UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

SEGMENTATION RÉSEAU

UNIVERSITÉ DU QUÉBEC

CESI
CENTRE D'EXPERTISE EN SÉCURITÉ DE L'INFORMATION

TLP : VERT (DIFFUSION PERMISE)

TABLE DES MATIERES

INTRODUCTION

Les enjeux technologiques auxquels sont confrontées les entreprises de nos jours obligent à penser, concevoir, mettre en place et optimiser l'adressage ainsi que la séparation des *Trafics* en fonction des types et des services fournis. On utilise ici la notion de segmentation du réseau. La segmentation réseau est une approche architecturale qui consiste à diviser celle-ci en plusieurs segments, ou sous-réseau, opérant chacun comme un mini-réseau en soi. Permettant aux administrateurs de contrôler le flux de *trafic* entre ces sous-réseaux en se basant sur des règles granulaires. Les entreprises utilisent la segmentation pour améliorer la surveillance de leur environnement, augmenter les performances, détecter les problèmes techniques, mais aussi, et surtout, pour renforcer leur sécurité.

Grâce à la segmentation, les équipes de sécurité disposent d'un outil puissant pour empêcher les utilisateurs non autorisés (ennemis de l'intérieur ou attaquants externes) d'accéder aux ressources vitales de l'entreprise : données clients, comptes financiers, propriété intellectuelle, etc. Aujourd'hui, ces ressources sont souvent réparties dans des environnements hybrides et multicloud (clouds publics, clouds privés et réseaux SDN) qui nécessitent tous d'être protégés contre les attaques. La segmentation joue un rôle certain dans cette sécurité. Mais afin de comprendre sa pertinence, il est important de se pencher d'abord sur la notion de confiance dans la sécurité du réseau.

OBJECTIF

La segmentation du réseau ne doit pas impliquer la simple division d'un réseau en petits et moyens réseaux, mais doit également répondre aux besoins de l'organisation complémentaire du réseau à exploiter.

- **Où** : Il fait référence à l'établissement des points de segmentation du réseau et à la logique utilisée pour appliquer la segmentation des actifs technologiques de l'organisation.

- **Comment** : Cela a à voir avec la mise en œuvre d'objectifs avec des contrôles d'accès.

- **Quoi** : Renforcez les contrôles d'accès en appliquant des mesures de sécurité avancées et performantes sur l'ensemble du réseau.

Bien entendu, toutes ces questions essentielles trouveront une réponse en fonction du contexte des réseaux que nous gérons. La façon dont vous appliquez les processus de segmentation peut varier considérablement. Par exemple, la microsegmentation. Qui peut être appliqué en fonction des processus exécutés, des applications utilisées, des points de terminaison existants et d'autres critères pouvant être pris en compte.

L'objectif est donc de mieux compartimenter et classifier les actifs de notre réseau pour améliorer la visibilité et rehausser le niveau de sécurité avec les actions de contrôles recommandées.

VISION GLOBALE DE LA SEGMENTATION RESEAU

DÉFINITION

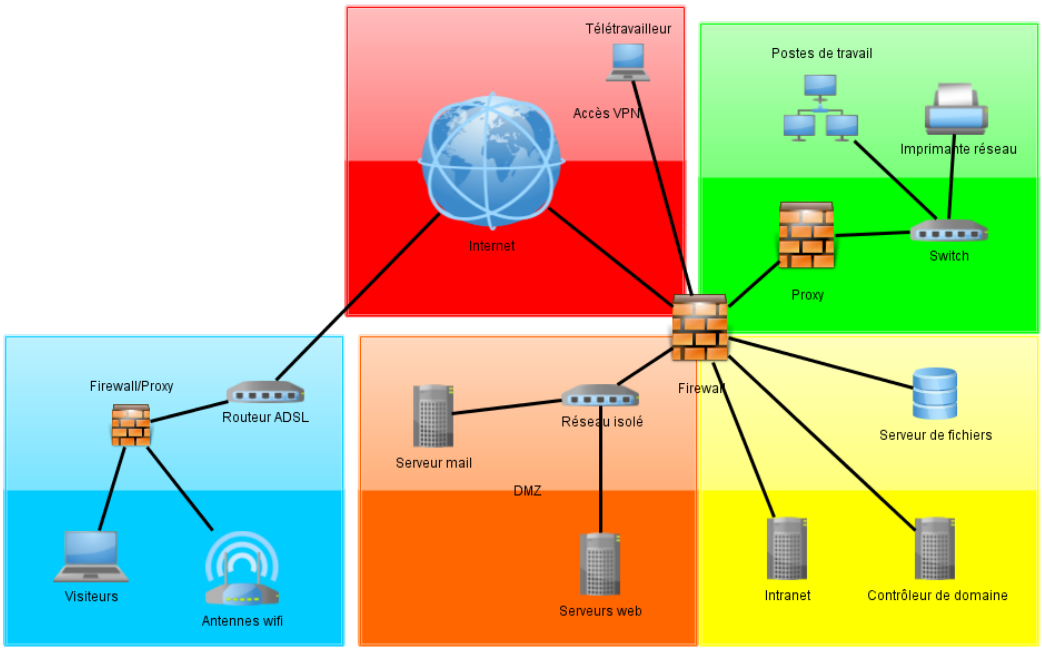
La segmentation réseau est un concept utilisé depuis longtemps par les professionnels de l'informatique pour diviser un réseau physique en plusieurs sous-réseaux. Cette division est réalisée sur une base logique, par le biais d'une approche de réseau défini manuellement, par le logiciel ou SDN (Software-Defined Networking).

Autrement dit, la segmentation réseau consiste à diviser un réseau en segments plus petits et, ce faisant, à séparer les systèmes et les applications les uns des autres. En divisant son réseau, une entreprise rend celui-ci plus performant et efficient, car le *trafic* qui circule dans chaque sous-réseau est particulièrement dédié à la communication entre les appareils qui y sont connectés. Cela n'implique donc aucun ralentissement dû au *trafic*, quels que soient les besoins des utilisateurs connectés au sous-réseau.

La segmentation réseau offre de nombreux avantages que nous allons évoquer un peu plus tard, mais c'est sur le plan de la sécurité que les bénéfices qu'elle génère sont les plus évidents. Grâce à elle, chaque réseau est consacré à des activités ayant besoin de fonctions spécifiques ; et ce sont uniquement les groupes d'employés désignés qui doivent pouvoir y accéder.

À titre d'exemple, la segmentation permet aux équipes de vente, au personnel des ressources humaines et du service à la clientèle d'utiliser les serveurs et les données nécessaires pour l'accomplissement de leur travail, mais uniquement aux serveurs et aux données dont elles ont réellement besoin. Ainsi, il sera plus facile d'assurer la confidentialité et l'intégrité des données.

Si un utilisateur non autorisé tente de s'introduire dans le réseau, ou si une panne se produit, le dommage sera donc limité au sous-réseau ciblé. C'est une façon simple de prévenir, sinon, de contenir les attaques et incidents. Ceci répond parfaitement aux besoins des entreprises de nos jours. **Note** : s'il existe des systèmes qui n'interagissent pas entre eux, il n'est pas nécessaire de les connecter au même réseau. S'ils le sont, il est plus facile pour un pirate informatique d'accéder à tout si les défenses du périmètre sont violées.



1. Vue globale d'une architecture réseau segmentée

AVANTAGES

Le principal avantage de la segmentation du réseau est de limiter les dommages causés par une attaque de cybersécurité. Sur le plan de la surveillance, les systèmes de sécurité peuvent fournir des alertes lorsqu'un terminal non autorisé tente d'accéder au système, identifiant ainsi les attaquants qui tentent de se propager de proche en proche (d'un objet connecté à l'autre, par exemple).

La segmentation peut également réduire la portée d'un audit réglementaire. Par exemple, en ce qui concerne les cartes de paiement, les audits ne doivent concerner que la partie du réseau qui traite et stocke les informations relatives aux cartes de paiement. Bien entendu, ces audits doivent valider les pratiques de segmentation appropriées.

Comme susmentionnée, la segmentation réseau présente de nombreux avantages. Elle peut également contribuer à améliorer les performances de votre infrastructure informatique. Avec moins d'hôtes sur chaque sous-réseau, le *trafic* local est également réduit au minimum. Par ailleurs, elle peut améliorer les capacités de surveillance et aider votre équipe informatique à identifier les comportements suspects.

Voici quelques bonnes raisons pour lesquelles vous devez segmenter votre réseau :

Visibilité accrue : lorsque vous segmentez votre réseau, vous allez installer un pare-feu qui donnera à votre organisation une meilleure visibilité sur tout le *trafic* passant par celui-ci.

Défense en profondeur : vous allez également mettre en place une défense périmétrique qui permettra de détecter et d'empêcher certaines menaces de pénétrer votre réseau.

Amélioration du contrôle d'accès : grâce au pare-feu qui met en œuvre la segmentation de votre réseau, vous pourrez appliquer des politiques de contrôle d'accès et restreindre l'accès au réseau selon les besoins des utilisateurs finaux.

Restriction des mouvements latéraux : en général, les pirates informatiques compromettent les postes de travail des utilisateurs. Pour ce faire, ils doivent se déplacer sur votre réseau afin d'accéder aux systèmes critiques et réussir leurs attaques. Le but de la segmentation réseau est de rendre cette tâche plus difficile et d'augmenter la probabilité de détection lorsque les cybercriminels essayent de franchir les limites des segments.

Gestion des menaces internes : vous pouvez aussi utiliser les défenses basées sur le périmètre pour détecter les menaces internes grâce à une plus grande visibilité des activités malveillantes des employés aux intentions malveillantes et des comptes compromis.

Amélioration des performances du réseau : l'autre objectif de la segmentation réseau est de diviser l'intranet de votre entreprise en plusieurs segments distincts, avec des rôles définis, ce qui réduit le risque de saturation du réseau.

Protection des systèmes critiques : au sein de votre réseau, il existe certains systèmes ayant des exigences de disponibilité très élevées, à l'instar des systèmes de contrôle industriel (ICS). Par conséquent, ces systèmes sont difficiles à protéger et à mettre à jour. Tout particulièrement pour les ICS, vous pouvez minimiser leur exposition aux menaces potentielles en les plaçant sur des segments de réseau isolés.

Sécurisation des systèmes non fiables : de nombreuses entreprises disposent actuellement des réseaux publics invités. L'utilisation croissante des dispositifs IoT (Internet of Things ou Internet des objets)? d'entreprise introduit également un certain nombre d'appareils connectés non sécurisés sur votre réseau. En isolant ces appareils sur un segment de réseau distinct, vous pouvez limiter la menace qu'ils représentent pour votre entreprise.

Limitation de l'accès aux ressources par des tiers : si l'accès à certaines bases de données de votre centre de données devait être fourni à un tiers, la segmentation réseau vous permet de limiter facilement les ressources accessibles pour garantir la sécurité des informations sensibles contre les menaces internes.

Simplification de la conformité

La plupart des tests de conformité, tels que les tests d'intrusion, impliquent toutes les machines de l'organisation qui peuvent accéder aux données protégées. La segmentation du réseau limite la portée de l'accès en confinant les données protégées et sensibles à des segments de réseau spécifiques, simplifiant ainsi vos responsabilités en matière de conformité.

Priorisation des systèmes critiques de l'organisation

Un élément essentiel de la sécurité de l'information consiste à faire une priorisation afin d'offrir le plus de sécurité aux systèmes les plus importants. Cela signifie qu'il faut les placer sur des segments de réseau hautement sécurisés et isolés, minimisant ainsi leur exposition aux menaces. De cette manière, l'organisation concentre ses efforts sur ce qui est essentiel en premier lieu.

Maitrise des réseaux non approuvés

Les réseaux invités, les politiques PAP (prenez vos appareils personnels ou BYOD) et l'utilisation croissante des objets connectés dans les milieux professionnels peuvent introduire des appareils non normalisés et qui ne sont pas forcément sécurisés dans les réseaux de l'organisation. Le fait de mettre ces appareils dans des réseaux dédiés, avec des restrictions adéquates, limite le risque de réussite d'attaques qui les exploitent pour se propager au reste du réseau de l'organisation.

Amélioration de la journalisation des événements

Le passage des flux de données, par un pare-feu ou un routeur, permet une journalisation complète ou partielle des accès autorisés ou bloqués pour des fins d'audit ou d'investigation. Par exemple, dans le cas d'une intrusion, les journaux des accès permettent de comprendre rapidement ce qui s'est passé et d'identifier les systèmes potentiellement compromis afin de pouvoir réagir de manière rapide et efficace.

ARCHITECTURE

Le ciblage VLAN est l'un des moyens de segmentation les plus populaires. Comment ça marche? Création d'un ensemble de réseaux isolés, chacun avec son propre domaine de diffusion au sein d'un réseau de données. L'une des choses que permet la segmentation du réseau au sein d'un VLAN est d'en bloquer l'accès aux cybercriminels qui veulent mener des attaques de toutes sortes. En fin de compte, il existe plusieurs risques de sécurité qui peuvent être atténués. Voici quelques-uns:

Réduction du reniflement de paquets, qui est généralement utilisé pour capturer le *trafic* au niveau de la trame Ethernet, afin d'avoir des informations sensibles des utilisateurs.

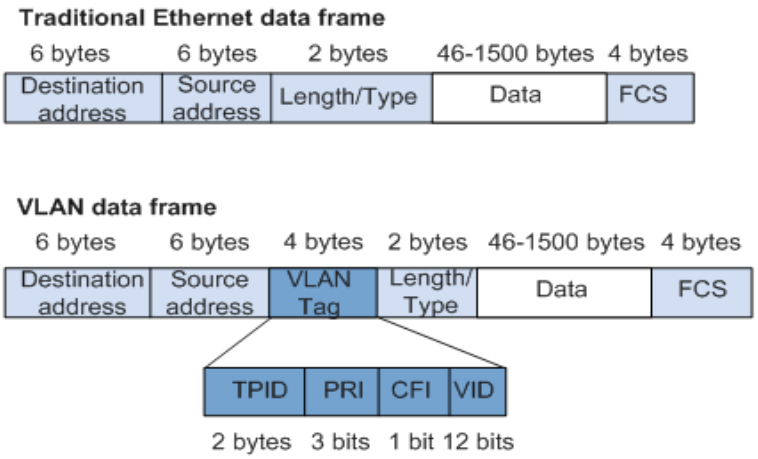
Accès aux serveurs et services uniquement et exclusivement au personnel autorisé.

La segmentation est considérée comme un ensemble de ports, chacun pouvant accepter une variété de périphériques. Ces ports, qui représentent chacun un segment du VLAN, n'ont aucune fonctionnalité tant qu'un appareil n'a pas les autorisations appropriées pour y accéder, grâce aux processus de segmentation. Lorsqu'un appareil souhaite accéder à l'un de ces ports, il est identifié par des données telles que l'adresse MAC, l'adresse IP source, l'adresse IP de destination et bien plus encore.

Il existe de nombreuses stratégies permettant de segmenter efficacement un réseau, mais les réseaux locaux virtuels (VLAN) et les sous-réseaux sont les plus populaires.

- Un VLAN est une structure logique permettant de séparer le *trafic* au niveau d'un commutateur IEEE 802.1Q. ;
- Les sous-réseaux, quant à eux, interviennent au niveau de l'adresse IP et du routeur.

Ces deux éléments sont souvent utilisés ensemble, à parité. De nombreuses approches de la segmentation réseau sont possibles. Il est par exemple courant pour les entreprises de diviser leur réseau en fonction des différents services, en attribuant un VLAN distinct au service financier, au service ingénierie, etc. Le *trafic* entre les services peut ainsi être inspecté ou limité en fonction des exigences métier. L'accès à une base de données des RH internes, par exemple, peut être limité aux appareils du sous-réseau ou du VLAN des RH. Autre approche fréquente : déployer des zones dont les exigences en matière de sécurité diffèrent. Les serveurs et bases de données, par exemple, sont souvent placés dans une « zone démilitarisée » (DMZ), bien plus sécurisée que le reste du réseau. Cette stratégie peut éviter qu'une station de travail infectée ne propage un malware jusqu'aux serveurs hébergeant des données stratégiques. La segmentation peut également se baser sur le type d'appareil. Les appareils IoT notamment sont souvent placés dans leur propre segment réseau pour renforcer la sécurité. Dans le monde de la santé, les machines à rayons X et autres dispositifs médicaux connectés peuvent être tenues à l'écart du reste du réseau. Enfin, il est possible d'associer différentes stratégies en fonction des exigences techniques et métier.



2. Champs d'une trame Ethernet

Type : valeur de 2 octets appelée valeur d'ID de protocole de balise (TPID). Pour Ethernet, il est défini sur 0x8100 hexadécimal.

Priorité : une valeur de 3 bits qui prend en charge la mise en œuvre du niveau ou du service.

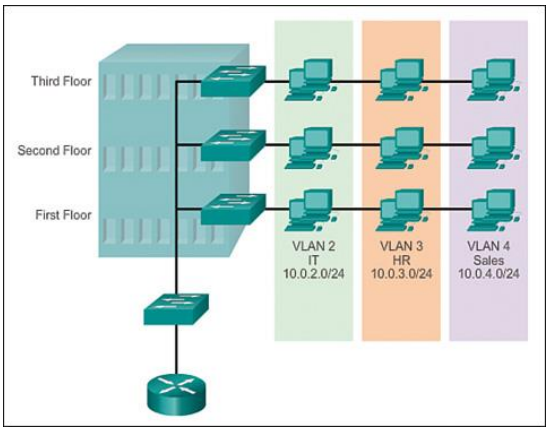
Identificateur de format canonique (CFI) : identificateur de 1 bit qui permet aux trames Token Ring d'être transportées sur des liaisons Ethernet.

ID VLAN (VID) : numéro d'identification VLAN 12 bits prenant en charge jusqu'à 4 096 ID VLAN.

PARTICULARITÉ DES VLANS

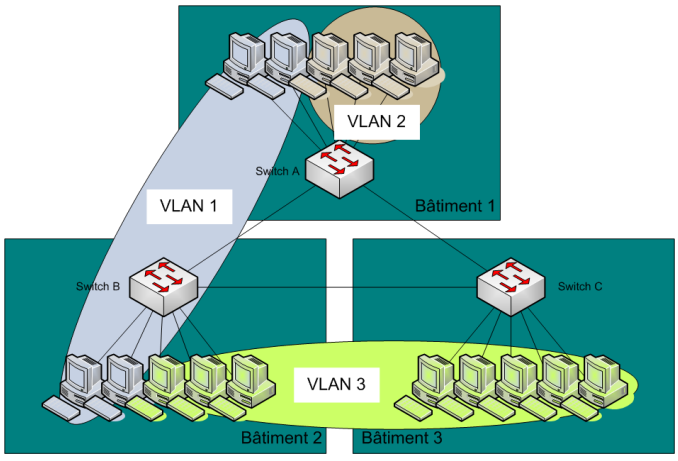
Au sein d'un inter réseau commuté, les VLANs offrent une segmentation et une flexibilité organisationnelle. Les VLANs permettent de regrouper des périphériques au sein d'un VLAN. Un groupe de périphériques au sein d'un VLAN communique comme s'ils étaient connectés au même câble. Les VLANs sont basés sur des connexions logiques, au lieu de connexions physiques.

Les VLANs permettent à un administrateur de segmenter les réseaux en fonction de facteurs tels que la fonction, l'équipe de projet ou l'application, sans tenir compte de l'emplacement physique de l'utilisateur ou de l'appareil. Les appareils au sein d'un VLAN agissent comme s'ils se trouvaient dans leur propre réseau indépendant, même s'ils partagent une infrastructure commune avec d'autres VLANs. Tout port de commutateur peut appartenir à un VLAN, et les paquets de monodiffusion, de diffusion et de multidiffusion sont transmis et inondés uniquement aux stations terminales du VLAN d'où proviennent les paquets. Chaque VLAN est considéré comme un réseau logique distinct et les paquets destinés aux stations qui n'appartiennent pas au VLAN doivent être transférés via un périphérique prenant en charge le routage.

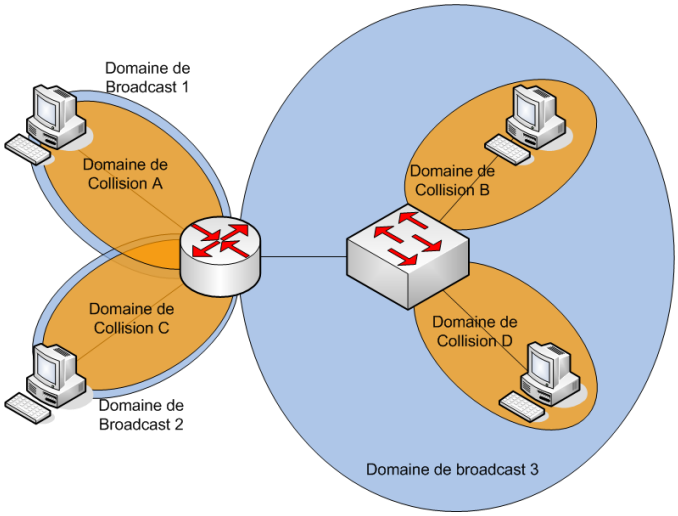


3. Vue globale de VLANs

Un VLAN crée un domaine de diffusion logique qui peut s'étendre sur plusieurs segments VLANs physiques. Les VLANs améliorent les performances du réseau en séparant les grands domaines de diffusion en plus petits. Si un périphérique d'un VLAN envoie une trame Ethernet de diffusion, tous les périphériques du VLAN reçoivent la trame, mais pas les périphériques des autres VLANs.



Domaine de collision (limite vlan)



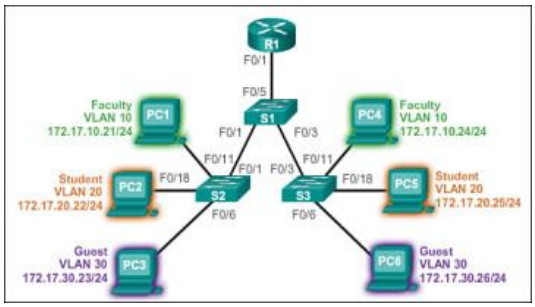
Domaine de diffusion (limite interfaces routeur)

4. Domaine de collision et Domaine de diffusion

Les **domaines de collision** sont des paquets entrant en conflit sur un segment réseau. Les **domaines de diffusion** sont un segment réseau où n'importe quel ordinateur connecté au réseau peut directement communiquer avec tous les autres ordinateurs du même VLAN, sans devoir passer par un routeur.

Les VLANs permettent la mise en œuvre de politiques d'accès et de sécurité en fonction de groupes spécifiques d'utilisateurs. Chaque port de commutateur ne peut être affecté qu'à un seul VLAN (à l'exception d'un port connecté à un téléphone IP ou à un autre commutateur).

AVANTAGES DES VLANS



5. Vue Adressage IP VLANs

La productivité des utilisateurs et l'adaptabilité du réseau sont importantes pour la croissance et le succès de l'entreprise. Les VLANs facilitent la conception d'un réseau pour soutenir les objectifs d'une organisation. Les principaux avantages de l'utilisation des VLANs sont les suivants :

Sécurité : les groupes qui possèdent des données sensibles sont séparés du reste du réseau, ce qui réduit les risques de violation d'informations confidentielles. Comme le montre la Figure ci-dessus, les ordinateurs des professeurs sont sur le VLAN 10 et complètement séparés du *trafic* de données des étudiants et des invités.

Réduction des coûts : les économies de coûts résultent d'un besoin réduit de mises à niveau coûteuses du réseau et d'une utilisation plus efficace de la bande passante et des liaisons montantes existantes.

Meilleures performances : la division des réseaux plats de couche 2 en plusieurs groupes de travail logiques (domaines de diffusion) réduit le *trafic* inutile sur le réseau et améliore les performances.

Réduire les domaines de diffusion : la division d'un réseau en VLAN réduit le nombre d'appareils dans le domaine de diffusion. Comme le montre la Figure ci-dessus, il y a six ordinateurs sur ce réseau mais il y a trois domaines de diffusion : Faculté, Étudiant et Invité.

Amélioration de l'efficacité du personnel informatique : les VLANs facilitent la gestion du réseau, car les utilisateurs ayant des exigences réseau similaires partagent le même VLAN. Lorsqu'un nouveau commutateur est provisionné, toutes les politiques et procédures déjà configurées pour le VLAN particulier sont mises en œuvre lorsque les ports sont attribués. Il est également facile pour le personnel informatique d'identifier la fonction d'un VLAN en lui donnant un nom approprié. Dans la Figure ci-dessus, pour faciliter l'identification, le VLAN 10 a été nommé « Faculté », le VLAN 20 est nommé « Étudiant » et le VLAN 30 « Invité ».

Gestion simplifiée des projets et des applications : les VLAN regroupent les utilisateurs et les périphériques réseau pour répondre aux exigences commerciales ou géographiques. Avoir des fonctions séparées facilite la gestion d'un projet ou le travail avec une application spécialisée ; un exemple d'une telle application est une plate-forme de développement d'apprentissage en ligne pour les professeurs.

MEILLEURES PRATIQUES SEGMENTATION RÉSEAU

La segmentation du réseau est une excellente idée pour minimiser l'impact des violations de données, car elles peuvent toujours se produire. En divisant le réseau en composants plus petits, vous pouvez isoler la section compromise et sauver les autres.

Mais la segmentation d'un réseau peut donner des résultats négatifs si elle n'est pas correctement effectuée en suivant les meilleures pratiques. Notre suggestion est donc de mettre l'accent sur les points mentionnés ci-dessous pour segmenter les réseaux de manière simple, sécurisée et conviviale.

Un résumé à garder en mémoire :

- Implémentation de contrôles sur plusieurs couches du modèle TCP/IP. (Exemple : Filtrage : MAC, IP, port, etc.)
- Application du principe du moindre privilège.
- Répartition des données et de l'infrastructure en respectant les prérequis de sécurité.
- Rejet par défaut de tout *trafic* réseau et autorisation du *trafic* de communication réseau à l'exception, via une liste d'approbation.

De façon plus générale, nos recommandations de meilleures pratiques se présentent comme suit :

Restreindre l'accès des tiers

L'accès de tiers peut être très dangereux pour les réseaux d'entreprise. Rapport 2020 de Forrester ont montré que 46 % des violations de données étaient causées par des initiés ou des tiers. Veillez donc à ne pas donner trop de privilèges et à minimiser les surfaces d'attaque en restreignant l'accès des tiers. Vous pouvez créer des segments spécifiques complètement séparés de votre réseau principal uniquement pour les tiers.

Faciliter l'autorisation & compliquer les accès illégaux

Gardez la segmentation du réseau suffisamment simple pour fournir aux utilisateurs un accès sécurisé sans effort. Surtout, ne laissez pas l'accès légitime au réseau être plus compliqué que l'accès illégal. Vous pourriez penser que cela augmentera la sécurité, mais c'est le contraire. Si la segmentation du réseau entraîne un processus d'accès trop compliqué et ennuyeux, révisez votre architecture et assurez-vous qu'elle offre une bonne expérience utilisateur.

Établir une communication en continu

Il existe un préjugé sur la segmentation réseau, qui voudrait que cette dernière introduise des barrières dans la communication entre départements. Au contraire, pour s'assurer de la mise en place de bons processus de communication, les entreprises peuvent avoir recours à des outils de modélisation du réseau. De cette façon, les contrôles d'accès sont configurés correctement et les processus de communication n'en pâtissent pas.

Avoir recours à l'automatisation

Pour une grande entreprise, engager une segmentation réseau peut s'avérer être un processus long et intensif. Et il se peut que ladite entreprise ne dispose pas des compétences et/ou des ressources nécessaires. Mais c'est à cela que servent les outils d'analyse et de monitorage pour l'automatisation de la sécurité.

Adopter une approche holistique

Les entreprises ont bien souvent une mauvaise perception de la segmentation réseau. Bien entendu, les directives doivent venir des RSSI, mais les équipes réseaux et sécurité doivent travailler en tandem. En adoptant une approche holistique de la segmentation réseau, les entreprises peuvent éliminer les silos en interne.

Suivre le principe du moindre privilège

Lors de la segmentation de votre réseau, il est important de minimiser qui et quoi a accès au sein et entre les systèmes en fonction des besoins réels. En d'autres termes, tout le monde n'a pas besoin d'accéder à toutes les parties du réseau. En suivant le principe du moindre privilège et de l'accès basé sur les rôles, vous pouvez empêcher les hôtes, les services, les utilisateurs et les réseaux d'accéder aux données et aux fonctions qui ne relèvent pas de leur responsabilité immédiate. Cela renforce la sécurité globale de votre réseau tout en facilitant la surveillance et le suivi du *trafic* sur l'ensemble de votre réseau.

Limiter l'accès des tiers

De même, il est important de limiter l'accès des tiers à votre réseau afin de minimiser les points d'entrée exploitables. Les risques d'accès à distance de tiers restent une vulnérabilité clé pour les organisations. En fait, un rapport récent a révélé que 44 % des organisations ont subi une violation au cours des 12 derniers mois, 74 % d'entre elles affirmant que cela résultait d'un accès trop privilégié à des tiers.

"Fournir un accès à distance à des tiers sans mettre en œuvre les mesures de sécurité appropriées garantit presque un incident de sécurité et une violation de données impliquant des informations sensibles et confidentielles", a déclaré le Dr Larry Ponemon, président et fondateur du Ponemon Institute. *"Il est important que les organisations évaluent les pratiques de sécurité et de confidentialité des tiers qui ont accès à leurs réseaux et s'assurent qu'ils ont juste assez d'accès pour s'acquitter de leurs responsabilités désignées et rien de plus."* Une façon d'y parvenir consiste à créer des portails isolés pour les tiers qui ont besoin d'accéder à votre réseau pour fournir des services. Cela limite leur accès aux seules zones de votre réseau qui sont nécessaires.

Auditez et surveillez votre réseau

La segmentation de votre réseau n'est que la première étape d'une stratégie de segmentation solide. L'étape suivante consiste à surveiller et à auditer en permanence votre réseau pour vous assurer que l'architecture est sécurisée et identifier les lacunes de vos sous-réseaux qui pourraient être exploitées. Surveillez votre réseau afin d'identifier et d'isoler rapidement les problèmes de *trafic* ou de sécurité. Effectuez ensuite des audits réguliers pour mettre en évidence les faiblesses architecturales. Ceci est particulièrement important à mesure que votre entreprise évolue et se développe ; à mesure que votre entreprise évolue, votre architecture réseau peut ne plus répondre à vos besoins. Des audits réguliers peuvent vous aider à évaluer quand et où vous devez ajuster la conception de votre segmentation de réseau pour des performances et une sécurité optimale.

Rendre les chemins d'accès légitimes plus faciles que les chemins illégitimes

Lors de l'évaluation et de la planification de la conception de votre architecture, faites attention à la façon dont vous tracez l'accès et aux chemins que les utilisateurs emprunteront pour se connecter à votre réseau. Bien qu'il soit important de créer des points d'accès sécurisés pour vos utilisateurs, faites attention à la manière dont des acteurs malveillants pourraient tenter d'accéder illégalement à

ces mêmes sous-réseaux. Par exemple, supposons que vous ayez des pares-feux entre vos fournisseurs et les données auxquelles ils ont besoin d'accéder, mais seuls certains de ces pares-feux sont capables de bloquer les mauvais acteurs. Si tel est le cas, vous devrez repenser votre architecture. Concevez votre réseau de manière que les chemins légitimes soient plus faciles à parcourir que les chemins illégitimes afin de renforcer votre sécurité.

Combiner des ressources réseau similaires

Gagnez du temps et réduisez les frais de sécurité en combinant des ressources réseau similaires dans des bases de données individuelles. Lorsque vous examinez votre réseau, classez les données par type et degré de sensibilité. Cette segmentation de votre réseau vous permet d'appliquer rapidement des politiques de sécurité tout en protégeant les données plus efficacement.

Ne pas sous ou sursegmenter

L'un des problèmes les plus difficiles de la segmentation du réseau est le degré de segmentation. Vous devez faire attention à ne pas sursegmenter ou sous-segmenter.

Segmenter le réseau plus loin que nécessaire peut créer des difficultés pour les employés. Sans oublier que certains d'entre eux ne pourront pas effectuer de tâches avec des autorisations d'accès trop restreintes.

La sous-segmentation, en revanche, posera des risques de sécurité pour votre réseau. La meilleure façon de bien diviser le réseau est de connaître les besoins des employés pour effectuer leur travail. Spécifiez correctement la description de travail et le segment de chacun.

Gartner note que l'une des erreurs les plus courantes commises par les organisations lors de la segmentation de leurs réseaux est la sur - segmentation ou la création de trop de zones. Avoir trop de segments ajoute une complexité inutile et rend plus difficile la gestion de votre réseau dans son ensemble.

Gardez à l'esprit que vous devez créer des politiques qui définissent ce qui a accès entre chaque paire de zones. Ainsi, plus vous créez de zones, plus vous devez gérer de politiques. La sursegmentation peut rapidement étendre la portée de votre gestion de la sécurité, la rendant coûteuse et inefficace. Pensez-y de cette façon : pendant que vous souhaitez regrouper des ressources réseau similaires, veillez à "construire une clôture autour du stationnement, et non une clôture et une porte autour de chaque voiture".

Visualisez votre réseau

Afin de concevoir une architecture réseau efficace et sécurisée, vous devez d'abord comprendre qui sont vos utilisateurs, quels composants composent votre réseau et comment tous les systèmes sont liés les uns aux autres. En d'autres termes, sans une image claire de votre état actuel, il sera difficile de planifier et d'atteindre l'état souhaité. Visualisez votre réseau avec un diagramme de réseau pour obtenir une vue d'ensemble de toutes les pièces mobiles et identifier qui a besoin d'accéder à quelles données afin que vous puissiez cartographier votre réseau avec succès.

Outils de gestion de VLANs, Sous-Réseau

Pour garantir une meilleure utilisation de l'espace d'adressage IP et des VLANs. Il permet également de prévenir les conflits d'adressage et d'utilisation.

Segmenter via le pare-feu

Les pares-feux constituent également une autre option. Ils peuvent être déployés à l'intérieur d'un centre de données ou d'un réseau afin de créer des zones internes, ce qui permet de segmenter les domaines fonctionnels les uns des autres et de limiter les surfaces

d'attaque. De cette manière, vous pouvez empêcher les menaces de se propager au-delà d'une zone de sécurité. Vous pouvez par exemple séparer les applications d'ingénierie des finances ou protéger les zones sensibles où résident les données PCI.

Les administrateurs réseau et de sécurité ont une bonne connaissance sur les pares-feux qui sont déployés sur le périmètre, mais ils ont souvent tendance à introduire une grande complexité lorsque ces mêmes pares-feux sont utilisés pour effectuer une segmentation interne. La raison est que des milliers de règles de pare-feu doivent être appliquées pour segmenter les réseaux internes et qu'il faut aussi tenir compte du fait qu'une mauvaise configuration du pare-feu pourrait casser une application et nuire à votre entreprise.

Utiliser le réseau défini par logiciel (SDN)

En utilisant le SDN, votre organisation pourra mettre en œuvre la microsegmentation, également appelée segmentation de sécurité ou segmentation basée sur l'hôte. Grâce à cette approche, vous allez pouvoir augmenter la granularité de la segmentation puisque vous allez isoler les charges de travail individuelles les unes des autres. En d'autres termes, vous ne serez plus contraint de travailler à l'échelle de plusieurs points d'extrémité, tel qu'on faisait avec la segmentation réseau dans sa forme traditionnelle.

Cette granularité supplémentaire augmente les avantages de la segmentation, car elle offre un niveau plus élevé de visibilité et de contrôle du réseau. Cette approche tend également à utiliser des modèles de liste blanche qui permettent de bloquer tous les *trafic*s réseau, sauf ceux qui sont autorisés. Le problème avec la segmentation basée sur l'hôte est que les professionnels qui ont souvent besoin d'une certaine période d'adaptation. De plus, la plupart des nouveaux utilisateurs doivent être formés à une nouvelle façon de créer des règles et d'appliquer la segmentation en utilisant le SDN, même s'ils sont familiers avec les pares-feux et les concepts de mise en réseau.

Considérer la microsegmentation

La virtualisation et le SDN offrent plus de granularité dans les contrôles d'accès. Cependant, cela peut s'avérer être à double tranchant, car il devient plus difficile pour les équipes réseau et de sécurité de déterminer les chemins d'accès au réseau. Il est donc nécessaire de disposer d'outils offrant une visibilité sur l'ensemble de l'infrastructure de l'entreprise, qu'il s'agisse d'un environnement physique ou virtuel, d'un centre de données ou d'un cloud.

IMPLÉMENTER DES MODÈLES DE SEGMENTATION RÉSEAU DANS AZURE

SEGMENTATION SELON AZURE

Vous pouvez créer des périmètres à définition logicielle dans votre empreinte réseau à l'aide des différents services et fonctionnalités Azure. Lorsqu'une charge de travail, ou certaines parties d'une charge de travail sont réparties sur plusieurs segments, vous pouvez contrôler le *trafic* qui rentre et sort de ces segments en vue de sécuriser les chemins de communication. Si un segment est compromis, il sera alors plus facile de réduire l'impact de l'attaque et d'empêcher celle-ci de se répandre latéralement dans le reste de votre réseau. Cette stratégie s'aligne sur le principe clé du modèle Confiance Zéro publié par Microsoft, qui vise à fournir une sécurité optimale à votre organisation.

Créez une stratégie d'endiguement des risques qui combine des approches éprouvées, à savoir :

- Contrôles et pratiques de sécurité réseau existants ;
- Contrôles de sécurité natifs disponibles dans Azure ;
- Approches Confiance Zéro.

VUE D'ENSEMBLE

Une stratégie de segmentation d'entreprise unifiée permet aux équipes techniques de segmenter l'accès de façon cohérente en utilisant les contrôles du réseau, des applications, des identités et d'autres contrôles d'accès. Créez une segmentation dans votre empreinte réseau en définissant des périmètres. Voici les principales raisons d'effectuer une segmentation :

- La possibilité de regrouper les ressources associées qui font partie des opérations de charge de travail (ou qui les prennent en charge).
- L'isolation des ressources.
- Les stratégies de gouvernance définies par l'organisation.

SUPPOSER LA COMPROMISSION est l'état d'esprit recommandé en matière de cybersécurité et la capacité à contenir un attaquant est essentielle pour protéger les systèmes informatiques. Modélisez un attaquant capable de pénétrer à divers endroits de la charge de travail et établissez des contrôles pour atténuer toute expansion supplémentaire.

Les contrôles réseau peuvent sécuriser les interactions entre les périmètres. Cette approche permet de renforcer la posture de sécurité et d'empêcher les tentatives de violation. En effet, les contrôles qu'elle utilise sont capables de détecter et de bloquer les attaquants quand ils tentent d'accéder à toute une charge de travail.

L'endiguement de vecteurs d'attaque au sein d'un environnement est critique. En revanche, pour être efficaces dans des environnements cloud, certaines approches traditionnelles peuvent s'avérer inadaptées et les organisations de sécurité peuvent être amenées à faire évoluer leurs méthodes.

Les approches traditionnelles de la segmentation ne parviennent généralement pas à atteindre leurs objectifs, car elles n'ont pas été développées selon une méthode pour s'aligner sur les cas d'utilisation d'entreprise et les charges de travail d'application. Souvent, ceci entraîne une complexité importante nécessitant de nombreuses exceptions de pare-feu.

Une meilleure pratique naissante en pleine évolution consiste à adopter une stratégie de Confiance Zéro basée sur les identités d'utilisateur, d'appareil et d'application. Contrairement aux contrôles d'accès réseau basés sur des éléments tels que les adresses IP source et de destination, des protocoles et des numéros de port, le modèle Zero Trust applique et valide un contrôle d'accès AU MOMENT DE L'ACCÈS. Cela évite d'avoir à faire des prédictions pour un déploiement, un réseau ou un sous-réseau entier : seule la ressource de destination doit fournir les contrôles d'accès nécessaires.

- Il est possible d'utiliser des groupes de sécurité réseau Azure pour les contrôles d'accès de base de couches 3 et 4 entre les réseaux virtuels Azure, leurs sous-réseaux et Internet.
- Azure Web Application Firewall et le Pare-feu Azure permettent d'effectuer des contrôles d'accès réseau plus avancés qui nécessitent la prise en charge de la couche Application.
- La solution de mot de passe d'administrateur local (LAPS) ou une solution Privileged Access Management tierce peut définir des mots de passe d'administrateur local forts et un accès juste à temps à ces derniers.

Comment l'organisation implémente-t-elle la segmentation réseau ?
Nous présentons certaines fonctionnalités de réseau Azure qui permettent de créer des segments et de restreindre l'accès à certains services.

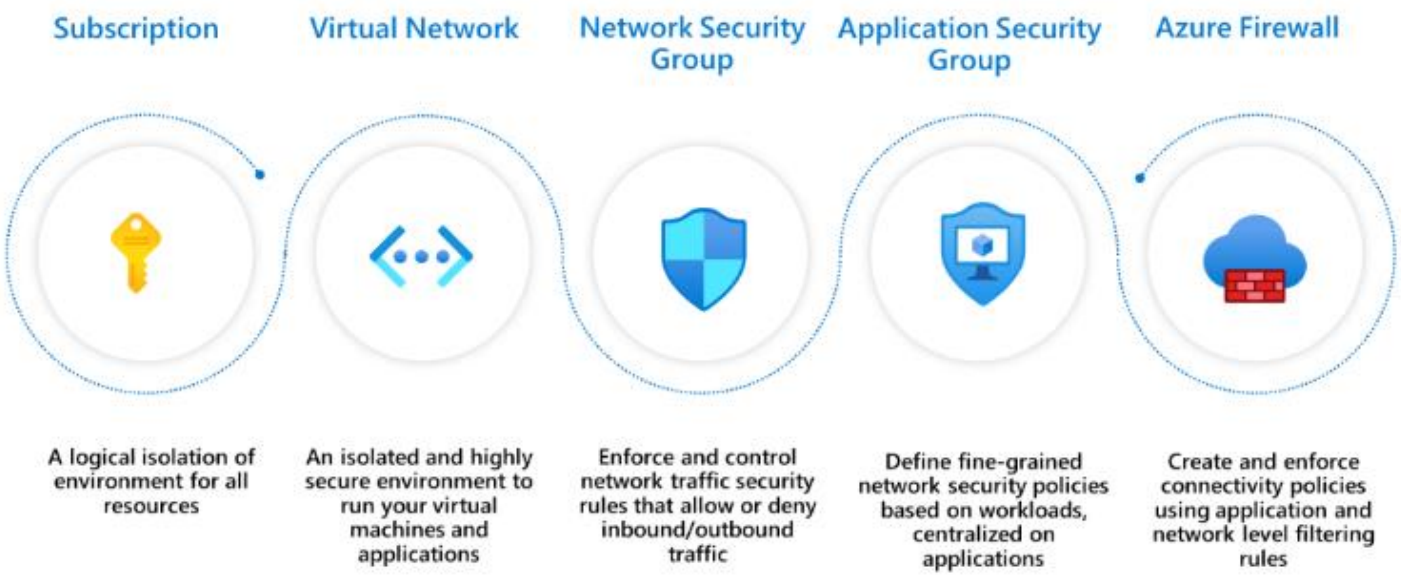
Alignez votre stratégie de segmentation réseau sur le modèle de segmentation de l'entreprise. Cela permet aux différentes équipes techniques (mise en réseau, identité, applications, etc.) d'éviter toute confusion et de réduire les éventuelles difficultés. Les équipes ne doivent pas développer des modèles de segmentation et de délégation chacune de leur côté si ceux-ci ne s'alignent pas les uns sur les autres.

Quelques points clés :

- Créez des périmètres à définition logicielle dans votre empreinte réseau et sécurisez des chemins de communication entre eux.
- Établissez une stratégie de segmentation Confiance Zéro complète.
- Alignez les équipes techniques de l'entreprise sur les stratégies de microsegmentation pour les applications héritées.
- Les réseaux virtuels Azure sont créés dans des espaces d'adressage privés. Par défaut, aucun *trafic* n'est autorisé entre deux réseaux virtuels. Vous ne devez ouvrir des chemins réseau que lorsque cela est vraiment nécessaire.
- Utilisez des groupes de sécurité réseau (NSG) pour sécuriser la communication entre les ressources d'un réseau virtuel.
- Utilisez les groupes de sécurité d'application afin de définir des règles de *trafic* pour les machines virtuelles sous-jacentes qui exécutent la charge de travail.
- Utilisez le Pare-feu Azure pour filtrer le *trafic* entre les ressources cloud, Internet et locales.
- Si vous n'avez pas besoin d'exercer dans plusieurs régions, placez les ressources dans un même réseau virtuel.
- Si vous devez exercer dans plusieurs régions, vous devez connecter plusieurs réseaux virtuels par le biais d'un peering.
- Pour les configurations avancées, utilisez une topologie hub-and-spoke. Un réseau virtuel est désigné comme hub dans une région donnée pour tous les autres réseaux virtuels qui sont désignés comme des spokes dans cette même région.

FONCTIONNALITÉS DE SEGMENTATION RÉSEAU DANS AZURE

Lorsque vous travaillez dans Azure, vous disposez de nombreuses options de segmentation.



6. Segmentation vue Azure

Abonnement: construction de haut niveau qui fournit une séparation des entités reposant sur une plateforme. Celle-ci est destinée à définir les limites entre les grandes organisations d'une entreprise. En outre, la communication entre les ressources de différents abonnements doit être explicitement provisionnée.

Réseau virtuel : créer au sein d'un abonnement dans des espaces d'adressage privés. Il fournit aux ressources une autonomie au niveau du réseau. Par défaut, aucun *trafic* n'est autorisé entre deux réseaux virtuels. Comme les abonnements, toute communication entre les réseaux virtuels doit être approvisionnée de manière explicite.

Groupes de sécurité réseau (NSG) : mécanismes de contrôle d'accès permettant de contrôler le *trafic* entre les ressources au sein d'un réseau virtuel, et également avec les réseaux externes, comme Internet, d'autres réseaux virtuels, etc. Les groupes de sécurité réseau permettent une stratégie de segmentation précise, grâce à la création de périmètres pour un sous-réseau, une machine virtuelle ou un groupe de machines virtuelles. Pour plus d'informations sur les opérations qu'il est possible d'effectuer avec les sous-réseaux dans Azure, consultez Sous-réseau (réseaux virtuels Azure).

Groupes de sécurité d'application (ASG) : similaires aux groupes de sécurité réseau, mais référencés avec un contexte d'application. Cela vous permet de regrouper un ensemble de machines virtuelles sous une balise d'application et de définir des règles de *trafic* qui sont ensuite appliquées à chacune des machines virtuelles sous-jacentes.

Pare-feu Azure : pare-feu natif cloud avec état fourni en tant que service, qui peut être déployé dans un réseau virtuel ou dans des déploiements de hubs Azure Virtual WAN pour le filtrage du *trafic* entre les ressources cloud, Internet et locales. Vous créez des règles ou des stratégies (à l'aide du Pare-feu Azure ou d'Azure Firewall Manager) en spécifiant l'autorisation/refus du *trafic* à l'aide des

contrôles de couche 3 à 7. Vous pouvez également filtrer le *trafic* vers Internet en utilisant à la fois Pare-feu Azure et des tiers en dirigeant tout ou partie du *trafic* via des fournisseurs de sécurité tiers pour le filtrage avancé et la protection des utilisateurs.

MODÈLE DE SEGMENTATION

Voici quelques modèles courants permettant de segmenter une charge de travail dans Azure. Chaque modèle fournit un type d'isolation et de connectivité différent. Choisissez un modèle répondant aux besoins de votre organisation.

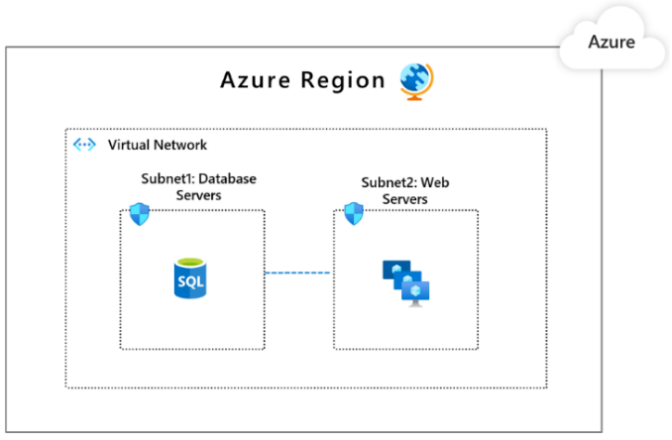
MODÈLE 1 : RÉSEAU VIRTUEL UNIQUE

Tous les composants de la charge de travail se trouvent dans un même réseau virtuel. Ce modèle convient si vous exercez dans une seule région, car un réseau virtuel ne peut pas s'étendre sur plusieurs régions.

Les méthodes courantes permettant de sécuriser des segments, comme des sous-réseaux ou des groupes d'applications, consistent à utiliser des groupes de sécurité réseau et des groupes de sécurité d'application. Vous pouvez également utiliser une application virtuelle réseau issue de la Place de marché Azure ou du Pare-feu Azure, afin d'appliquer et de sécuriser cette segmentation.

Dans cette image, Subnet1 comprend la charge de travail de la base de données. Subnet2 comprend les charges de travail web. Vous pouvez configurer des groupes de sécurité réseau qui autorisent Subnet1 à communiquer uniquement avec Subnet2, et Subnet2 à ne communiquer qu'avec Internet.

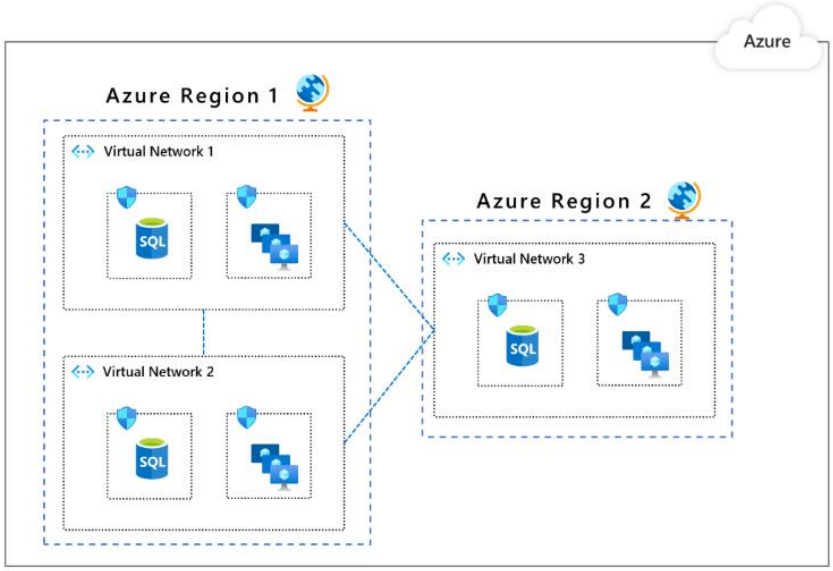
Prenons l'exemple d'un cas d'usage impliquant plusieurs charges de travail placées dans des sous-réseaux distincts. Vous pouvez placer des contrôles qui permettront à une charge de travail de communiquer avec le back-end d'une autre charge de travail.



MODÈLE 2 : PLUSIEURS RÉSEAUX VIRTUELS QUI COMMUNIQUENT PAR LE BIAIS D'UN PEERING

Les ressources sont réparties ou répliquées sur plusieurs réseaux virtuels. Les réseaux virtuels peuvent communiquer par le biais d'un peering. Ce modèle convient si vous devez regrouper des applications dans des réseaux virtuels séparés, ou si vous avez besoin de plusieurs régions Azure. L'un des avantages de ce modèle est la segmentation intégrée, car vous devez appairer explicitement un

réseau virtuel avec un autre. Le peering de réseaux virtuels n'est pas transitif. Vous pouvez effectuer une segmentation supplémentaire à l'intérieur d'un réseau virtuel en utilisant des groupes de sécurité réseau et des groupes de sécurité d'application, comme indiqué dans le modèle 1.



8. Azure Virtual Network multi-connexion

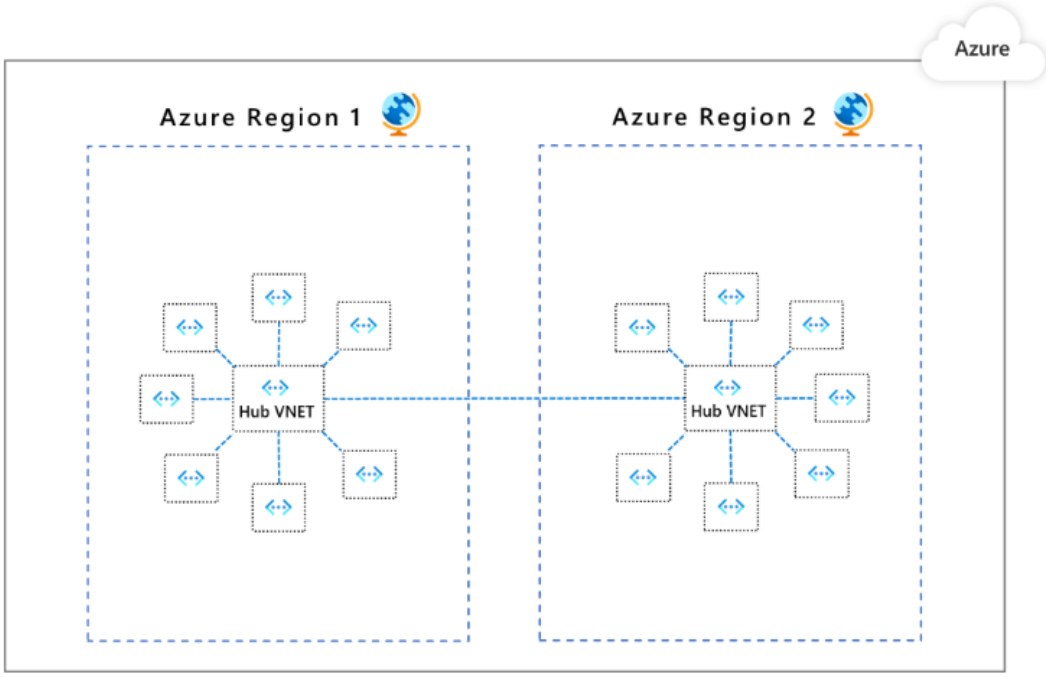
MODÈLE 3 : PLUSIEURS RÉSEAUX VIRTUELS DANS UN MODÈLE HUB-AND-SPOKE

Un réseau virtuel est désigné comme HUB dans une région donnée pour tous les autres réseaux virtuels qui sont désignés comme des SPOKES dans cette même région. Le hub et ses *spokes* sont connectés par le biais d'un peering. Tout le *trafic* transite par le hub et peut servir de passerelle pour les hubs d'autres régions. Dans ce modèle, les contrôles de sécurité sont configurés au niveau des hubs afin de pouvoir segmenter et contrôler le *trafic* entre les autres réseaux virtuels de façon scalable. L'un des avantages de ce modèle est que, lorsque votre topologie de réseau s'étend, les frais liés à la posture de sécurité n'augmentent pas (sauf lorsque vous effectuez une extension vers de nouvelles régions).

L'option native recommandée est le Pare-feu Azure. Cette option fonctionne à la fois sur les réseaux virtuels et sur les abonnements et a pour but de régir les flux de *trafic* à l'aide des contrôles des couches 3 à 7. Vous pouvez définir vos règles de communication et les appliquer de manière cohérente. Voici quelques exemples :

- Le réseau virtuel 1 ne peut pas communiquer avec le réseau virtuel 2, mais il peut communiquer avec le réseau virtuel 3.
- Le réseau virtuel 1 ne peut pas accéder à l'Internet public, sauf à *.github.com.

Avec la préversion d'Azure Firewall Manager, vous pouvez gérer de façon centralisée des stratégies sur plusieurs Pare-feu Azure et permettre aux équipes DevOps de personnaliser davantage les stratégies locales.



9. Azure Virtual Network peering par region

COMPARAISON DES MODÈLES

Considérations	Modèle 1	Modèle 2	Modèle 3
Connectivité/Routage : comment chacun des segments communique avec les autres	Le routage système fournit une connectivité par défaut à n'importe quelle charge de travail d'un sous-réseau.	Identique au modèle 1.	Aucune connectivité par défaut entre les réseaux spokes. Pour permettre la connectivité, le hub doit comprendre un routeur de couche 3, comme le Pare-feu Azure.
Filtrage du trafic au niveau du réseau	Le trafic est autorisé par défaut. Utilisez des groupes de sécurité réseau et des groupes de sécurité d'application pour filtrer le trafic.	Identique au modèle 1.	Le trafic entre les réseaux virtuels Spoke est refusé par défaut. Ouvrez les chemins sélectionnés pour autoriser le trafic via la configuration du Pare-feu Azure.
Journalisation centralisée	Journaux des groupes de sécurité réseau et des groupes de sécurité d'application pour le réseau virtuel.	Agrégez les journaux des groupes de sécurité réseau et des groupes de sécurité d'application de tous les réseaux virtuels.	Le Pare-feu Azure journalise tout le trafic accepté ou refusé qui est envoyé au hub. Affichez les journaux dans Azure Monitor.
Points de terminaison publics ouverts involontaires	DevOps peut ouvrir accidentellement un point de terminaison public par le biais de règles NSG/ASG incorrectes.	Identique au modèle 1.	Un point de terminaison public ouvert accidentellement dans un spoke ne permettra pas l'accès, car le paquet de retour sera supprimé via un pare-feu avec état (routage asymétrique).
Protection au niveau de l'application	Les groupes de sécurité réseau et les groupes de sécurité d'application fournissent uniquement la prise en charge de la couche réseau.	Identique au modèle 1.	Le Pare-feu Azure prend en charge le filtrage de nom de domaine complet pour HTTP/S et MSSQL pour le trafic sortant et entre les réseaux virtuels.

10. Microsoft Azure comparaison des modèles

LA MICROSEGMENTATION

DÉFINITION DE LA MICROSEGMENTATION

La microsegmentation est une technique de cybersécurité qui permet aux entreprises de mieux gérer l'accès réseau entre les ressources (par exemple, le *trafic* de serveur à serveur/**est-ouest**). En identifiant de façon unique chaque ressource (p. ex. serveur, application, hôte, utilisateur), votre entreprise peut configurer des autorisations qui permettent un contrôle fin du *trafic* de données. Lorsqu'elle est mise en œuvre selon les principes de **Zero Trust**, la **microsegmentation** vous permet de stopper le **déplacement latéral des menaces**, d'empêcher la compromission de la charge de travail et de mettre fin aux violations de données.

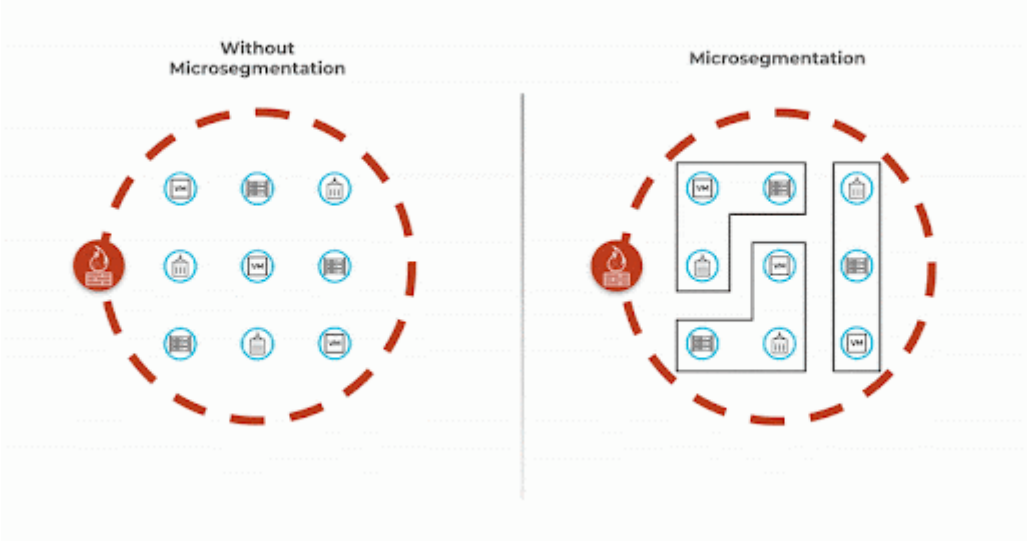
DIFFÉRENCES ENTRE MICROSEGMENTATION ET SEGMENTATION RÉSEAUX

Bien que la segmentation du réseau et la microsegmentation soient souvent utilisées de manière interchangeable, il s'agit de concepts complètement différents.

La segmentation du réseau convient mieux au *trafic* nord-sud, c'est-à-dire le *trafic* qui entre et sort du réseau. Avec la segmentation du réseau, une entité, telle qu'un utilisateur, est considérée comme fiable une fois qu'elle se trouve dans une zone définie du réseau.

La microsegmentation, quant à elle, convient mieux au *trafic* est-ouest, c'est-à-dire au *trafic* qui se déplace latéralement à travers le data center ou le réseau en cloud (de serveur à serveur, d'application à serveur, etc.). Pour simplifier, la segmentation du réseau est comparable aux murs extérieurs et aux douves d'un château, tandis que la microsegmentation serait les gardes qui se tiennent à chacune des portes intérieures du château.

11. Comparaison MicroSegmentation et Segmentation



12. Microsegmentation avec plus de granularité

FAIBLESSES DE LA SEGMENTATION RÉSEAU

Les solutions de microsegmentation traditionnelles basées sur le réseau s'appuient sur des pares-feux, qui utilisent les adresses réseau pour faire appliquer les règles. Mais les réseaux étant en constante évolution, les politiques doivent être continuellement mises à jour au fur et à mesure que les applications et les appareils se déplacent, ce qui représente un véritable défi pour les data centers sur site, dans les environnements multiclouds et là où les adresses IP sont éphémères.

De plus, les approches de segmentation basées sur l'adresse réseau ne peuvent pas identifier ce qui communique : elles ne peuvent par exemple pas déterminer l'identité du logiciel. Elles peuvent uniquement vous dire comment cela communique, par exemple avec l'adresse IP, le port ou le protocole d'où provient la « requête ». Cela signifie que, tant qu'elles sont jugées sûres, les communications sont autorisées, même si les équipes informatiques et de sécurité ne savent pas exactement ce qui tente de communiquer.

En outre, dès qu'une entité se trouve à l'intérieur d'une « zone sécurisée » sur le réseau, elle est considérée comme fiable, ce qui peut entraîner des failles et, sur un réseau plat, des déplacements latéraux.

La microsegmentation est unique en ce qu'elle permet au service informatique de fonder les politiques et les autorisations sur l'identité des ressources, ce qui en fait la méthode idéale pour créer des groupements intelligents de charges de travail basés sur les caractéristiques des charges de travail individuelles communiquant à l'intérieur du data center.

Qui plus est, la microsegmentation ne repose pas sur des réseaux en évolution dynamique ni sur les exigences commerciales ou techniques qui leur sont imposées, elle est donc à la fois plus solide et plus fiable pour la sécurité du réseau.

Elle est également beaucoup plus simple à gérer. Vous pouvez en effet protéger un segment avec seulement quelques politiques basées sur l'identité au lieu de centaines de politiques de pare-feu basées sur l'adresse.

LES AVANTAGES DE LA MICROSEGMENTATION

SÉCURITÉ PROACTIVE DU RÉSEAU ET DE L'INFORMATIQUE

La microsegmentation élimine les obstacles à la sécurité communs à la segmentation traditionnelle en créant des politiques adaptées aux applications qui accompagnent toutes les applications et tous les services. Ainsi, les violations potentielles de données sont limitées aux ressources concernées, et non à l'ensemble du réseau. Certains services de microsegmentation proposent même des fonctionnalités qui reposent sur l'automatisation pour identifier tous les logiciels communicants, recommander des politiques de **Zero Trust** et vous permettre de les appliquer en un clic.

DIMINUTION DE LA VULNÉRABILITÉ

Au lieu de contrôles statiques qui s'appuient sur les adresses IP, les ports et les protocoles, les équipes peuvent prendre l'empreinte cryptographique de chaque charge de travail afin de fournir une protection cohérente aux charges de travail opérant dans un data center interne ou dans le cloud. La prise d'empreinte dissocie la sécurité de votre charge de travail des structures d'adresses IP pour éviter les problèmes liés aux contrôles basés sur l'IP.

ÉVALUATION CONTINUE DES RISQUES

La microsegmentation vous permet de quantifier votre exposition aux risques en mesurant automatiquement la surface d'attaque visible de votre réseau pour appréhender le nombre de voies de communication possibles utilisées entre les applications. Certains services vérifient même les identités des logiciels communicants chaque fois qu'un logiciel sollicite une communication, ce qui atténue les risques, prend en charge les mandats de conformité réglementaire et fournit des rapports de risques visualisés.

SEGMENTATION ZERO TRUST

Comme mentionné plus haut, un modèle de sécurité Zero Trust repose sur les principes de la microsegmentation. La politique est appliquée aux charges de travail, et non aux segments du réseau, ce qui vous permet de dénier toute confiance à toute ressource à tout emplacement pour laquelle vous ne pouvez pas établir un contexte suffisant.

Par exemple, avec un modèle Zero Trust, en particulier un modèle basé sur le cloud, une société pourrait mettre en place une politique stipulant que les appareils médicaux ne peuvent parler qu'à d'autres appareils médicaux. Si un terminal ou une charge de travail devait se déplacer, les politiques et attributs de sécurité se déplaceraient avec eux en temps réel.

DÉFINITION ZERO TRUST

Zero Trust est un cadre destiné à sécuriser les entreprises dans un monde mobile et cloud, qui stipule qu'aucun utilisateur ou application ne doit être considéré comme fiable par défaut. Suivant un principe fondamental de Zero Trust, l'accès basé sur le moindre privilège, la confiance est établie sur la base du contexte (par exemple, l'identité et l'emplacement de l'utilisateur, la posture de sécurité du terminal, l'application ou le service demandé) avec des contrôles de politique à chaque étape.

Une architecture Zero Trust obéit à la maxime « ne jamais faire confiance, toujours vérifier ».

LIENS UTILES ET RÉFÉRENCES

https://www.cases.lu/knowhow/glossary/NetworkSegmentation_fr.html

https://fr.wikipedia.org/wiki/IEEE_802.1Q

https://standards.ieee.org/ieee/802.1Q/6844/

https://www.researchgate.net/figure/Structure-of-framework-IEEE-8021Q_fig4_266201925

https://www.ciscopress.com/articles/article.asp?p=2208697&seqNum=4

https://reussirsonccna.fr/introduction-aux-vlans/

https://reussirsonccna.fr/domaine-de-collision-et-de-diffusion/

https://fr.wikipedia.org/wiki/Domaine_de_diffusion

https://fr.wikipedia.org/wiki/Domaine_de_collision

https://itigic.com/fr/4-network-segmentation-best-practices-to-level-up/

https://www.globalsecuritymag.fr/Segmentation-reseau-tirer-le,20190408,86016.html

https://www.strongdm.com/blog/network-segmentation

https://securityscorecard.com/blog/network-segmentation-best-practices-to-maximize-cybersecurity

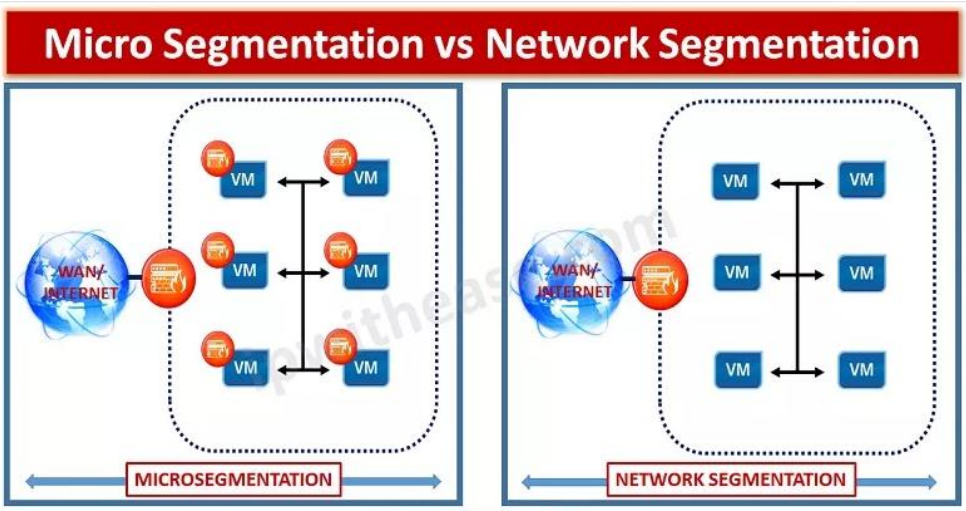
https://docs.microsoft.com/fr-fr/azure/architecture/framework/security/design-network-segmentation

https://networkinterview.com/micro-segmentation-vs-network-segmentation/

https://networkinterview.com/wp-content/uploads/2019/10/microsegmentation-vs-network-segmentation.png

https://www.paloaltonetworks.com/cyberpedia/what-is-microsegmentation

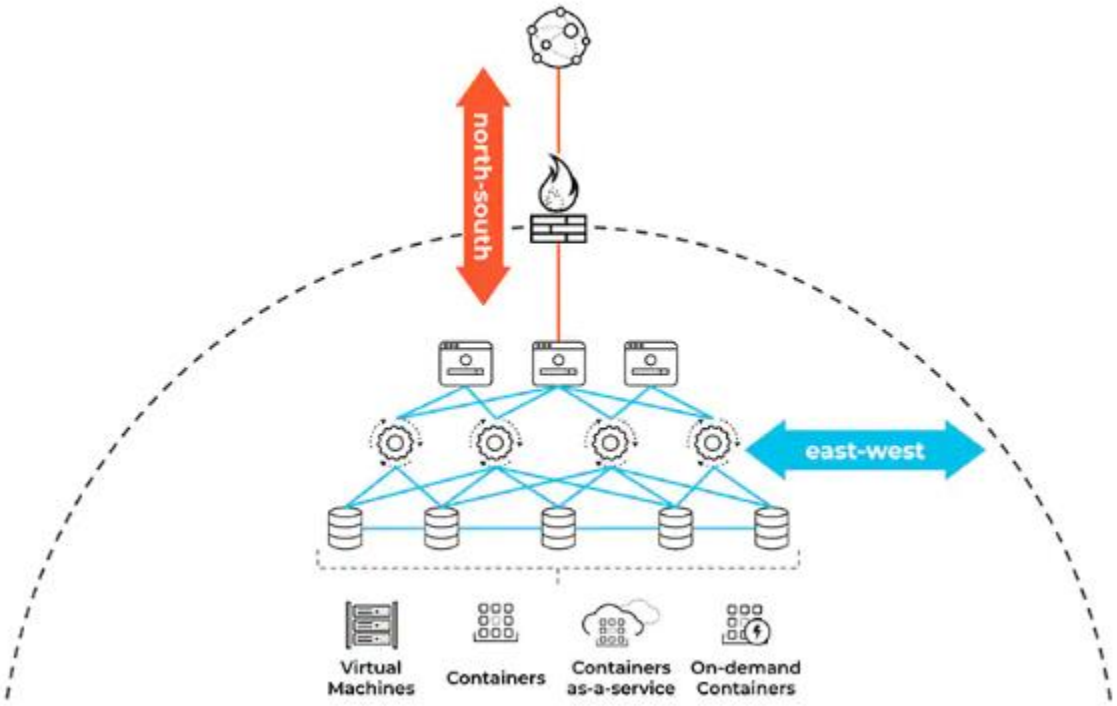
ANNEXE 1 – GRAPHIQUE MICROSEGMENTATION



13. Microsegmentation overview

Parameter	Micro Segmentation	Network Segmentation
Terminology	Micro-segmentation is used to logically divide the data centre into distinct security segments upto individual workload level.	Network segmentation creates sub-networks within the overall network to prevent attackers from moving inside the perimeter and attack the production workload.
Related terminologies	firewalls, virtual LANs (VLANs), and access control lists (ACLs)	VMs, containers, Cloud, Data Centers
SDN based control	Essential	Optional
Management and control	Centralized. This reduces overhead of managing security for individual hosts	Not mandatory to perform central management via orchestrators
Policies	Granular policies	Network/segment level policies
Policy enforcement on	Subnets and VLANs.	VMs and hosts
Network Virtualization	Required	Not required
Scope	More Granular since controls lateral movement across hosts	More on perimeter level and across Zones and subnets
Host to Host communication control	Microsegmentation can be useful tool in this case	Network Segmentation will not be able to control/detect security threat
Traffic path control	Eat-West traffic (lateral traffic movement)	North-South
Benefits	• Enforce granular tier-level segmentation within the same application group. Hence greater security • Enforce policy upto Layer 7 • Critical applications will keep safe, even in the case of a breach	• Enforce security at perimeter to protect against entry of attacks. • Simpler to implement than Micro-segmentation
Disadvantages	High Skill required including application level visibility to employ Microsegmentation.	Less proficient skill requirement for deploying network based segmentation solution

14. Tableau comparatif Segmentation et Microsegmentation



15. Microsegmentation *trafic* Nord-Sud et Est-Ouest

RÉVISIONS

Date	Action	Auteur	Ver.
2024-01-22	Ajustement du TLP	Jean-François Blais	1.1
2022-12-12	Approbation	CESI	1.0
2022-11-15	Révision linguistique	Marie-Josée	0.6
2022-10-22	Révision microsegmentation	Aboubakar	0.5
2022-09-03	Microsegmentation	Aboubakar	0.4
2022-07-16	Table des matières et Schémas	Aboubakar	0.3
2022-06-13	Avantages et fonctionnement	Aboubakar	0.2
2022-05-27	Version courante et initiale	Aboubakar	0.1