Chapitre 3
Connectivité hybride - VPN

1. Introduction

L'hybridation de votre réseau, c'est-à-dire l'interconnexion de vos environnements privés aux environnements cloud Azure, est une étape clé. Comme évoqué précédemment, et bien que certains services soient accessibles depuis des points de terminaison publics, l'hybridation de votre réseau vous permet d'accéder aux ressources déployées sur des plans d'adressage IP privés. Dès lors, votre environnement Azure, d'un point de vue réseau, est similaire à tout autre site présent dans votre environnement.

Ce chapitre se concentre sur les connectivités hybrides de type VPN : d'abord site à site (S2S) pour l'interconnexion d'un site, puis point à site (P2S) pour l'interconnexion de vos utilisateurs.

2. VPN site à site (S2S)

2.1 Principe et description des VPN site à site Azure

Les réseaux VPN site à site sont une des approches à l'hybridation de vos réseaux avec le cloud Microsoft Azure. La connectivité VPN IPsec, simple et rapide, rend possibles les communications sécurisées entre deux espaces d'adressage privés non conflictuels, qu'il s'agisse par exemple d'interconnecter votre réseau local à Azure ou un autre fournisseur cloud à Azure. Ainsi, l'accès à vos ressources situées dans le cloud Azure se fait au travers d'adressages privés, comme pour vos ressources internes actuelles. Inversement, vos ressources Azure peuvent également joindre les réseaux locaux pour redescendre des données localement ou entre différents fournisseurs cloud.

L'hybridation de vos réseaux rend donc totalement privée une partie de vos ressources internes et ne permet plus d'y accéder librement en dehors de votre réseau d'entreprises. Les ressources publiques et exposées, elles, le resteront, mais seront clairement distinguées en termes de sécurité et d'accès.

Dans Azure, la mise en place d'une connectivité hybride de type VPN requiert différents éléments de configuration :

– Une ou plusieurs passerelles VPN Azure.
– Une ou plusieurs passerelles VPN locales.
– Une connexion VPN entre vos passerelles incluant les configurations IPsec.

Avant d'aborder les spécificités techniques liées aux passerelles VPN, il est important d'évoquer dans un premier temps les différents SKU disponibles.

2.1.1 Passerelles VPN Azure et SKU associés

La mise en place d'une connectivité VPN site à site, dans Azure, repose sur des passerelles de réseau virtuel de type VPN, ou *VPN Gateways*. Ces passerelles VPN assurent la connectivité entre vos passerelles VPN locales (pare-feu, routeur…) et le cloud Azure. Il existe un nombre relativement important de SKU de passerelles VPN, et ce dans le but de répondre au mieux à vos attentes en termes de connectivité et de coût. On distingue cependant deux grands types de passerelles :

– Les passerelles de type Basic (un seul SKU associé).
– Les passerelles de type Standard (l'ensemble des SKU restants).

Les passerelles VPN dites "Basic" sont relativement limitées et ne sont pas recommandées dans le cadre d'architectures importantes ou de déploiements de production avancés. Elles sont même souvent considérées comme obsolètes et seulement utilisées dans des environnements de test. Les limitations associées à ce type de passerelles sont nombreuses et c'est pourquoi il est important de les maîtriser pour orienter au mieux votre décision lors du déploiement.

Pour commencer, les passerelles de SKU Basic sont les seules passerelles dont les VPN sont basés sur une stratégie, ou *Policy-Based*. De par cette configuration, les premières limites ne tardent pas à se faire ressentir. À titre d'exemple, les passerelles ne supportent qu'un seul tunnel et ne peuvent en aucun cas coexister avec un ExpressRoute (cf. chapitre Connectivité hybride - ExpressRoute). De même, il est impossible de déployer du VPN point à site sur cette dernière. Lorsque les VPN sont basés sur des stratégies, les passerelles vont d'abord chiffrer le trafic avant de le rediriger dans le tunnel VPN suivant la liste des réseaux autorisés par stratégie. Le fonctionnement intrinsèque de la passerelle l'oblige donc à n'avoir qu'un seul tunnel, ce qui limite fortement les possibilités de déploiement.

Le reste des passerelles disponibles, dites "Standard", correspondent à l'ensemble des SKU restants. Ces dernières sont plus complètes et reposent cette fois sur un modèle basé sur le routage, ou *Route-Based*. Contrairement au modèle basé sur stratégie, ces passerelles vont d'abord diriger le trafic vers un tunnel, puis le chiffrer. Les décisions de routage reposent sur vos itinéraires, permettant ainsi que plusieurs tunnels puissent être gérés simultanément depuis une même passerelle. De même, le déploiement de VPN point à site ou la cohabitation avec une passerelle ExpressRoute est cette fois supporté.

Plus encore, ces passerelles supportent des configurations fréquemment utilisées dans les réseaux locaux d'entreprise, telles que le routage par BGP (*Border Gateway Protocol*) ou les déploiements de type actif-actif.

Pour être précis, le SKU Basic peut, dans une certaine mesure, être basé sur des itinéraires également. Cependant, celui-ci reste moins complet et notamment limité en termes de tunnel (10 contre 30) ou de fonctionnalités en point à site (pas de Radius, d'IKE…).

Remarque

Le choix du modèle basé sur routage ou stratégie est déterminant car celui-ci ne peut être modifié. Il est impossible de convertir simplement de l'un vers l'autre des modèles. Toutefois, il reste possible de convertir votre passerelle entre différents SKU basés sur des stratégies.

Il existe un nombre important de SKU différents. Le premier SKU ne concerne que les passerelles de type Basic. Pour le reste, il ne s'agit que de passerelles de type Standard. Les SKU se distinguent par la génération de la passerelle, son maximum d'utilisateurs point à site, sa capacité à supporter de la redondance interzone, ou encore et surtout par sa bande passante maximale. La bande passante est le paramètre différenciant le plus souvent retenu pour sélectionner la bonne passerelle de type Standard.

Remarque

Notez que la bande passante indiquée correspond au total cumulé de la passerelle VPN dans sa globalité. Cette mesure inclut donc l'ensemble des tunnels site à site ainsi que les connexions point à site. Un tunnel unique possède une bande passante de 1 Gbps maximum.

La liste complète des passerelles est la suivante, dans l'ordre des SKU et des générations :

SKU	Redondance Inter-zone	Tunnels max S2S/ VNET2VNET	Tunnels max P2S SSTP / IKEv2	Bande passante cumulée	BGP
Basic	✗	10	128 / ✗	100 Mbps	✗
VpnGw1 Generation 1	✗	30	128 / 250	650 Mbps	✓
VpnGw1AZ Generation 1	✓	30	128 / 250	650 Mbps	✓
VpnGw2 Generation 1	✗	30	128 / 250	1 Gbps	✓
VpnGw2AZ Generation 1	✓	30	128 / 250	1 Gbps	✓
VpnGw2 Generation 2	✗	30	128 / 250	1,25 Gbps	✓
VpnGw2AZ Generation 2	✓	30	128 / 250	1,25 Gbps	✓
VpnGw3 Generation 1	✗	30	128 / 1000	1,25 Gbps	✓
VpnGw3AZ Generation 1	✓	30	128 / 1000	1 Gbps	✓
VpnGw3 Generation 2	✗	30	128 / 1000	2,5 Gbps	✓
VpnGw3AZ Generation 2	✓	30	128 / 1000	2,5 Gbps	✓
VpnGw4 Generation 2	✗	30	128 / 5000	5 Gbps	✓
VpnGw4AZ Generation 2	✓	30	128 / 5000	5 Gbps	✓
VpnGw5 Generation 2	✗	30	128 / 10000	10 Gbps	✓

SKU	Redondance Inter-zone	Tunnels max S2S/ VNET2VNET	Tunnels max P2S SSTP / IKEv2	Bande passante cumulée	BGP
VpnGw5AZ Generation 2	✔	30	128 / 10000	10 Gbps	✔

2.1.2 Déploiement des passerelles VPN Azure et passerelles locales

Quel que soit le SKU sélectionné pour votre passerelle, son déploiement se fait sous la forme d'une ressource PaaS. Celle-ci est directement intégrée dans un réseau virtuel, et plus précisément au sein d'un sous-réseau dédié nommé *GatewaySubnet*. Une fois de plus, le déploiement peut être réalisé au travers du portail, de PowerShell, d'Azure CLI ou encore différents outils d'automatisation.

Bien qu'une passerelle apparaisse en tant que ressource PaaS unique lors de sa configuration, celle-ci est nécessairement constituée de deux machines virtuelles sous-jacentes. Ce point est important et nous reviendrons dessus plus tard dans ce chapitre, ainsi que sur les différents types de redondances supportées par les passerelles.

Il est conseillé de déployer votre passerelle dans un sous-réseau en /27, ou moins. Bien qu'un /29 soit tout à fait supporté, il limite à terme l'évolutivité de votre plateforme cloud. Si vous souhaitez par exemple combiner les technologies VPN et ExpressRoute, il est recommandé de déployer un /27 minimum. Notez également que la modification d'un tel plan d'adressage à la suite du déploiement d'une première passerelle peut s'avérer complexe et source d'interruptions de service. Cette démarche inclut en effet la suppression de votre passerelle existante, le redimensionnement du sous-réseau et la création d'une nouvelle passerelle.

Les passerelles VPN Azure déployées dans ce sous-réseau s'interconnectent avec vos passerelles VPN locales au travers d'Internet. L'interconnexion des deux environnements crée une hybridation de vos réseaux et leur permet de communiquer comme s'ils n'en formaient qu'un. À nouveau, attention aux différents plans d'adressage privés qui ne doivent en aucun cas entrer en conflit avec le plan d'adressage utilisé dans votre environnement Azure. Ces passerelles locales doivent être créées dans votre environnement Azure et portent le nom de passerelles VPN locales, ou *local gateway*. Chacune d'entre elles sera déclarée avec son adresse IP publique et les plans d'adressage locaux privés qui lui sont associés. Si deux passerelles locales sont configurées, deux adresses IP publiques sont nécessaires. Les plans d'adressage locaux cibles, eux, peuvent être identiques.

Une liste d'équipements VPN officiellement supportés est disponible directement sur le site de Microsoft. Cette dernière inclut les équipements des acteurs principaux du marché, tels que : Juniper, Arista, Checkpoint, F5, Cisco, Citrix, Palo Alto, SonicWall, Sophos, Ubiquiti ou encore WatchGuard par exemple. Si un constructeur n'apparaît pas, cela ne signifie en aucun cas qu'il est impossible de s'y connecter au travers d'une passerelle Azure. Cependant, le support sera limité et assuré par le constructeur concerné. L'intégration et la connectivité au travers de certains de ces partenaires sont parfois même facilitées par la mise à disposition de configurations prédéfinies, sous forme de script de configuration. Quand bien même des paramètres ne correspondraient pas à vos prérequis et seraient à modifier, vous pourrez entièrement personnaliser ces scripts.

Lorsque vos passerelles VPN Azure et locales sont en place, il ne reste plus qu'à configurer la connectivité VPN entre les deux au travers d'une "connexion" Azure. C'est ici que sont configurés les paramètres IPsec relatifs à vos tunnels VPN.

2.1.3 Politiques IKE/IPsec

Avant d'aborder les concepts de chiffrement et de sécurité liés aux passerelles VPN Azure, revenons sur quelques concepts clés.

Les périphériques VPN situés de part et d'autre d'un tunnel VPN IPsec sont appelés pairs IPsec. Pour qu'une connexion soit effective entre eux, un ensemble de paramètres de chiffrement et d'authentification doivent être échangés entre l'initiateur et le répondeur. Chaque périphérique possède ainsi des listes définies d'arguments appelées SA (*Security Association*), associées aux différentes phases de négociation VPN. Ces dernières doivent correspondre des deux côtés du lien avant de pouvoir continuer les négociations et monter le tunnel.

Ces négociations reposent sur le protocole IKE (*Internet Key Exchange*, v1 ou v2) et se déroulent en deux phases :

– La phase 1, ou ISAKMP SA (*Internet Security Association and Key Management Protocol Security Association*), disponible en mode principal ou mode agressif.

Cette phase initiale permet l'établissement d'une première session sécurisée de type ISAKMP entre les deux extrémités du tunnel. Les algorithmes de hachage et de chiffrement, ou encore les méthodes d'authentification (clé partagée par exemple) y sont négociés.

– La phase 2, ou IPsec SA (*Internet Protocol Security*), disponible en mode rapide ou mode rapide PFS.

Cette seconde phase, réalisée au travers du tunnel déployé en phase 1, permet un échange de clé et l'établissement de deux sessions bidirectionnelles entre vos périphériques. À nouveau, une liste de paramètres, cette fois nécessaires à l'établissement du tunnel IPsec, est négociée. Celle-ci inclut notamment l'algorithme de hachage et de chiffrement, le groupe Diffie Hellman, ou encore la durée de vie de l'association de sécurité.

Ces deux phases peuvent être quelque peu modifiées suivant la version IKE en place. En effet, l'IKEv1 et l'IKEv2 possèdent des caractéristiques particulières et différenciantes, dont certaines sont exposées dans le tableau suivant :

Version	IKEv1	IKEv2
Ports UDP	500	4500
Messages	Phase 1 = 6 ou 3 (*Main mode / Aggressive mode*) Phase 2 = 3 messages	Phase 1 = 4 Phase 2 = 2
Authentification EAP	✗	✓
NAT-Traversal supporté	✗	✓
Paramètre de Keep Alive par défaut	✗	✓
Consommation de bande passante réduite	✗	✓

L'IKEv2 apparaît donc logiquement comme un choix privilégié pour vos déploiements de tunnels site à site. L'IKEv1, quant à lui, intervient plutôt lorsque l'équipement pair ne supporte pas l'IKEv2 ou dans de rares exceptions.

Revenons à présent sur les possibilités offertes par les passerelles VPN Azure au sujet du chiffrement de vos tunnels VPN. Simplement résumé, ces dernières supportent l'ensemble des standards de sécurité et de chiffrement actuels. Elles assurent par conséquent une interopérabilité optimale et s'adaptent à une majorité d'enjeux sécuritaires et de contextes.