Un point de terminaison privé est une interface réseau qui utilise une adresse IP privée de votre réseau virtuel. Cette interface réseau vous connecte de manière privée et sécurisée à un service optimisé par Azure Private Link. En activant un point de terminaison privé, vous intégrez le service dans votre réseau virtuel.

https://learn.microsoft.com/en-us/azure/private-link/private-endpoint-overview

Azure Private Link vous permet d'accéder aux services Azure PaaS (par exemple, stockage Azure et base de données SQL) et aux services hébergés par le client/partenaire Azure via un point de terminaison privé dans votre réseau virtuel.

Le trafic entre votre réseau virtuel et le service transite par le réseau fédérateur Microsoft. L'exposition de votre service à l'Internet public n'est plus nécessaire. Vous pouvez créer votre propre service de liaison privée dans votre réseau virtuel et le proposer à vos clients. La configuration et la consommation à l'aide d'Azure Private Link sont cohérentes dans les services Azure PaaS, détenus par le client et partagés par les partenaires.

Flux de travail

L'application Web reçoit une demande HTTP d'Internet qui nécessite un appel d'API à Azure SQL Database.

Azure Bastion est un service que vous déployez et qui vous permet de vous connecter à une machine virtuelle à l'aide de votre navigateur et le portail Azure Bastion fournit une connectivité RDP et SSH sécurisée à toutes les machines virtuelles du réseau virtuel dans lequel il est provisionné. L'utilisation d'Azure Bastion protège vos machines virtuelles contre l'exposition des ports RDP/SSH au monde extérieur, tout en fournissant un accès sécurisé à l'aide de RDP/SSH.

La machine virtuelle se connecte au réseau virtuel via une interface virtuelle montée dans le ManagementSubnet du réseau virtuel.

Azure Private Link configure un point de terminaison privé pour Azure Keyvault dans le PrivateLinkSubnet du réseau virtuel.

La machine virtuelle envoie une requête pour l'adresse IP d'Azure Keyvault. La requête traverse l'interface virtuelle dans ManagementSubnet. Le CNAME d'Azure Keyvault dirige la requête vers la zone DNS privée. La zone DNS privée renvoie l'adresse IP privée du point de terminaison privé configuré pour Azure Keyvault.

La machine virtuelle se connecte à Azure Keyvault via le point de terminaison privé dans le PrivateLinkSubnet.

Le pare-feu Azure Keyvault autorise uniquement le trafic provenant de PrivateLinkSubnet à se connecter. Le Keyvault est inaccessible depuis l'Internet public.

**Composants**

Ce scénario utilise les services Azure suivants :

* Machine virtuelle Azure
* Hôte Azure Bastion
* Coffre de clés Azure
* Réseau virtuel Azure

Azure Private Link fournit un point de terminaison privé dans un réseau virtuel pour la connectivité aux services Azure PaaS comme Azure Storage et SQL Database, ou aux services client ou partenaire.

Azure DNS héberge des zones DNS privées qui fournissent un service DNS fiable et sécurisé pour gérer et résoudre les noms de domaine dans un réseau virtuel sans qu'il soit nécessaire d'ajouter une solution DNS personnalisée.