NETWORKWORLD FROM IDG
CONTENU SPONSORISÉ

eBook

COMMENT ACTIVER UN PÉRIMÈTRE RÉSEAU FLEXIBLE AVEC UN **SD-WAN SÉCURISÉ**

2 Introduction
3 Problèmes du périmètre réseau
4 Sécurité en dehors du périmètre
5 Nouvelles exigences réseau
6 SASE : Secure Access Service Edge
7 Encradré : SD-WAN Session Smart™ de Juniper Networks
8 Les nombreux avantages du SD-WAN sécurisé dans une architecture SASE
8 Conclusion

JUNIPER NETWORKS

IDG COMMUNICATIONS INC.

EN 2020, des millions d'employés ont soudainement dû adopter le télétravail. Même lorsque la pandémie reculera, nombre d'entre eux ne retourneront pas au bureau, ou de façon partielle.

Dans les faits, plus de la moitié (55 %) des employés continuent de travailler de chez eux au moins trois jours par semaine, d'après l'étude de PwC sur le télétravail réalisée en 2021. Et leurs employeurs vont certainement les soutenir. Selon cette même étude, 52 % des responsables ont indiqué que les employés ont été plus productifs lorsqu'ils travaillaient à domicile et 83 % ont déclaré que le télétravail a été une réussite. Il est donc probable qu'un modèle de travail hybride devienne la nouvelle norme.

Ce bouleversement des habitudes de travail a une incidence sur les réseaux des entreprises. Fournir des services aux employés dans l'enceinte relativement sécurisée du pare-feu de l'entreprise et connecter les utilisateurs finaux aux applications et données dont ils ont besoin depuis l'extérieur du périmètre réseau sont deux problématiques entièrement différentes.

Prendre en charge les employés à distance n'est pas le seul défi à relever. La pandémie a accéléré l'adoption par l'entreprise des applications cloud et SaaS (software-as-a-service). D'après une étude 2020 d'IDG sur le cloud computing, d'ici 2022, plus de la moitié des entreprises (55 %) travailleront entièrement dans le cloud, ou presque. En moyenne, 36 % de leurs applications passeront au modèle SaaS d'ici 2022.

TÉMOIGNAGE DE RÉUSSITE DU TÉLÉTRAVAIL

Employés qui s'attendent à continuer de travailler à domicile

Responsables qui pensent que les employés sont plus productifs lorsqu'ils travaillent de chez eux

Responsables qui estiment que le télétravail est une réussite

SOURCE : ÉTUDE DE PWC SUR LE TÉLÉTRAVAIL, 2021

ADOPTION DU CLOUD

Entreprises qui fonctionneront intégralement dans le cloud, ou presque, d'ici 2022 :

Entreprises

Ces entreprises s'attendent à ce que 36 % de leurs applications soient SaaS d'ici 2022

Applications SaaS

SOURCE : ÉTUDE D'IDG SUR LE CLOUD COMPUTING, 2020

PROBLÈMES DU PÉRIMÈTRE RÉSEAU

Cette mutation rapide du réseau de l'entreprise a de profondes implications sur le modèle de sécurité du périmètre réseau. Pour commencer, l'augmentation massive du nombre de télétravailleurs accroît la surface d'attaque. Lorsque les employés travaillent au bureau, le service informatique peut déployer la sécurité gérée sur les postes de travail, gérer les paramètres de pare-feu et s'assurer qu'il n'y a qu'un seul chemin pour accéder au réseau et le quitter.

Lorsque les employés travaillent chez eux, le service informatique peut quand même contrôler leurs postes de travail et d'autres équipements. Dans certains cas, les employés doivent se connecter via un réseau privé virtuel.

Mais le service informatique n'a aucun contrôle sur les autres équipements susceptibles d'être connectés au réseau personnel d'un employé : c'est-à-dire les téléviseurs, routeurs personnels, caméras ou thermostats. L'un de ces équipements pourrait présenter des défauts de sécurité, or ils partagent le même réseau que l'ordinateur portable de l'employé. Ainsi, même si le portable est connecté par l'intermédiaire d'un VPN, la configuration du réseau domestique fait courir des risques à l'entreprise.

En outre, les tunnels chiffrés sont complexes et peu pratiques à gérer et à faire évoluer. Ils augmentent le temps de traitement et peuvent nuire à l'expérience de l'utilisateur. Et si l'utilisation du VPN est trop préjudiciable pour permettre aux employés de travailler efficacement, ils risquent de vouloir contourner les stratégies de l'entreprise. Le VPN devient alors inutile.

SÉCURITÉ EN DEHORS DU PÉRIMÈTRE

L'autre changement de taille concerne la prolifération des charges de travail dans le cloud et les applications SaaS. Chaque cloud et chaque service possédera sa propre sécurité, qui doit être configurée et protégée. Au final, plus de la moitié des utilisateurs de l'entreprise seront situés en dehors du pare-feu, comme de nombreuses charges de travail.

La sécurité du réseau n'a pas suivi le même rythme d'évolution que ces changements, et les cybercriminels en ont profité. En avril 2020, par exemple, le FBI a indiqué qu'il recevait trois à quatre fois plus de plaintes pour cyberattaques que d'ordinaire. De plus, les méthodes des pirates informatiques sont de plus en plus sophistiquées. En 2020, 35 % des cyberattaques provenaient de malwares ou de méthodes auparavant inconnus, alors que ce chiffre était de 20 % avant la pandémie, selon un rapport de Deloitte.

Par ailleurs, la pandémie oblige les entreprises à repenser leur architecture réseau interne. Par exemple, l'utilisation grandissante de la visioconférence a un impact important sur la bande passante du réseau. Selon un rapport de Twilio, en 2020, 30 % des entreprises ont commencé à utiliser les conférences Web pour la première fois.

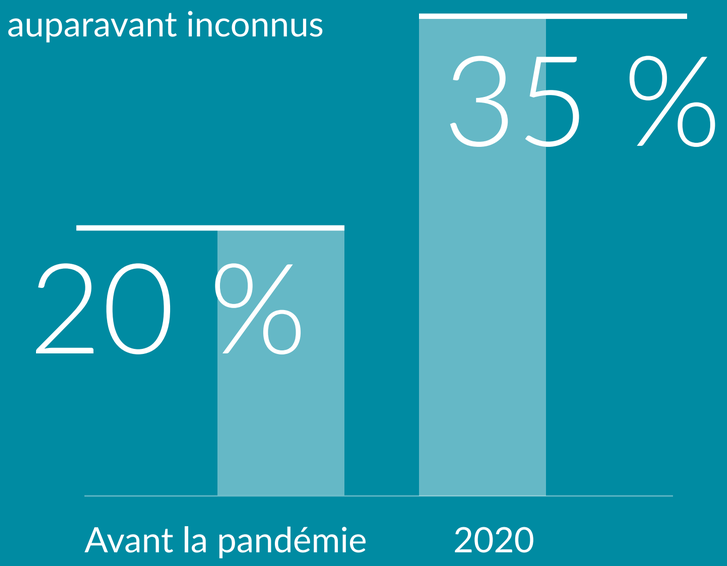
Le streaming vidéo en direct consomme beaucoup de bande passante, et les nombreux appels vidéo à distance des employés accentuent cette consommation. Sans une architecture capable de prendre en charge les flux vidéo peer-to-peer, la liaison Internet entrante va rapidement se retrouver surchargée. À la lumière de tous ces changements, il n'est pas surprenant que 70 % des responsables prévoient d'investir dans l'infrastructure informatique afin de sécuriser la connectivité virtuelle.

Les exigences d'un réseau sécurisé moderne

En résumé, le modèle traditionnel de la sécurité informatique de l'entreprise, basé sur un périmètre, ne suffit plus. Le service informatique ne peut pas déployer un pare-feu au domicile de chaque employé. Il ne peut pas non plus inspecter les connexions des employés et le trafic cloud et SaaS en le faisant transiter vers un centre de données de l'entreprise sans générer une latence énorme. Autrement dit, cet effet de « tromboning du trafic » rendrait le réseau complètement inutilisable en raison de performances médiocres et des coûts supplémentaires. La création d'une architecture réseau en étoile à partir de plusieurs VPN deviendrait bien trop difficile à gérer.

DES MENACES DE PLUS EN PLUS SOPHISTIQUÉES

Utilisation de malwares ou de méthodes de cyberattaque auparavant inconnus



SOURCE : DELOITTE

LES NOUVELLES EXIGENCES DU RÉSEAU

Même si le monde a changé, les employés, les partenaires et les clients ont encore besoin d'un accès rapide, homogène et immédiat aux applications et aux données, indépendamment de l'endroit où ils se trouvent. Pour répondre aux attentes des utilisateurs finaux, maîtriser les coûts et réduire la complexité, la nouvelle architecture réseau doit répondre à un certain nombre d'exigences critiques.

Baser les autorisations sur l'identité, et non sur l'emplacement

Avec autant d'équipements, d'utilisateurs et d'applications à l'extérieur du pare-feu, les autorisations et les accès reposant sur les adresses IP ne fonctionnent pas, en particulier parce que les adresses IP sont éphémères dans les environnements d'autoscaling comme le cloud. En conséquence, le réseau doit pouvoir exploiter un système qui authentifie l'identité de chaque utilisateur, équipement et charge de travail.

Utiliser une approche « zero trust »

Dans ce modèle, l'ensemble du trafic est considéré comme non fiable et refusé par défaut, sauf s'il est identifié, authentifié et autorisé. L'approche Zero trust suit le principe de moindre privilège. Ainsi, tous les utilisateurs, équipements et charges de travail sont régis par des stratégies qui accordent aux utilisateurs l'accès aux seules ressources dont ils ont besoin pour leur travail. Ni plus, ni moins.

L'approche Zero trust doit être présente dans tous les aspects du travail. Le service informatique de l'entreprise ne peut pas continuer avec un état d'esprit « n'importe où vers n'importe où ». Il ne faire confiance à aucune connexion et intégrer la sécurité au chemin réseau. Le Zero trust est une structure de sécurité puissante. Dans les faits, avec 40 % des responsables informatiques et de la sécurité en quête d'une architecture Zero trust pour leur environnement l'an dernier, il s'agissait de la solution technologique la plus recherchée selon l'**étude 2020 d'IDG sur les priorités de la sécurité**.

Un réseau orienté sessions

Selon la définition de base, une session est une connexion temporaire formée par deux ressources réseau afin qu'elles puissent communiquer. Les sessions sont bidirectionnelles, autrement dit, il existe deux flux d'informations liés. Elles ont une direction, associée à la ressource qui a initié la session. Et pour finir, elles présentent des états.

Ces caractéristiques rendent chaque session unique, c'est pourquoi le réseau peut associer des paquets et des flux à une session. Au lieu de simplement envoyer des paquets, un réseau orienté sessions prend, en fonction des sessions, des décisions de routage dynamiques qui s'alignent sur des stratégies et s'étendent au-delà du réseau de manière sécurisée. Cette approche du réseau sécurisé est beaucoup plus simple et plus agile.

Un avantage majeur des réseaux orientés sessions est qu'ils peuvent être étendus de manière élastique. Comme mentionné plus haut, de nombreuses entreprises prévoient de déplacer leurs charges de travail vers le cloud, c'est pourquoi elles doivent être en mesure d'appliquer leurs stratégies lorsqu'elles se connectent à des ressources sur des réseaux que le service informatique ne contrôle pas. Concrètement, cela signifie que le service informatique doit étendre le périmètre de façon flexible pour englober ces ressources. Cette flexibilité permet au service informatique de sécuriser les sessions même lorsqu'elles transitent sur des réseaux qui changent constamment.

Créer une architecture réseau basée sur la périphérie

Le traitement ne peut plus être réservé à un noyau central. Les utilisateurs, les équipements et les charges de travail sont désormais largement dispersés, et parfois des milliers de kilomètres les séparent du centre de données. À de telles distances, même la vitesse de la lumière n'est pas assez rapide pour éliminer la latence, et les performances s'en ressentent. Par conséquent, le traitement doit avoir lieu en périphérie, près de l'utilisateur final. Puisque les fournisseurs de cloud à grande échelle ont créé le cloud en périphérie, cette étape devient de plus en plus facile.

SASE : SECURE ACCESS SERVICE EDGE

Découvrez le Secure Access Service Edge, une architecture réseau plus connue sous l'appellation SASE (qui se prononce « sassi »). Le SASE réunit la gestion de la sécurité unifiée, le SD-WAN, un pare-feu en tant que service, un broker de sécurité pour l'accès au cloud, une passerelle Web sécurisée et une architecture réseau Zero trust (ZTNA) pour créer un modèle de service unique, fourni sur le cloud qui rapproche la sécurité de la périphérie.

Le SASE intègre un certain nombre de fonctions, mais il a tout de même besoin d'une solution SD-WAN sécurisée et basée sur des sessions, une solution qui regroupe plusieurs fonctions intermédiaires, comme la DPI, le pare-feu et l'équilibrage de charge, réduisant ainsi la complexité et les coûts.

Le résultat est une plate-forme beaucoup plus simple et plus agile, capable de s'adapter en fonction des fluctuations de l'activité de l'entreprise. Après tout, il est beaucoup plus facile de mettre à l'échelle un logiciel qu'une myriade de boîtiers middleware qui ont été ajoutés au routage pour reconnaître les sessions. Et alors que l'architecture Zero trust est extrêmement complexe et fastidieuse à déployer sur les réseaux traditionnels périmétriques, il est possible de la mettre en œuvre en intégrant la sécurité au chemin réseau avec la solution SD-WAN adaptée.

Il est beaucoup plus facile de mettre à l'échelle un logiciel qu'une myriade de boîtiers middleware qui ont été ajoutés au routage pour reconnaître les sessions.

Cette conception du SD-WAN fournit une protection contre les attaques, indépendamment de l'emplacement des ressources numériques. Le réseau comprend les services de réseau et les achemine à l'équipement de sécurité approprié, qu'il soit situé dans une filiale de l'entreprise ou dans le cloud.

Mais cela ne signifie pas que les périmètres et les pare-feu traditionnels sont devenus inutiles. Les pare-feu de petite taille servent toujours à protéger un site de l'entreprise, par exemple, et tous les fournisseurs de réseau dignes de ce nom doivent être en mesure de prendre en charge un modèle hybride. Mais s'ils sont utilisés seuls, ils ne peuvent pas offrir la protection, l'agilité et la flexibilité nécessaires à un réseau dispersé géographiquement et en constante évolution. Cette problématique exige une solution SD-WAN doublée d'un SASE.

ENCADRÉ

SD-WAN SESSION SMART™ DE JUNIPER NETWORKS

Si le SASE donnait lieu à une solution SD-WAN sur-mesure, ce serait SD-WAN Session Smart™ de Juniper Networks (auparavant 128 Technology).

Reposant sur le Secure Vector Routing au lieu d'une architecture de tunnels, les routeurs Session Smart™ initient chaque session avec des métadonnées pour savoir si elle provient d'une source de confiance. Elle peut ensuite être étendue à un nombre illimité de routeurs, à tout moment. Cette approche systématique de refus par défaut peut facilement segmenter le trafic par groupes et utilisateurs afin d'activer la stratégie Zero trust. Il n'est donc pas nécessaire d'utiliser un tunnel chiffré point à point. De ce fait, le réseau est hautement évolutif, hautement sécurisé, et son encombrement est réduit de plus de 60 %. Voilà qui est particulièrement important lorsque le service informatique gère des connexions par satellite coûteuses ou des réseaux domestiques de petite taille. Session Smart™ offre au service informatique une visibilité sans limite sur le trafic réseau, ce qui permet de gérer un réseau global du client au cloud à l'aide d'une source unique.

Le chiffrement adaptatif est l'une des fonctions du SD-WAN Session Smart™ qui lui permet de se démarquer. Environ 80 % du trafic Internet est déjà chiffré, il n'est donc pas nécessaire de le chiffrer une deuxième fois, la raison principale étant que cela ajoute une charge de traitement supplémentaire inutile qui augmente la latence et réduit les performances. Et pourtant, c'est précisément ce que font les VPN et de nombreux autres systèmes de sécurité réseau traditionnels. Grâce à la console de gestion de Session Smart™, appelée « Session Smart™ Conductor », le service informatique peut facilement définir des stratégies afin que le trafic chiffré provenant de sources telles que Zoom ou Microsoft 365 ne soit pas chiffré une nouvelle fois. La console identifie les données de ces sources et d'autres applications SaaS pour les router en toute sécurité sur Internet lorsque c'est possible, afin de garantir une expérience utilisateur optimale.

Le SD-WAN Session Smart™ étant maintenant une offre de Juniper Networks, les clients peuvent tirer parti du machine learning et du moteur AIOps pour réparer automatiquement le réseau, et utiliser l'assistant de réseau virtuel Mist Marvis pour identifier rapidement et facilement les interruptions réseau, afin de minimiser les temps d'arrêt et les erreurs manuelles fatales. Session Smart™ gère la majeure partie des tâches de routine du réseau de sorte que le personnel informatique peut se concentrer sur les projets à valeur ajoutée.

« Une fois que l'hyper-segmentation des utilisateurs, des stratégies, etc., est mise en place, vous pouvez tirer parti du modèle d'IA créé par Juniper » explique Sue Graham Johnston, vice-présidente et directrice générale de Juniper. « Vous alimentez le cloud avec vos données, l'opérateur définit des stratégies, et le réseau fonctionne de façon autonome. »

Tous ces avantages ont amené des entreprises telles que Momentum Telecom, un fournisseur de services VoIP et de communications unifiées, à déployer Session Smart™.

« Nous avons évalué la rapidité, la simplicité, l'orchestration du réseau, tout ce qui tourne autour du produit, et nous l'avons intégré à tous nos centres de données et bureaux. » MARK MARQUEZ, Vice-président exécutif de la technologie, Momentum

« Nous étions à la recherche d'une solution SD-WAN vraiment adaptée aux besoins de nos clients et capable d'améliorer le fonctionnement de leur entreprise » explique Mark Marquez, vice-président en charge des technologies pour Momentum. « Les applications qu'ils utilisaient nous poussaient à utiliser le cloud. Nous avons étudié la sécurité offerte par Session Smart™ ainsi que le chiffrement adaptatif qu'il propose. Nous avons évalué la rapidité, la simplicité, l'orchestration du réseau, tout ce qui tourne autour du produit, et nous l'avons intégré à tous nos centres de données et bureaux. » Pour en savoir plus, visitez **juniper.net**.

JUNIPER NETWORKS

LES NOMBREUX AVANTAGES DU SD-WAN SÉCURISÉ DANS UNE ARCHITECTURE SASE

La combinaison puissante d'une solution SD-WAN sécurisée et d'une architecture SASE peut être bénéfique à l'entreprise à plus d'un titre.

Expérience utilisateur optimale

Après le taux de disponibilité, c'est désormais l'expérience utilisateur qu'il faut surveiller. Si l'expérience utilisateur est mauvaise, la sécurité est reléguée au second plan. Le service informatique a besoin d'une solution réseau qui surveille l'expérience utilisateur, qui puisse s'auto-diagnostiquer et s'auto-réparer dès que nécessaire et appliquer des stratégies globales de sécurité et de performances, quel que soit l'emplacement de l'utilisateur.

Gestion plus simple du WAN

Toutes les solutions SD-WAN ne se valent pas. Le service informatique doit tester et piloter plusieurs solutions. La solution est-elle vraiment innovante et capable de moderniser le réseau ? Ou s'agit-il seulement de quelques améliorations superficielles ? Il est essentiel de comprendre les différences pour garantir un retour sur investissement efficace.

Réduction des coûts

Une solution SD-WAN adaptée permet au service informatique de réduire ses coûts de plusieurs manières. Il est possible de réduire les coûts de connectivité (en utilisant le haut débit sur MPLS, par exemple), d'adopter du matériel whitebox générique et d'y installer une solution logicielle, ou encore de regrouper plusieurs fonctions intermédiaires dans une même solution.

CONCLUSION

Le nouveau monde du travail, le SaaS et le cloud exigent un nouveau modèle de sécurité plus flexible, plus souple et plus agile que jamais auparavant. Une solution SD-WAN sécurisée doit imposer un accès ZTNA aux utilisateurs, aux équipements et aux charges de travail distants, optimiser les performances, minimiser la latence et répondre aux exigences d'une architecture SASE.

Pour en savoir plus, visitez le site **www.juniper.net/fr/fr/products/routers/session-smart-router.html.**

JUNIPER NETWORKS