Forcepoint

Présentation succincte

Forcepoint Next Generation Firewall et Microsoft Azure

Le Firewall d'entreprise le plus sécurisé et le plus efficace – géré de manière centralisée, toujours actif et inlassable.

Le défi

- Les entreprises et les organisations doivent maintenir le même niveau de sécurité sur leurs environnements cloud et hybrides qu'avec leurs infrastructures traditionnelles sur site.
- Construire et maintenir une infrastructure hybride ou cloud sécurisée peut s'avérer coûteux et pose un défi technique.
- Le respect de la conformité réglementaire peut être difficile à atteindre et pose un défi technique

La Solution

- Forcepoint Next Generation Firewall est une solution logicielle conçue pour offrir une sécurité maximale pour un coût et une complexité minimums.
- Le Centre de Gestion de Sécurité Forcepoint (SMC) donne aux équipes TI la capacité de gérer des milliers de Firewalls, de rationaliser les processus et de fournir une visibilité inégalée avec des contrôles granulaires.
- Notre solution rationalise les efforts de mise en conformité en proposant des politiques prêtes à l'emploi qui permettent de garantir la conformité sur les réseaux virtuels et physiques, tout en offrant un accès facile aux rapports d'audit.

Résultat

- Une sécurité maximale dans les systèmes cloud et hybrides avec un minimum de complexité.
- Réponse rapide en cas d'incident
- Uniformisation de la conformité, de la mise en œuvre et de la gestion de la conformité aux réglementations
- Réduction du coût total d'acquisition (CTA) de l'infrastructure et de la sécurisation du réseau.

Forcepoint Next Generation Firewall connecte et protège les réseaux d'entreprise exigeants et distribués. Les déploiements élastiques sans contact et la doctrine de sécurité réseau Zero Trust offrent l'efficacité, la fiabilité et les hautes performances de sécurité dont vous avez besoin pour défendre votre périphérie.

Après avoir gagné la confiance de milliers de clients dans le monde entier, les solutions de sécurité réseau de Forcepoint sont maintenant disponibles sur le marketplace Microsoft Azure. Ces solutions permettent aux entreprises d'aborder les problèmes critiques de manière efficace et économique.

Forcepoint Security pour les environnements de cloud public

Les services basés dans le cloud et les déploiements virtuels transforment les entreprises de toutes les formes et de toutes les tailles. Le matériel traditionnel sur site disparaît rapidement parce que les entreprises ont besoin d'une plus grande efficacité, d'une plus grande souplesse et d'un meilleur contrôle des coûts sans contraintes de maintenance ou de frais généraux, pour garder leur compétitivité. Afin d'aider ses clients à rester compétitifs, Forcepoint a stratégiquement conçu ses solutions de sécurité réseau pour qu'elles soient centrées sur le logiciel, ce qui signifie que vous pouvez les emporter avec vous lorsque vous migrez vers le cloud. L'adoption généralisée des architectures infonuagiques ajoute aux professionnels de la sécurité et aux responsables informatiques une nouvelle pression, car ils doivent veiller à ce que ces nouveaux environnements soient tout aussi sécurisés que leurs prédécesseurs physiques.

Forcepoint Next Generation Firewall sert de fondation à des solutions logicielles conçues pour offrir une sécurité maximale pour un coût et une complexité minimales. Notre centre de gestion de la sécurité (SMC) fournit une plateforme unifiée offrant une visibilité et un contrôle inégalés, ainsi qu'une application cohérente des politiques, afin de garantir la conformité réglementaire dans les environnements physiques, virtuels et cloud.

Sécurité Cloud Microsoft Azure

Pour assurer la sécurité dans les environnements cloud, Forcepoint apporte à Azure une technologie de pointe en matière de Next Generation Firewall, avec une évolutivité, une efficacité opérationnelle et une sécurité sans faille. Étendez facilement et en toute sécurité le réseau de votre entreprise – des centres de données et de la périphérie du réseau à vos succursales et sites distants - à votre environnement de cloud Azure via une passerelle VPN (Virtual Private Network) sécurisée. Notre gestion centralisée vous permet de créer et de déployer des politiques rapidement et de manière cohérente sur l'ensemble de vos systèmes. Vous pouvez rapidement et précisément repérer ce qui se passe à la fois dans votre environnement Azure et dans votre réseau physique.

Les clients qui passent au Forcepoint Next Generation Firewall font état d'une baisse de 86 % des cyberattaques, d'une diminution de 53 % du temps de travail de l'équipe TI et d'une diminution de 70 % de la maintenance planifiée.

Sécurité maximum – Complexité minimum

L'architecture logicielle des solutions de sécurité de Forcepoint, telles que la protection contre les menaces avancées, l'inspection approfondie des paquets et le contrôle au niveau des applications, est conçue pour un déploiement facile et élastique sur site, virtuel ou dans le cloud. Des contrôles granulaires des utilisateurs, des applications et des protocoles permettent à votre équipe de sécurité de tirer parti de la puissance de l'automatisation pour réduire la complexité et minimiser le temps consacré aux tâches banales d'hygiène de sécurité. L'approche globale et intégrée de Forcepoint en matière de défense profonde peut être adaptée aux besoins spécifiques de chaque personne, chaque lieu ou chaque bien, y compris avec des Firewalls uniques ou multiples, des VPN, des IPS et pour la protection par filtrage des URL. Notre Next Generation Firewall intégral offre toutes les fonctionnalités existantes que l'on retrouve dans un appareil matériel avancé, y compris l'inspection dynamique, la politique granulaire et le contrôle d'accès, ainsi que les connexions ISP redondantes, mais sans nécessiter de boîtier.

Une visibilité et un contrôle en temps réel

Forcepoint Next Generation Firewall offre une visibilité et un contrôle complets du flux de trafic au sein des environnements virtuels et cloud, ce que les consoles de gestion traditionnelles ne peuvent pas faire. Notre emblématique SMC fournit des rapports rapides ainsi que des capacités de basculement automatisé pour alerter les administrateurs si un système est sur le point de tomber en panne. Il peut prendre des décisions automatisées basées sur des règles préconfigurées afin d'éviter toute interruption de l'expérience utilisateur. Gérez n'importe quel nombre ou combinaison d'appareils ou de clusters Forcepoint physiques ou virtuels, ainsi que des versions logicielles exécutées sur du matériel x86 standard. Le SMC renforce également la sécurité des systèmes virtuels grâce à un tableau de bord holistique de surveillance, qui offre une visibilité complète des applications et un contrôle granulaire.

Simplifiez la mise en conformité réglementaire

Il est difficile de se conformer aux dernières exigences réglementaires telles que PCI DSS, HIPAA, Sarbanes-Oxley et FISMA dans le monde physique, mais il est encore plus difficile de le faire dans l'espace numérique. Les contrôles traditionnels autour de chaque application ne sont pas présents dans un environnement virtuel, ce qui rend presque impossible de déterminer quelles informations ont été consultées, qui les a consultées et à quel moment, et cela risque d'alerter les auditeurs. Le SMC Forcepoint vous offre le niveau de surveillance, d'analyse et de rapport dont vous avez besoin pour garantir la conformité des réseaux virtuels et physiques. Il recueille des données complètes sur tous les événements du réseau et les présente dans des journaux d'audit clairs et faciles à comprendre. Le SMC répertorie également les paramètres de sécurité, signale les modifications apportées au système et fournit les rapports d'audit précis dont vous avez besoin, juste en appuyant sur un bouton.

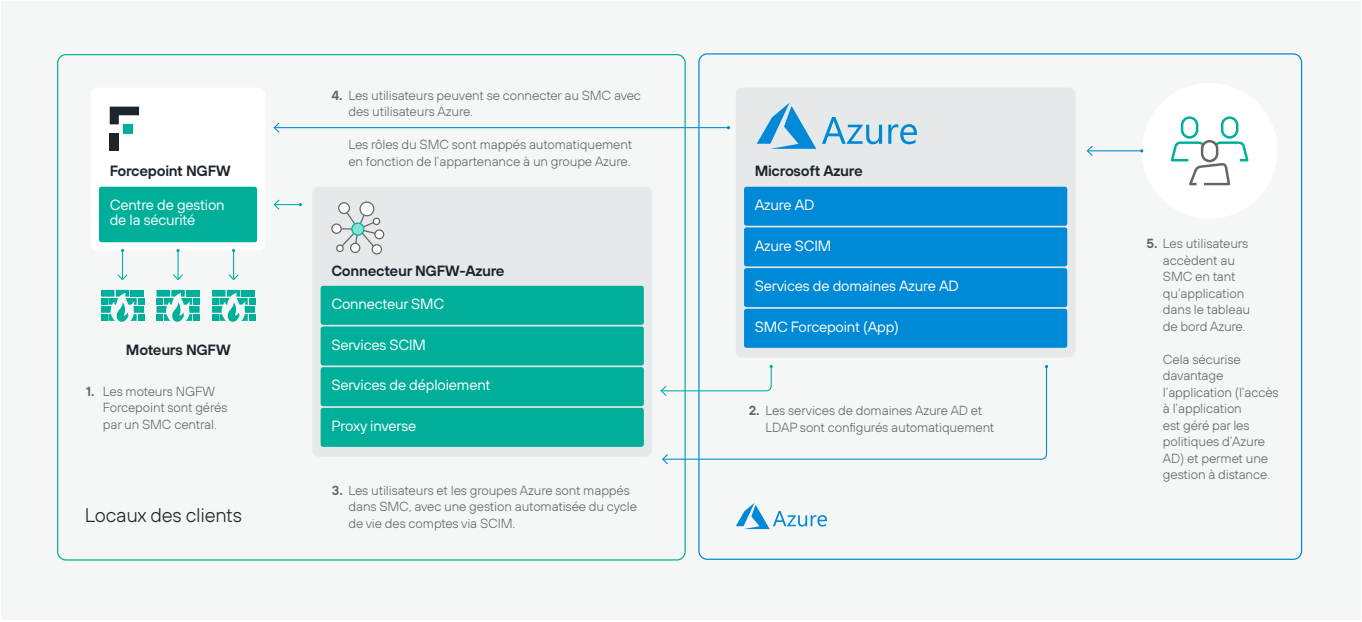
Déploiement rapide et élastique

Pour déployer facilement Forcepoint Next Generation Firewall dans votre environnement Microsoft Azure, rendez-vous sur le marketplace Microsoft Azure.

→ Aller sur le Marketplace

Solutions Forcepoint Next Generation Firewall + Microsoft Azure

Optimisez votre investissement Azure et étendez les capacités de vos solutions Forcepoint grâce à nos intégrations uniques. Pour plus de détails sur nos intégrations, y compris des instructions de mise en œuvre étape par étape, veuillez consulter le site forcepoint.github.io



Azure Active Directory (AD) - Intégration d'accès sécurisé hybride

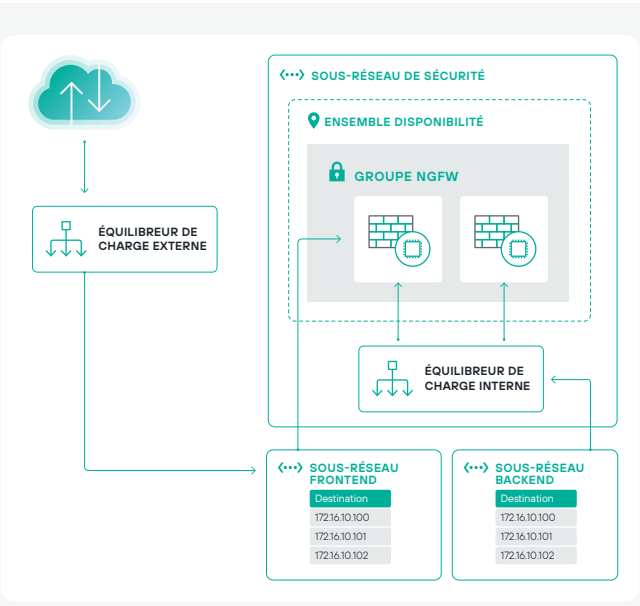
Active l'accès et l'authentification de Forcepoint SMC par le biais d'utilisateurs et de politiques Azure AD.

- → Donne au SMC le rôle d'une application Azure pour les capacités de gestion à distance.
- → Des utilisateurs Azure AD choisis individuellement peuvent se voir attribuer différents niveaux d'accès dans le SMC, ce qui permet de mettre en place plusieurs scénarios de gestion à distance pour l'ensemble d'une flotte de moteurs de Next Generation Firewall.
- → Active la gestion et le contrôle centralisés dans le SMC, mais avec la sécurité supplémentaire des politiques d'authentification Azure AD.

Haute disponibilité avec l'intégration d'Azure Resource Manager (ARM)

Automatise le déploiement d'un ensemble redondant de moteurs de Next Generation Firewall dans Azure, en s'appuyant sur un modèle ARM configuré pour déployer l'ensemble de la pile.

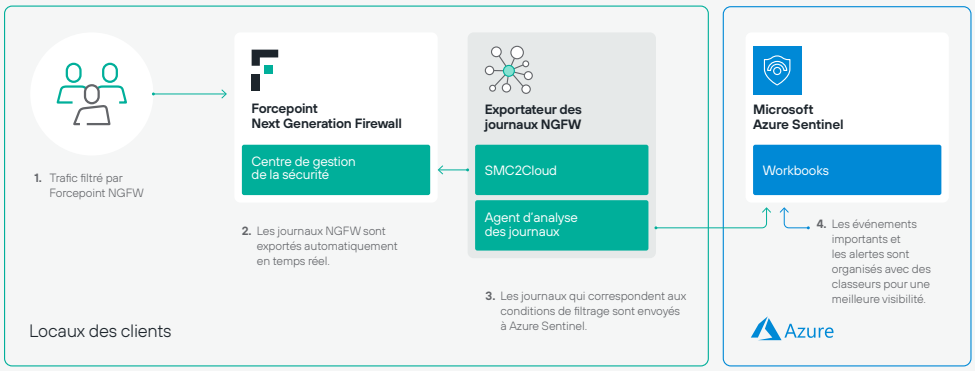
- → Modèle de document ARM configuré pour déployer une pile qui contient 2 équilibreurs de charge réseau et 3 sous-réseaux pour gérer le trafic entre les réseaux internes et externes.
- → Active le fonctionnement des moteurs de Next Generation Firewall en mode haute disponibilité pour assurer un flux réseau ininterrompu entre les utilisateurs et les charges de travail.



Intégration avec Azure Sentinel

Active l'exportation de journaux de données pertinents issus du Next Generation Firewall en fonction des filtres configurés par l'utilisateur.

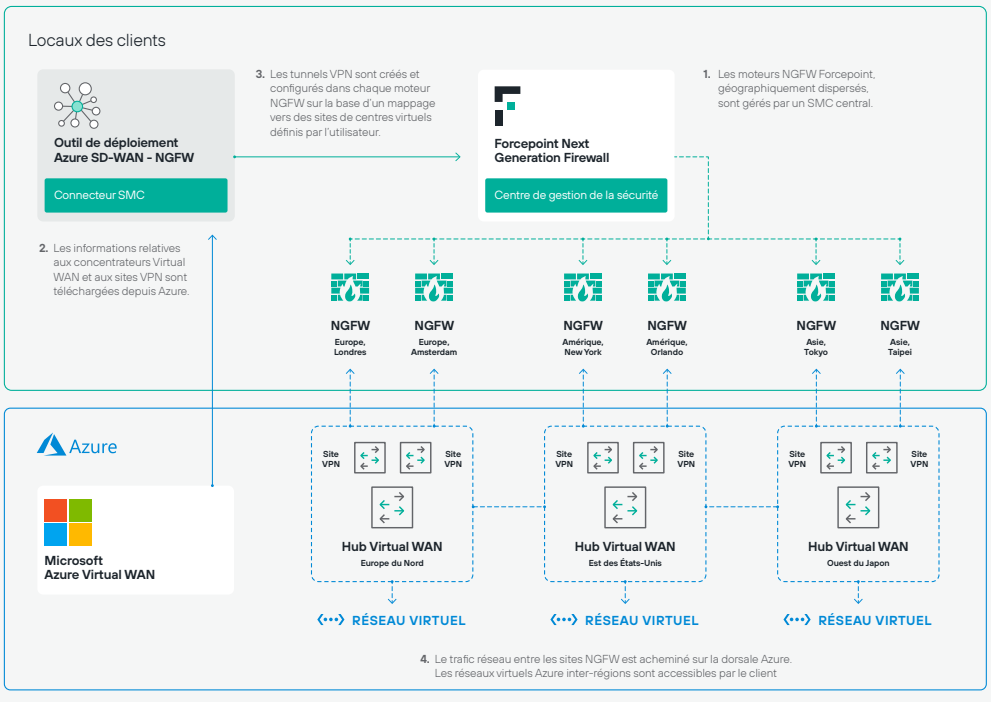
→ Exportation automatique et en temps réel des journaux du Next Generation Firewall vers Azure Sentinel.
→ Intègre les journaux dans le système d'analyse de journaux Azure Sentinel et visualisation des événements à l'aide de Workbooks.



Intégration Azure Virtual WAN

Active la création et la configuration automatique de tunnels IPsec entre une flotte de moteurs de Next Generation Firewall contrôlée par le SMC Forcepoint et des sites géographiques Virtual WAN.

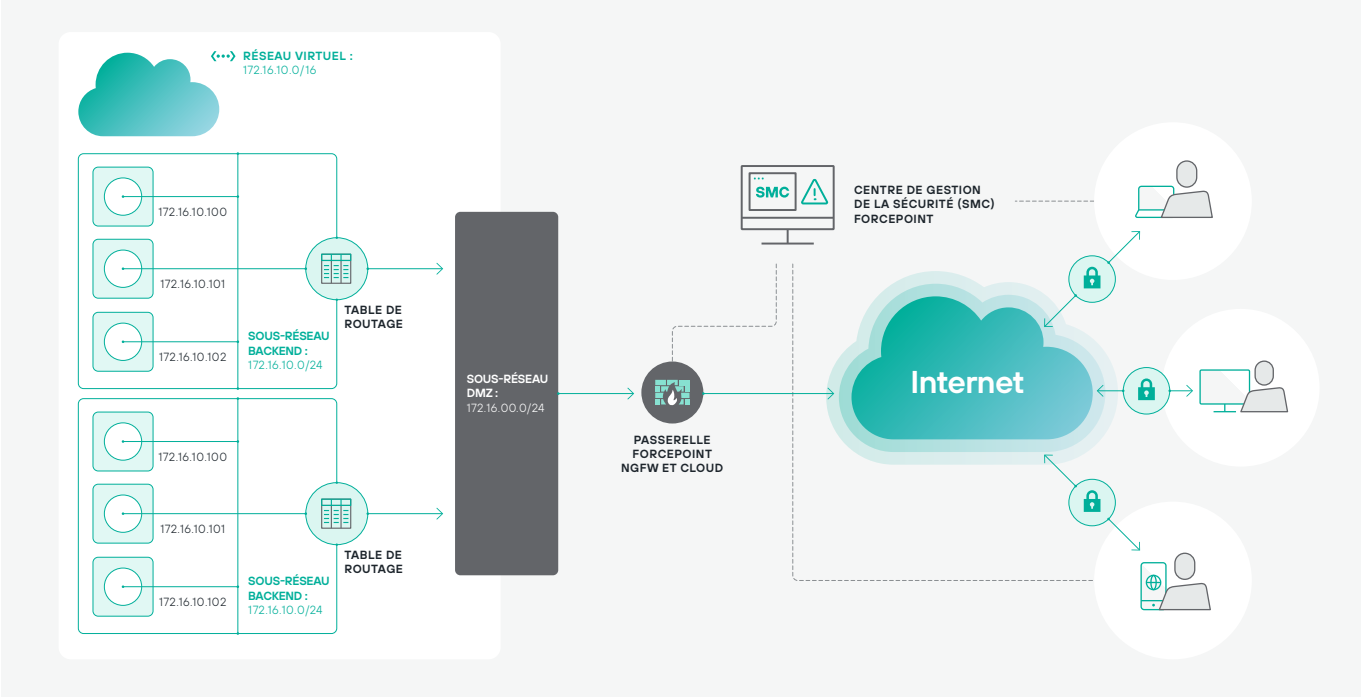
→ Crée une couche SD-WAN qui peut être utilisée pour acheminer le trafic entre les sites vers la dorsale de réseau Azure Virtual WAN
→ Donne aux administrateurs la capacité de créer des tunnels VPN redondants dans chaque moteur Next Generation Firewall contrôlé par le SMC utilisant la norme IPsec
→ Permet de connecter les tunnels VPN de chaque moteur de Next Generation Firewall aux régions WAN virtuelles Azure spécifiées.

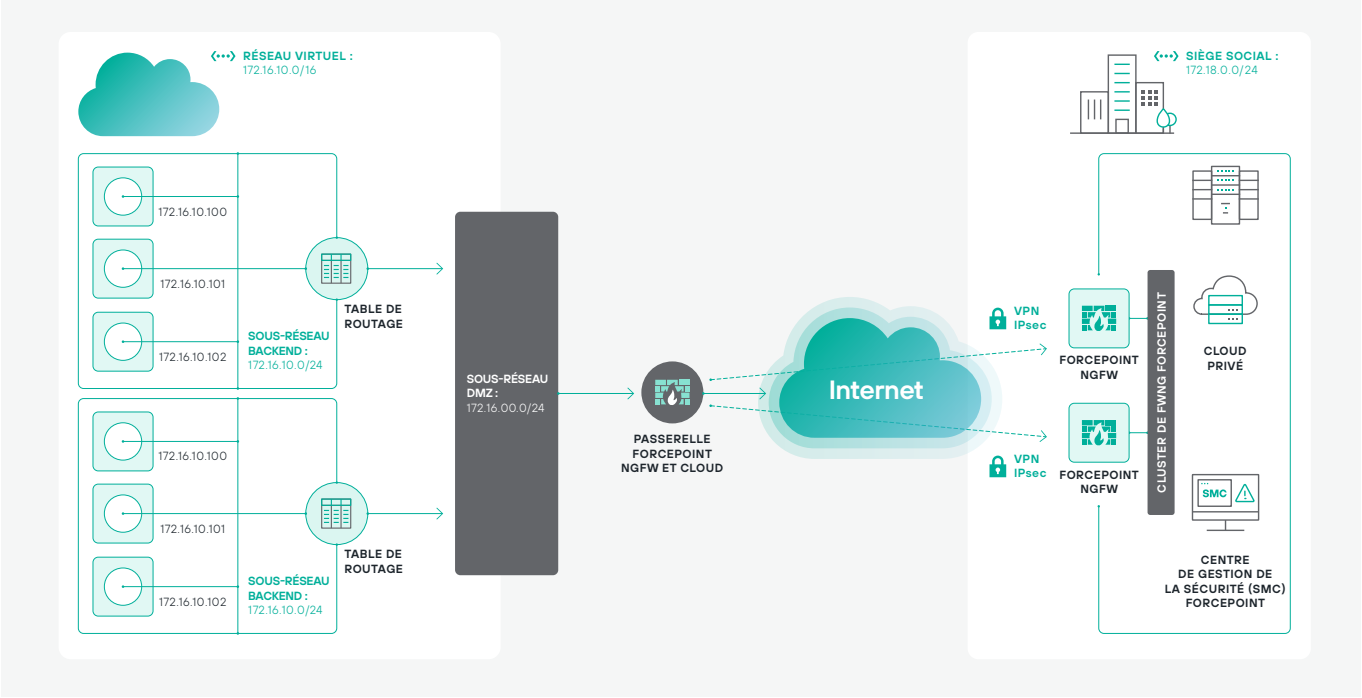


Connectivité avec le Centre de données de l'entreprise

Les passerelles physiques et virtuelles du Forcepoint Next Generation Firewall sécurisent les centres de données sur site de votre entreprise et les centres virtuels du cloud Azure. Pour cela, vous pouvez :

- → Créer une ou plusieurs connexions VPN entre le réseau de votre centre de données et votre appareil VPN logiciel Forcepoint qui s'exécute dans votre réseau virtuel Azure.
- → Gérer et contrôler tous vos Firewalls Forcepoint, logiciels comme physiques, aux deux extrémités des connexions VPN via le SMC.
- → Assurer la continuité des activités côté siège social avec la connexion VPN, mais vous pouvez aussi utiliser un cluster de Firewalls physiques comme solution de secours.





Redirection Inter-régions VNET-to-VNET

Créer des tunnels VPN sécurisés entre deux ou plusieurs appareils VPN logiciel Forcepoint pour connecter des réseaux virtuels à l'intérieur, ou entre plusieurs régions, du cloud Azure. Pour cela, vous pouvez :

→ Gérer, contrôler et appliquer les politiques de sécurité aux deux extrémités de la connexion VPN à l'aide du SMC Forcepoint.