cloud. Il permet à une entreprise de visualiser et d'appliquer sa posture de sécurité dans le Cloud de manière cohérente sur l'ensemble de ses services de Cloud public, garantissant la conformité aux bonnes pratiques et aux réglementations de sécurité dans le Cloud afin d'éviter les dérives de configuration.

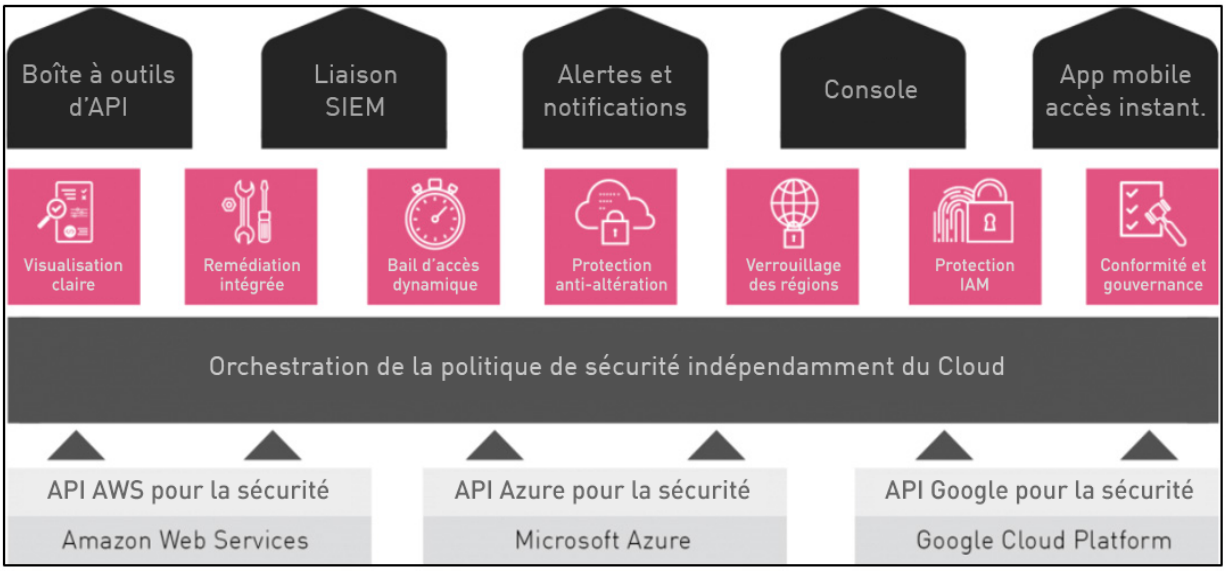


**Figure 3 : Diagramme de CloudGuard Dome9**

Les fonctionnalités de CloudGuard Dome9 jouent un rôle particulièrement important dans le respect de bon nombre des principales exigences architecturales du schéma de sécurité du Cloud 2.0, comme décrit dans le reste de ce livre blanc.

# CloudGuard Log.ic : Analyses et supervision de la sécurité du Cloud

CloudGuard Log.ic est une solution de protection contre les menaces et d'intelligence de sécurité pour le Cloud public. Dernier-né de la famille CloudGuard, il ajoute un contexte aux journaux du Cloud, les transforme en logique de sécurité compréhensible, et permet aux équipes de sécurité de faire passer la sécurité du Cloud à un niveau supérieur. Grâce à CloudGuard Log.ic, les entreprises peuvent désormais visualiser chaque flux de données et piste d'audit dans les environnements élastiques actuels du Cloud, et comprendre les données et les activités résidant dans le Cloud pour accélérer les processus d'investigation.

CloudGuard Log.ic permet la détection des intrusions dans le Cloud, la visualisation du trafic réseau et l'analyse de l'activité des utilisateurs. Ses algorithmes de cartographie d'objets associent un inventaire du Cloud et des informations de configuration avec des données de contrôle en temps réel issues de différentes sources, dont :

- VPC Flow Logs, CloudTrail, Amazon GuardDuty, AWS Inspector (pour les clients AWS)
- Azure vNET Flow Logs and blobs, Azure Monitor, Azure Advanced Threat Protection, Azure Security Center (pour les clients Azure)

ainsi que les flux de Check Point ThreatCloud, la réputation des adresses IP et des bases de données géographiques.

Il en résulte des informations contextualisées et enrichies pour améliorer la visualisation, les requêtes, les alertes signalant des intrusions et les notifications signalant des infractions de la politique. Ces informations peuvent également être acheminées vers des solutions de SIEM tierces. Grâce à la détection embarquée des menaces, la technologie CloudBots de CloudGuard Log.ic étend également les capacités de remédiation à l'infini, vous permettant de créer une réponse personnalisée à tout type d'alerte réseau ou de piste d'audit. CloudGuard Log.ic est la seule plate-forme qui attribue le trafic réseau à des services éphémères natifs dans le Cloud tels que :

- les fonctions Lambda d'Amazon ainsi que d'autres composants de plate-forme natifs dans le Cloud (RDS, Redshift, ELB, ALB, ECS) pour les clients AWS,
- les fonctions d'automatisation d'Azure ainsi que d'autres composants Microsoft Azure natifs dans le Cloud (SQL Azure, Data Warehouse, Azure Virtual Machine, Azure Functions et Azure Container Service) pour les clients Azure,

pour fournir une visibilité et une compréhension complètes de votre infrastructure dans le Cloud au fil du temps.

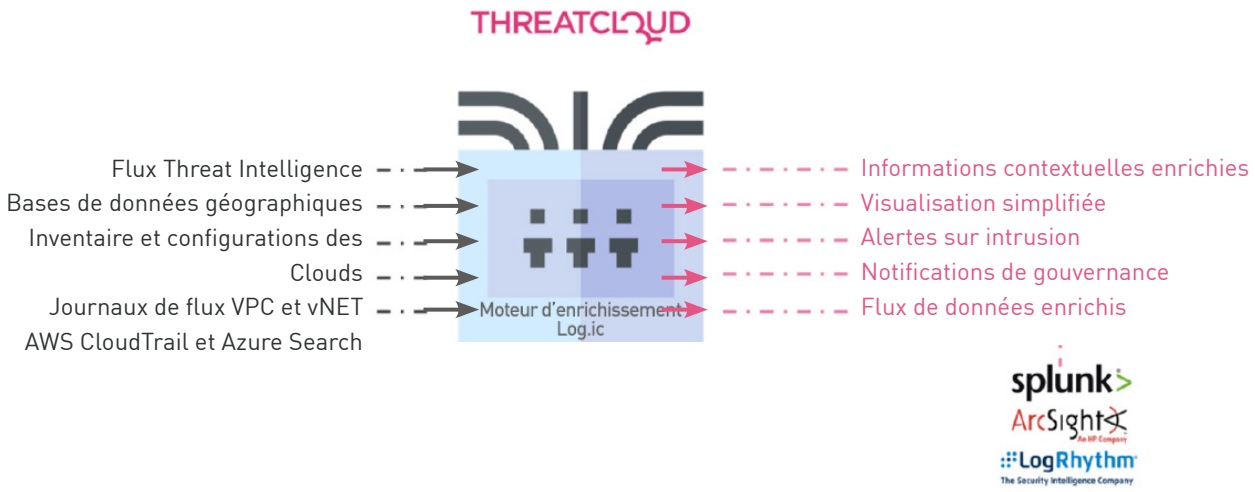


**Figure 4 : Diagramme des flux de CloudGuard Log.ic**

CloudGuard Log.ic utilise les meilleures pratiques de détection par signature, des règles intégrées, des sources d'intelligence sur les menaces et des flux de trafic existants, pour créer un référentiel de l'activité de votre réseau et de vos utilisateurs. Il utilise également des algorithmes d'IA et de détection d'anomalies pour capturer les activités non autorisées ou malveillantes, y compris dans les applications sans serveur. Log.ic fournit aux administrateurs de la sécurité des alertes en temps réel signalant des intrusions et des infractions de la politique, déclenchées à partir de critères personnalisés.

**La plus grande base de données d'IOC au monde comme source :** CloudGuard Log.ic utilise Check Point ThreatCloud pour enrichir les journaux avec différents flux d'intelligence, notamment :

- Plus de 750 millions de hachages, de sites et d'adresses de serveurs de C&C malveillants
- 11 millions de signatures comportementales
- 2,5 millions de détections quotidiennes
- Des dizaines de flux externes

**Remédiation automatique avec CloudBots :** CloudBots est un framework sans serveur qui déclenche une fonction de remédiation en un seul clic, et fonctionne entièrement dans votre environnement. Ajoutez CloudBots pour créer une réponse personnalisée à tout type d'alerte réseau, piste d'audit ou autre, et remédiez aux menaces immédiatement avec CloudGuard Log.ic.

CloudGuard Log.ic Explorer est un outil d'exploration visuelle qui vous permet d'analyser l'activité réseau entrante et sortante de votre environnement dans le Cloud. Vous pouvez utiliser des requêtes prédéfinies, ou définir des requêtes personnalisées à l'aide du langage de requêtes de CloudGuard Dome9. La visibilité sur chaque élément et sur le trafic de votre VPC AWS ou vNET Azure est complète, avec la possibilité de zoomer sur l'entité ou la connexion associée. La visualisation contextualisée permet d'effectuer des enquêtes approfondies, répondre aux incidents et traquer les menaces.

Le connecteur Firehose de CloudGuard Log.transmet un JSON hautement contextualisé du trafic journalisé à différents produits de SIEM, en vue d'effectuer des analyses plus poussées. Connectez-vous à Splunk, ArcSight, LogRythm et bien d'autres, pour les alimenter en données critiques sur les actifs éphémères et documenter la posture de sécurité.

# Schéma 2.0 : solution et principes architecturaux

Le schéma de sécurité du Cloud 2.0 (en tant que conception de haut niveau) est applicable aux principaux Clouds publics, y compris Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP), Oracle Cloud Infrastructure, Alibaba Cloud, IBM Cloud, et autres.

Dans cette section, nous expliquons en détail comment le schéma 2.0 peut être mise en œuvre à l'aide des produits Check Point afin de se conformer aux directives architecturales de sécurité évoquées dans la Présentation du schéma de sécurité du Cloud 2.0, telles que la protection de plusieurs périmètres (réseau, données, traitement et identités), la séparation systématique des flux de trafic au sein de l'environnement, la segmentation et la micro-segmentation, l'agilité, l'automatisation et l'administration unifiée sur plusieurs plates-formes.

## Sécurité dès la conception

Cette approche de sécurité à plusieurs niveaux tire parti des caractéristiques inhérentes d'Internet comme moyen supplémentaire de bloquer les types de trafic indésirables, d'une manière qui ne peut être contournée par la politique de sécurité. La Figure 5 montre comment le modèle en étoile du schéma 2.0 prend en charge la sécurité dès la conception.

Le nœud nord utilise une connexion de peering non transitoire avec les rayons afin de contrôler le flux de trafic. Le peering non transitoire, par définition, isole systématiquement les ressources du Cloud du trafic entrant.

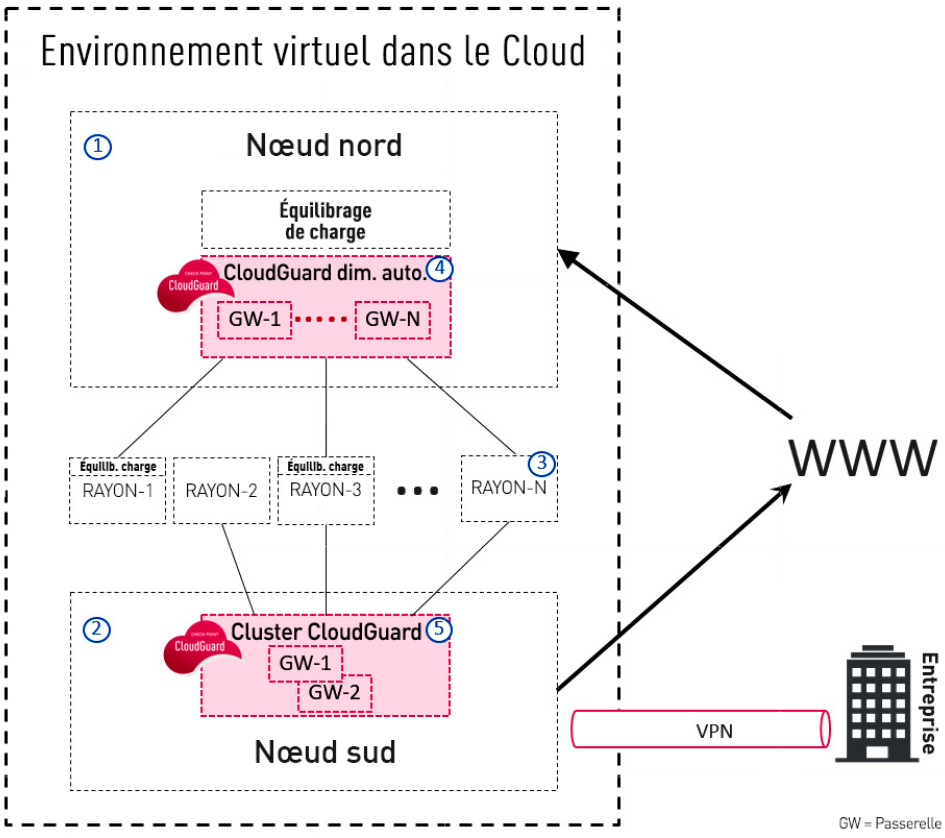


**Figure 5 : Modèle en étoile de CloudGuard IaaS**

**où :**

**1 = Nœud nord pour le trafic entrant provenant d'Internet**

**2 = Nœud sud pour le trafic en provenance et à destination du réseau de l'entreprise, l'accès est-ouest entre les rayons et le trafic sortant vers Internet**

**3 = VM dans le Cloud de rayon à segment avec différents niveaux de sécurité et d'accès**

**4 = Dimensionnement automatique de CloudGuard : un ensemble de pare-feux élastiques pour l'application de la politique de sécurité Internet**

**5 = Cluster haute disponibilité de CloudGuard IaaS.**

L'architecture de sécurité dans le Cloud peut utiliser le peering VPC d'Amazon, qui est non transitoire (une limitation documentée), pour relier du trafic entrant à des environnements réseau isolés. Le mouvement latéral du trafic entre les segments isolés se fait donc exclusivement par ce nœud.

L'exemple ci-dessus permet également à un rayon de ne pas être du tout connecté au nœud nord, empêchant toute exposition possible à Internet.

## Protection du périmètre du réseau

Le contrôle du périmètre du réseau est effectué sur les nœuds nord et sud, avec différentes protections mises en place de manière efficace à la demande. Le trafic entrant depuis Internet et sortant vers Internet est inspecté par les passerelles de sécurité CloudGuard IaaS déployées sur les nœuds, ce qui permet d'appliquer la politique de sécurité de l'entreprise.

Notez qu'il est possible (et recommandé) d'appliquer des politiques et des blades de sécurité différentes aux nœuds nord et sud. Par exemple, il est recommandé que le nœud sud soit configuré avec une protection contre les logiciels malveillants pour empêcher le mouvement latéral des menaces. Le trafic passant par le nœud est inspecté par les passerelles et comparé à la politique de sécurité.

## Segmentation

CloudGuard IaaS prend en charge la segmentation inter-VPC/vNET en plaçant les charges de travail du Cloud dans différents rayons et en appliquant des contrôles de sécurité sur le trafic entrant ou sortant d'un rayon. Les trois principaux types de rayons du schéma 2.0 sont :

- **Vers Internet uniquement** (par ex. RAYON-1 dans la Figure 5) : Ces rayons sont uniquement connectés aux nœuds nord et ne sont accessibles qu'au trafic entrant provenant d'Internet. Ces rayons hébergent généralement des serveurs frontaux qui doivent être accessibles depuis Internet comme, par exemple, les sites web hébergeant des campagnes publiques. Afin d'éviter une exposition publique indésirable des ressources privées (d'entreprise), la connectivité de ces rayons aux ressources de l'entreprise ou à d'autres rayons de l'environnement est systématiquement bloquée et ne peut être activée par simple configuration de routage ou de politique.
- **Vers l'interne (entreprise) uniquement** (par ex. RAYON-2 dans la Figure 5) : Ces rayons sont uniquement connectés aux nœuds sud et ne sont donc pas systématiquement accessibles depuis Internet. Ils sont accessibles par toute combinaison de VPN, de connectivité directe depuis le réseau de l'entreprise ou par d'autres rayons de l'environnement (conformément à la politique de sécurité des pare-feux du nœud sud). Un cas typique d'utilisation d'un rayon côté privé est l'hébergement de serveurs de bases de données auxquels nous voulons avoir une connectivité sécurisée sans qu'ils soient directement accessibles depuis Internet.

- **Combinés** (par ex. RAYON-3 dans la Figure 5) : Ces rayons sont adaptés à des serveurs qui doivent être accessibles depuis Internet mais qui nécessitent également un accès interne à d'autres rayons ou au réseau de l'entreprise. Un exemple serait un serveur web qui est exposé à Internet et qui a également besoin d'un accès à un serveur applicatif ou une base de données.

CloudGuard Dome9 prend en charge la segmentation intra-VPC/vNET à l'aide des contrôles de sécurité natifs du Cloud pour bloquer le trafic entre les charges de travail au sein d'un sous-réseau. L'administration unifiée des listes d'accès et des groupes de sécurité de Dome9 est particulièrement utile dans les environnements multi-Cloud. Grâce à CloudGuard Dome9, vous bénéficiez d'une meilleure granularité au niveau du sous-réseau et pouvez, en théorie (et aussi en pratique, si vous le souhaitez), créer une politique ou une isolation spécifique à la VM ou à l'instance au niveau de la couche 4.

Dans ce cas précis, les fonctionnalités de CloudGuard Dome9 étendent celles de CloudGuard IaaS : CloudGuard IaaS est principalement utilisé pour la segmentation au niveau de l'infrastructure et des garde-fous, tandis que CloudGuard Dome9 prend en charge la micro-segmentation effectuée à l'aide des contrôles natifs du Cloud.

CloudGuard Dome9 ajoute une autre couche de segmentation (entre les services et entre les utilisateurs) avec une élévation des privilèges, juste le temps d'effectuer des opérations d'administration, qui se superpose aux services IAM natifs du Cloud. Les utilisateurs de l'IAM qui souhaitent accéder à des services protégés peuvent élever eux-mêmes leurs privilèges ou les élever via l'administrateur de Dome9. L'autorisation n'est fournie que pour une durée limitée. Pendant ce temps, l'utilisateur de l'IAM peut accéder aux services protégés. L'accès aux services est à nouveau bloqué une fois le délai expiré.

Cette fonction durcit la console du compte du prestataire et empêche les utilisateurs d'apporter des modifications non autorisées ou accidentelles aux paramètres du compte à l'insu et sans l'autorisation d'un administrateur. Elle réduit également de manière significative le rayon d'action d'un pirate cherchant à s'approprier l'identité d'un compte possédant des privilèges élevés.

## Agilité et automatisation

Aujourd'hui, les technologies de l'information ont pour objectif de faciliter les activités de l'entreprise au lieu de les freiner. Le modèle en étoile du schéma 2.0 favorise l'agilité des entreprises puisque des rayons peuvent être créés et entièrement détenus par les différentes fonctions de l'entreprise ou, en fait, par quiconque au sein de l'entreprise. CloudGuard Dome9 peut appliquer le principe d'absence de connectivité directe entre les rayons, obligeant le trafic des rayons à passer par le nœud sud et ses contrôles de sécurité. De cette façon, les propriétaires de rayons ont la possibilité de posséder et gérer la sécurité à l'intérieur de leurs rayons, sans compromettre la sécurité générale.

CloudGuard IaaS veille à ce que cette agilité ne nuise pas à la posture de sécurité de l'entreprise en appliquant une automatisation à plusieurs niveaux. Au niveau de l'infrastructure, le déploiement des ressources CGI peut être automatisé via des modèles d'implémentation tels qu'AWS CloudFormation ou Azure Resource Manager Template. Ces scripts préconfigurés simplifient la mise en œuvre des passerelles CGI dans différentes configurations de déploiement, notamment autonome, en cluster et par dimensionnement automatique. L'environnement requis (sous-réseaux, accès Internet, configuration du routage, etc.) est créé à l'avance.

Une autre couche d'automatisation consiste à utiliser une CME (Cloud Management Extension) pour fournir automatiquement des ressources dans des configurations de Clouds publics dynamiques telles que le dimensionnement automatique et l'équilibrage de charge. Tout ajout ou suppression de passerelles de sécurité dans l'environnement déclenche un processus automatisé de mise en service ou de mise hors service de la passerelle à partir de la couche de la politique de sécurité/ SmartConsole. Par exemple, chaque fois qu'une nouvelle passerelle est ajoutée dans l'environnement, le processus d'automatisation reposant sur une CME découvrira automatiquement la nouvelle passerelle, en effectuera la configuration initiale, la redémarrera, établira une communication interne sécurisée avec le serveur d'administration, et poussera la politique de sécurité vers la passerelle.

De même, la CME peut également automatiser la configuration de sécurité des paramètres d'équilibrage de charge puisqu'elle peut détecter la configuration de l'écouteur sur l'équilibreur de charge, et peut créer automatiquement les règles pertinentes dans la politique de sécurité. Ce comportement apporte des avantages significatifs aux activités quotidiennes, la sécurité devenant une partie intégrante plutôt qu'un élément freinant. Les modifications apportées à l'équilibreur de charge sont automatiquement répercutées dans la politique du pare-feu, de manière transparente.

L'automatisation est également possible au niveau des règles de la politique de sécurité, le contrôleur de CloudGuard permettant l'utilisation des objets natifs du Cloud dans la politique de sécurité. Les objets natifs du Cloud ajoutés sont automatiquement et continuellement suivis par le serveur d'administration, et toute modification apportée côté Cloud (comme le marquage d'une instance avec une balise incluse dans la politique de sécurité, la modification d'une IP ou du nom d'une instance, etc.) est automatiquement et instantanément répercutée à toutes les passerelles connectées au serveur d'administration.  Ainsi, les responsables métiers peuvent agir rapidement tout en s'assurant que les politiques et les normes de sécurité de l'entreprise sont respectées.

CloudGuard Dome9 protège également activement les charges de travail, les PaaS et les fonctions sans serveur qui s'exécutent dans le Cloud public, en les entourant de garde-fous qui les protègent sans entraver leur agilité. Il peut par exemple analyser le texte d'une fonction sans serveur pour détecter les fuites potentielles (par ex. les clés des API), vérifier la liste des autorisations et des privilèges dans son code, et comparer la communication des fonctions sans serveur avec des listes d'URL suspectes. Ces fonctions, ainsi que d'autres fonctionnalités de CloudGuard Dome9, réduisent les surfaces d'attaque et bloquent de nombreuses tentatives d'exploitation, de manière transparente pour les propriétaires de rayons, qui peuvent ainsi poursuivre leurs activités en toute tranquillité.

## Gouvernance et conformité du Cloud

Compte tenu du manque de visibilité sur les actifs dans le Cloud et de sa nature hautement dynamique, le Cloud présente des défis importants en matière de conformité et d'audit de conformité. Si l'on tient compte de l'impact des environnements hybrides et multi-Clouds complexes, le maintien d'un dispositif de sécurité dans le Cloud conforme aux exigences de la gouvernance d'entreprise et de la réglementation peut parfois sembler une mission impossible.

Bien qu'il ne s'agisse pas principalement d'une solution de conformité du Cloud, CloudGuard IaaS contribue à la conformité du Cloud par la répercussion automatisée des modifications des règles de sécurité à toutes les passerelles de sécurité connectées au serveur d'administration. CloudGuard IaaS s'appuie par ailleurs sur la blade Check Point GRC (gouvernance, risque, conformité) pour surveiller les passerelles de sécurité 24 heures sur 24 et 7 jours sur 7, avec :

- Des alertes instantanées sur les changements de politique susceptibles de réduire la sécurité, avec des recommandations pour y remédier
- Des évaluations en temps réel de la conformité à la réglementation
- Des rapports d'audit qui identifient les lacunes au niveau des paramètres de configuration et les faiblesses de la sécurité

Le moteur de conformité de CloudGuard Dome9 compare la conformité des environnements dans le Cloud avec les normes et les bonnes pratiques du secteur, ou avec les politiques de sécurité de l'entreprise. Il peut également vérifier la conformité en utilisant des règles prêtes à l'emploi.

Les règles de sécurité complètes de CloudGuard Dome9 couvrent un grand nombre de normes courantes telles que PCI-DSS et HIPAA, ISO 27001, RGPD, NIST, CIS et bien d'autres. Elles peuvent être appliquées immédiatement telles quelles sur tous les comptes Cloud de l'entreprise. De nouvelles règles peuvent être également élaborées et testées, ou des règles existantes peuvent être modifiées, à l'aide d'un générateur de règles graphique intuitif, adaptant les politiques de sécurité aux besoins et aux objectifs de conformité spécifiques de chaque entreprise. De toutes ces façons, le puissant moteur de conformité de CloudGuard Dome9 permet à l'entreprise de se conformer à la fois aux réglementations de tiers et aux politiques de sécurité spécifiques de l'entreprise, et de réagir rapidement en cas d'erreurs de configuration et de modifications accidentelles.

Le moteur de conformité fonctionne avec les trois principaux prestataires de Cloud (AWS, Azure et GCP) pour vérifier facilement la conformité dans les environnements multi-Cloud. Il peut également effectuer des évaluations dans des groupes de Kubernetes en comparant la conformité avec des normes telles que les benchmarks CIS pour Kubernetes et autres.

Le moteur de conformité vérifie les comptes en ligne en permanence et envoie des notifications lorsque des problèmes sont détectés. Il génère également des comptes-rendus enrichis comportant des résultats détaillés des évaluation ou des rapports de synthèse des résultats dans les différentes régions et les comptes VPC/vNET. Les détails peuvent être facilement consultés à partir des résultats de haut niveau. Pour obtenir des informations plus rapidement, les rapports peuvent être structurés et filtrés en fonction des niveaux de gravité, des entités évaluées, etc. Les rapports d'historiques peuvent être utilisés pour mettre en évidence les tendances d'un large éventail de paramètres.

## Visibilité

Les clients du Cloud se plaignent souvent du manque de visibilité pour identifier et quantifier leurs actifs dans le Cloud. Ces actifs invisibles et non gérés entraînent de graves lacunes dans l'application des règles de sécurité. Les clients du Cloud ont besoin d'outils d'orchestration pour le Cloud afin d'identifier et de surveiller efficacement leurs actifs dans le Cloud, et visualiser leurs environnements dans le Cloud. Dans l'architecture en étoile, la totalité du trafic réseau passe par les nœuds, ce qui permet d'obtenir une visibilité grâce à l'utilisation de journaux de sécurité.

CloudGuard IaaS utilise la blade de gestion des événements SmartEvent pour offrir une visibilité totale sur les menaces du point de vue des risques de sécurité, ce qui accélère la réponse aux incidents. Les utilisateurs peuvent maîtriser les événements de sécurité grâce à la conformité, le reporting, les analyses des événements et des investigations en temps réel. Cette véritable visibilité sur le réseau leur permet ainsi de répondre immédiatement aux incidents de sécurité.

CloudGuard Dome9 permet aux entreprises de visualiser tous les actifs dans le Cloud, évaluer la posture de sécurité (y compris les groupes de sécurité, les instances, etc.), corriger les erreurs de configuration pour empêcher les menaces, gérer les groupes de sécurité natifs dans le Cloud, et appliquer la sécurité à partir d'une source unique d'autorité réseau.

CloudGuard Log.ic est une technologie d'intelligence de sécurité native dans le Cloud qui combine les informations d'inventaire et de configuration du Cloud avec différentes données de surveillance en temps réel pour fournir une détection des intrusions dans le Cloud, une visualisation du trafic réseau et une analyse de l'activité des utilisateurs.

CloudGuard Log.ic analyse le trafic réseau et les journaux d'événements des prestataires de services dans le Cloud, les rendant compréhensibles en fournissant un contexte qui, autrement, serait absent.

CloudGuard Log.ic permet à l'entreprise de visualiser toutes les ressources actives dans un compte donné, celles qui sont connectées et qui envoient du trafic entre elles, ainsi que les statistiques pour chaque élément. Log.ic permet également de visualiser les événements réseau dans le Cloud. Ainsi, par exemple, les entreprises peuvent déterminer quelle fonction sans serveur a été invoquée, par quelle passerelle le trafic circule, quel type d'actif communique, et à quel VPC/vNET il appartient.

CloudGuard Log.ic s'intègre à l'un des principaux flux d'intelligence sur les menaces, repérant le trafic entrant et sortant en provenance et à destination d'hôtes malveillants. Il avertit de toute activité malveillante ou de tout événement suspect et indésirable, et demande à l'utilisateur de prendre des mesures en conséquence. Des requêtes prêtes à l'emploi ou personnalisées peuvent être utilisées pour rechercher des événements notables dans les journaux, en temps réel.

## Absence de frontières

Les entreprises ont tendance à mettre en œuvre des environnements multi-Cloud et hybrides complexes. Le schéma de sécurité du Cloud prend intrinsèquement en charge le dimensionnement en dehors des limites d'une seule plate-forme de Cloud. Il gère également la connectivité entre les plates-formes dans le Cloud tout en conservant les mêmes principes architecturaux et la même posture de sécurité dans tous les environnements.

Afin de minimiser les risques associés à la surveillance et la sécurisation de ces environnements complexes, CloudGuard IaaS met en œuvre un maillage VPN (voir Figure 6) qui sécurise la connectivité entre plusieurs sites.

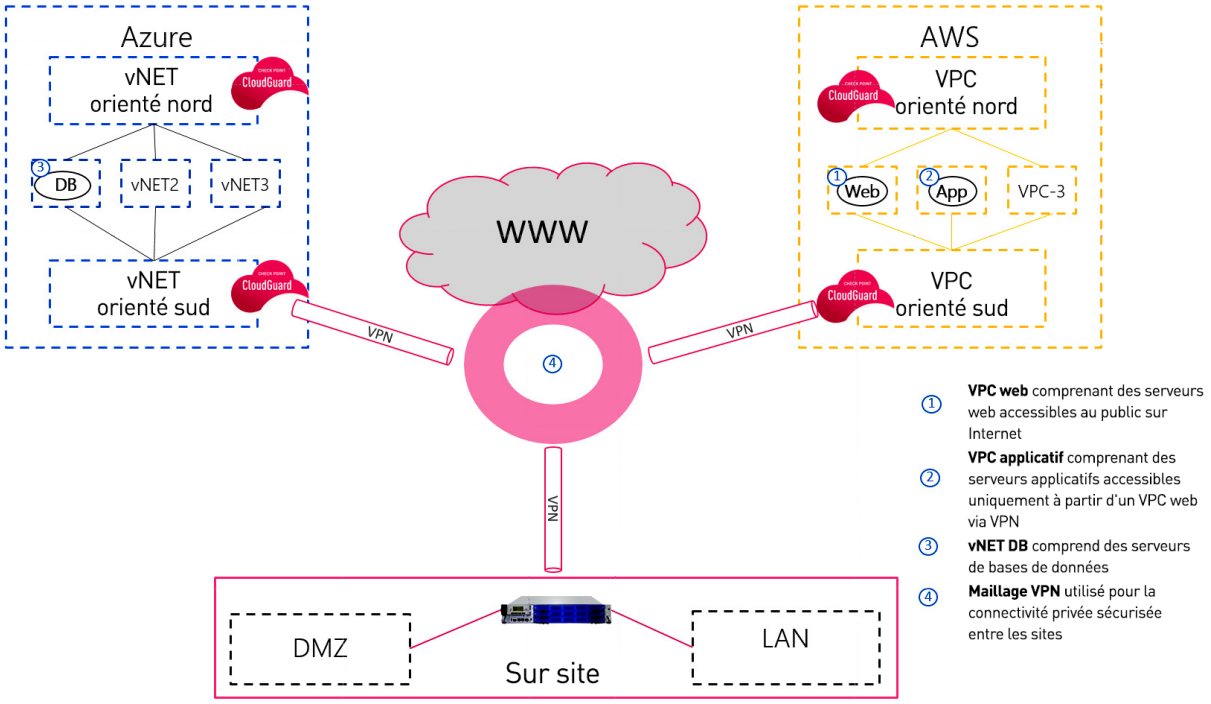


**Figure 6 : Implémentation de passerelles CloudGuard IaaS sur les plates-formes pour le contrôle du trafic et l'application des politiques de sécurité sur des sites spécifiques**

**où :**

**1 = Un VPC web comprenant des serveurs web accessibles au public sur Internet**

**2 = Un VPC applicatif comprenant des serveurs applicatifs accessibles uniquement à partir d'un VPC web via VPN**

**3 = La base de données MSSQL Azure**

**4 = Maillage VPN utilisé pour la connectivité privée sécurisée entre les sites**

Le cas d'utilisation de l'architecture multi-Cloud illustré à la Figure 6 est celui d'une entreprise de jeux en ligne qui déploie ses services sur AWS, Azure et un Datacenter sur site, en choisissant l'approche la plus adaptée à chaque plate-forme, en fonction de l'expertise de l'équipe et de sa supériorité technologique. Le serveur web frontal et les serveurs applicatifs sont hébergés dans plusieurs zones d'AWS pour assurer la redondance, tandis que la gestion des identités et l'authentification sont fournies par le serveur AD sur site. La base de données et le stockage sont hébergés dans Azure.

La mise en place de passerelles CloudGuard IaaS sur les différentes plates-formes nous permet de contrôler spécifiquement le trafic dans chaque zone, et d'appliquer des politiques de sécurité entre les différentes zones et à l'intérieur de celles-ci.

CloudGuard Dome9 applique également le principe de l'absence de frontières en fournissant et en orchestrant ses fonctionnalités de sécurité auprès des trois principaux prestataires de services dans le Cloud : Amazon Web Services, Microsoft Azure et Google Cloud Platform (GCP). Dome9 prend également en charge l'intégration des clusters de Kubernetes dans l'inventaire des Clouds de Dome9 afin que des évaluations de conformité puissent être effectuées sur ces clusters. Un cluster peut se trouver sur site ou dans un environnement dans le Cloud, y compris les environnements managés dans le Cloud.

## Administration unifiée

L'implémentation et l'administration de la sécurité dans un environnement multi-Cloud peuvent être difficiles, car elles impliquent la gestion et le contrôle de ressources qui utilisent différents outils de gestion dans différents endroits. Tenter de maintenir une politique de sécurité unifiée dans de telles conditions est non seulement fastidieux et inefficace, mais souvent source d'erreurs. Il est également difficile de déterminer les problèmes de connectivité, ou résoudre rapidement et efficacement les problèmes de sécurité, dans un tel environnement.

Le schéma 2.0 prend en charge l'administration intégrée de la sécurité afin que les entreprises puissent traduire leurs définitions de sécurité en un ensemble simple de règles, et mettre en œuvre ces règles de manière cohérente dans des environnements multi-Cloud et hybrides complexes.

D'autres défis souvent rencontrés dans les environnements multi-Cloud sont la mise en œuvre d'une politique de sécurité unifiée et l'obtention d'une visibilité de bout en bout sur les événements de sécurité.

Le serveur d'administration de la sécurité (SMS) Check Point R80 est une solution intégrée d'administration de la sécurité qui comprend la politique de sécurité, la journalisation, la supervision, la corrélation des événements et la création de rapports. Prenant en charge les principaux prestataires de Cloud publics et privés, le SMS permet aux entreprises de traduire leurs définitions de sécurité en un ensemble simple de règles qui peuvent être efficacement administrées et appliquées en tant que politique de sécurité unifiée. Les administrateurs peuvent également facilement identifier les risques de sécurité dans l'environnement.

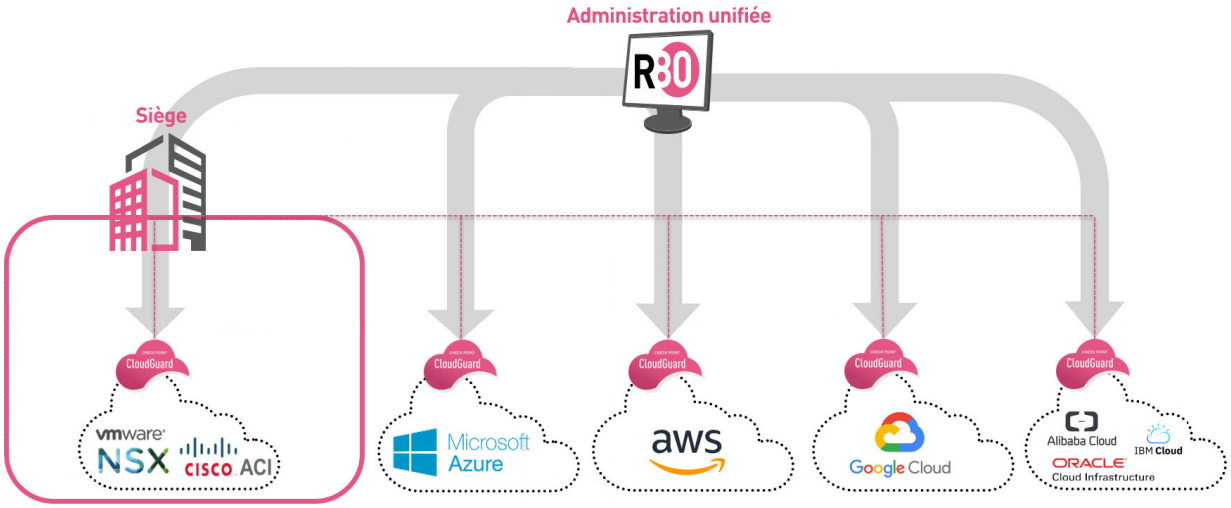


**Figure 7 : Serveur d'administration de la sécurité Check Point R80 pour une administration unifiée**

Le déploiement du SMS R80 est flexible, et il peut être localisé n'importe où dans l'environnement. Il est également possible d'implémenter le SMS en mode haute disponibilité sur plusieurs plates-formes (par ex. un serveur d'administration primaire situé sur place avec un serveur secondaire situé dans un site secondaire à des fins de reprise sur incident).

L'administration unifiée est également l'une des principales propositions de valeur de CloudGuard Dome9, avec son interface centralisée qui simplifie l'administration et l'orchestration de la sécurité sur l'ensemble des ressources du Cloud.

# Résumé

Le schéma de sécurité du Cloud 2.0 est un framework reposant sur les meilleures pratiques en matière de sécurité dans le Cloud, pour implémenter une infrastructure sécurisée s'appuyant sur les principes architecturaux essentiels de la sécurité dans le Cloud, à savoir une protection avancée contre les menaces sur tous les vecteurs d'attaque (réseau, données, messagerie, identités, utilisateurs), la sécurité dès la conception, la segmentation, l'agilité sécurisée, une automatisation robuste et l'indépendance vis-à-vis des prestataires.

Le schéma 2.0 garantit que la totalité du trafic à destination et en provenance d'environnements réseau isolés passe par les contrôles de sécurité d'un courtier central. Chaque environnement isolé est un segment dont les contrôles de sécurité peuvent être adaptés au type de trafic entrant et sortant. Les segments orientés vers Internet, par exemple, sont configurés pour surveiller le trafic extérieur entrant afin de détecter les menaces ou les anomalies, et peuvent systématiquement bloquer le mouvement latéral du trafic. En revanche, les segments privés (d'entreprise) peuvent être configurés pour inspecter et sécuriser efficacement le trafic latéral.

Le schéma 2.0 favorise également l'agilité des entreprises. Les propriétaires de segments, tels que les différents métiers, peuvent fonctionner librement, mais les contrôles de sécurité gérés de manière centralisée garantissent que les politiques de sécurité de l'entreprise sont respectées de manière cohérente sur toutes les plates-formes et tous les comptes.

Les solutions de Check Point pour le Cloud, CloudGuard IaaS, CloudGuard Dome9 et CloudGuard Log.ic, fonctionnent ensemble pour assurer une mise en œuvre du schéma 2.0 en toute transparence.

CloudGuard IaaS, par exemple, applique une sécurité périmétrique avancée sur les nœuds, implémente un VPN maillé pour une connectivité sécurisée entre plusieurs prestataires, comptes et actifs, et permet aux entreprises d'administrer et d'appliquer efficacement une politique de sécurité s'appuyant sur des règles dans des environnements complexes. CloudGuard IaaS prend également en charge l'automatisation et l'orchestration au niveau du déploiement de l'infrastructure (à l'aide de modèles d'implémentation) ainsi que l'approvisionnement dynamique des ressources pendant l'exécution afin de prendre en charge de manière sécurisée le dimensionnement automatique et l'équilibrage de la charge des services dans le Cloud. De plus, l'automatisation au niveau de la politique permet aux objets natifs du Cloud de s'adapter automatiquement à la politique de sécurité de l'entreprise. CloudGuard IaaS permet également la résilience des déploiements multizones.

CloudGuard Dome9 est une puissante solution SaaS de gestion de la posture de sécurité dans le Cloud (CSPM), qui visualise et applique de manière cohérente la posture de sécurité d'une entreprise sur l'ensemble des prestataires et des services. CloudGuard Dome9 identifie et signale rapidement tout trafic anormal dans l'environnement de l'entreprise, ce qui permet de réagir rapidement et, le cas échéant, de déclencher des processus de remédiation automatisés. Son moteur de conformité compare en permanence la conformité avec les exigences de tiers ou de l'entreprise, en fournissant des ensembles de règles qui peuvent être utilisés tels quels ou adaptés aux besoins spécifiques de l'entreprise en matière de conformité. CloudGuard Dome9 durcit les services IAM natifs du Cloud pour protéger les actifs et les activités sensibles par des élévations de privilèges à durée limitée.

Enfin et surtout, CloudGuard Log.ic est un outil d'intelligence de sécurité dans le Cloud qui tire des informations et un contexte exploitables du trafic réseau et des journaux d'événements des prestataires de services dans le Cloud.

Contactez Check Point pour plus d'informations ou demandez une démonstration des solutions de sécurité ci-dessus pour vous aider à concevoir une architecture sécurisée dans le Cloud.

**Siège mondial**
5 Ha'Solelim Street, Tel Aviv 67897, Israël | Tél. : +972 3 753 4555 | Fax : +972 3 624 1100 | Email : info@checkpoint.com

**Siège français**
120 avenue Charles de Gaulle, 92200 Neuilly sur Seine | Tél. : +33 (0)1 55 49 12 00 | Email : info_fr@checkpoint.com

**www.checkpoint.com**