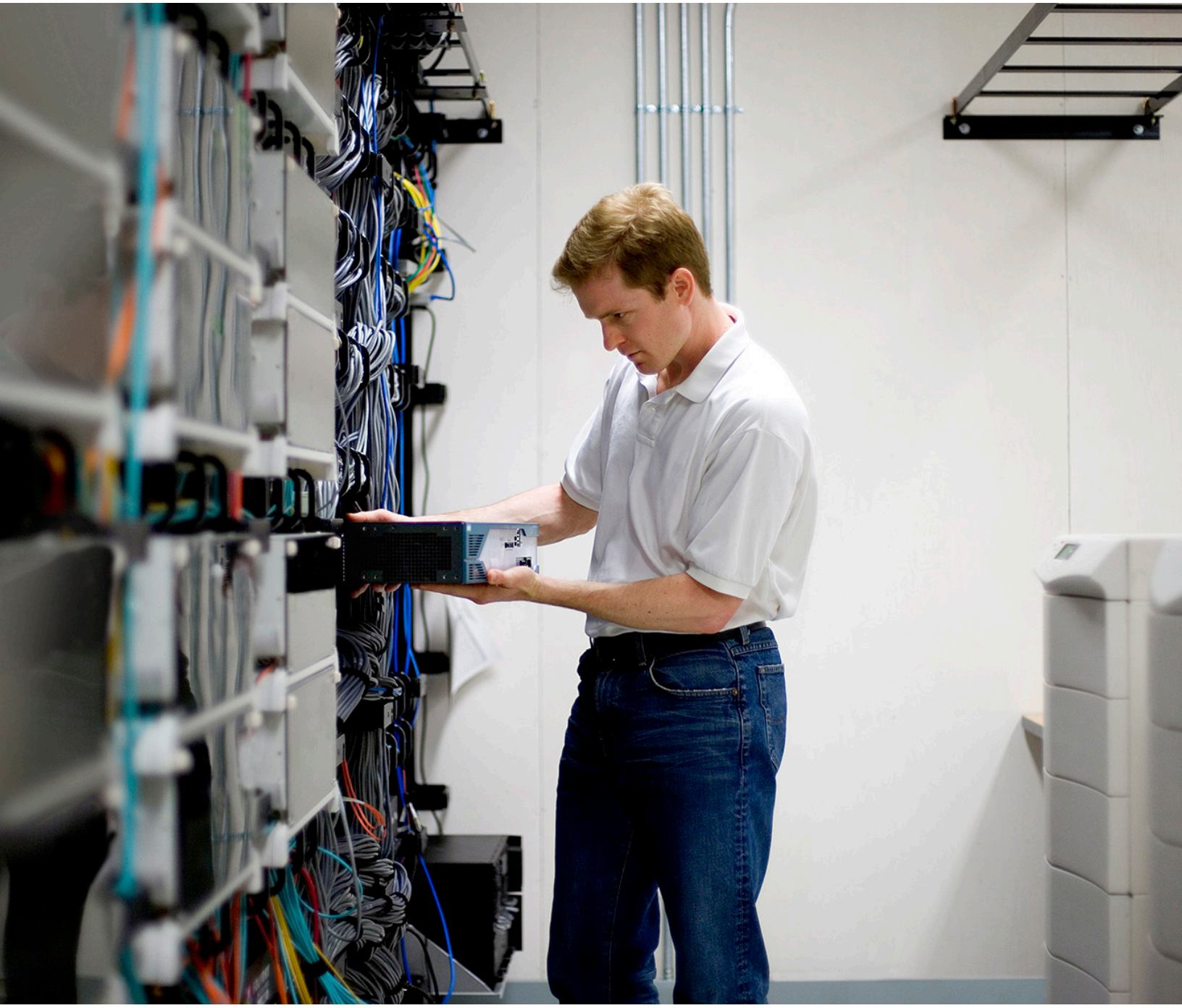
La gestion intelligente des points d'entrée au réseau d'entreprise



Résumé

Dans notre nouvel environnement numérique, la périphérie du réseau a pris une importance sans précédent. Elle est souvent négligée, alors que c'est justement en périphérie que se jouent l'échec ou la réussite de toutes les initiatives numériques. Les enjeux liés à cette partie du réseau sont nombreux :

- La périphérie est votre première ligne de défense contre toute infiltration d'éléments non fiables ou malveillants dans vos appareils.
- C'est le canal par lequel vous délivrez vos applications ou services les plus utilisés, et ceux dans lesquels vous avez le plus investi.
- Elle constitue le lien stratégique entre les différentes entités d'organisations hautement décentralisées.
- Elle relie également votre entreprise à vos clients.
- C'est là que les appareils de l'Internet des objets (IoT) sont connectés et gérés.
- Et c'est la partie à analyser en priorité pour évaluer l'état de votre activité.

Certains déploient en périphérie du réseau comme si toutes les solutions réseau se valaient. Nous ne sommes pas de cet avis, et pensons que la nouvelle ère numérique demande le déploiement d'une intelligence importante en périphérie.

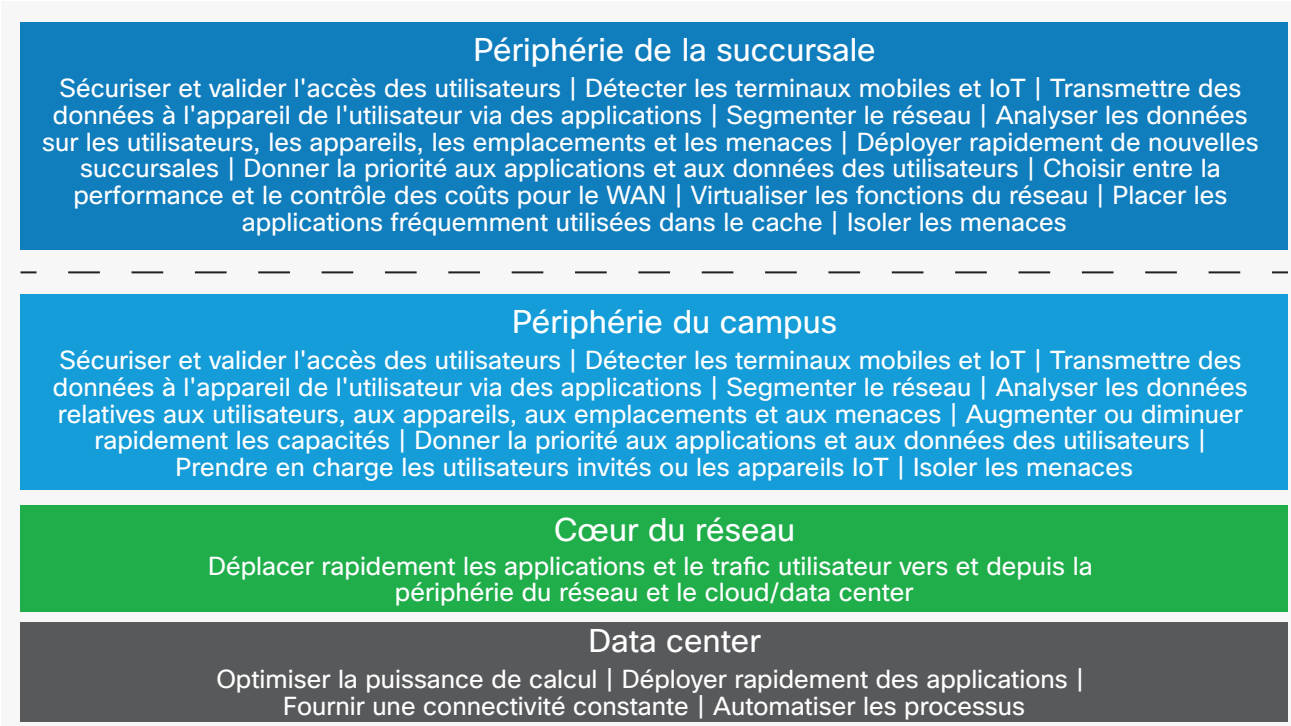
Nous proposons des solutions et des fonctionnalités stratégiques pour stimuler l'activité commerciale. Cisco réinvente la gestion des points d'entrée au réseau numérique en misant sur :

- La défense des ressources essentielles à la périphérie. Les entreprises peuvent contrer 99,2 % des attaques en donnant à leur réseau un rôle de détecteur et d'exécuteur. Ceci peut être accompli tout en fournissant des informations plus complètes pour améliorer la protection et permettre des réponses plus rapides.
- La vision en temps réel des applications et des appareils, avec une capacité d'itinérance huit fois plus rapide et une visibilité sur plus de 1 200 applications. Cette initiative est possible grâce à nos partenariats stratégiques avec Apple et plusieurs innovations Wi-Fi.
- Une adaptation rapide du réseau à mesure que votre entreprise évolue vers une approche logicielle des réseaux LAN sans fil, LAN et WAN. Ceci entraîne une réduction des coûts de déploiement de 79 % grâce à la séparation des logiciels et du matériel, et à la virtualisation de la périphérie WAN.
- Une plate-forme conçue pour répondre aux exigences futures en créant une base normalisée et programmable prête à recevoir de nouvelles fonctionnalités quand celles-ci sont requises.
- La mise à disposition d'informations plus détaillées, plus rapidement, en provenance des points de vente ou des lieux de contact avec la clientèle, avec jusqu'à un mètre de précision supplémentaire dans les données de localisation pour vous permettre de prendre les meilleures décisions.

Le réseau est un moteur de changement essentiel dans quasiment toutes les entreprises s'apprêtant à effectuer leur transformation numérique. Cette transformation les aidera à accroître leur agilité et leur productivité, à améliorer leur contact avec leurs clients et à protéger leurs principales ressources et données relevant de la propriété intellectuelle.

La périphérie du réseau joue un rôle clé dans ce processus et présente des enjeux plus nombreux et plus variés que l'infrastructure de réseau centrale ou les data centers. Comme l'illustre la figure 1, il suffit de comparer les couches du réseau pour constater que sa périphérie doit remplir le plus grand nombre de fonctions au sein du campus. C'est également le cas pour les sites distants.

Figure 1. Couches du réseau et leurs fonctions



Le rôle de la périphérie du réseau

La transformation numérique confère un rôle plus important que jamais à la périphérie du réseau, qui connaît une activité particulièrement intense :

- **Elle constitue votre première ligne de défense.** C'est en périphérie que les politiques sont appliquées et validées, sans limiter votre capacité d'accès aux ressources dont vous avez besoin. Si l'accès est mal géré, votre entreprise peut faire l'objet d'infiltrations ou d'une multiplication de programmes malveillants. Ce risque s'accroît sans cesse dans un environnement de plus en plus riche en menaces. Les appareils, les micrologiciels et même les systèmes d'exploitation sont des points d'intrusion potentiels.
- **C'est le canal par lequel vous délivrez vos applications les plus utilisées.** La périphérie du réseau est la zone où les priorités sont établies. Une expérience négative en périphérie ralentira l'adoption des applications et entraînera une baisse du ROI.
- **La périphérie constitue le lien stratégique entre les différentes entités d'organisations hautement décentralisées.** Il est essentiel de proposer une expérience transparente à vos collaborateurs, partenaires et clients, quel que soit le lieu où ils se trouvent. Un réseau de second ordre offrira des expériences irrégulières aux utilisateurs clés.
- **La périphérie relie les entreprises à leurs clients.** Si vous évoluez dans le secteur du commerce ou de l'hôtellerie, un accès insatisfaisant nuira à votre capacité de cultiver une relation individuelle avec vos clients et aura un impact négatif sur votre marque.
- **La périphérie est conçue pour faire face aux exigences croissantes de l'Internet des objets.** La périphérie du réseau a un impact sur l'environnement physique en provoquant l'entrée de presque tous les secteurs dans l'ère numérique en améliorant les opérations et en réduisant les coûts. Privées des fonctionnalités nécessaires en périphérie, les entreprises peuvent accumuler du retard en termes de réduction des coûts et d'efficacité opérationnelle.
- **C'est la région à analyser en priorité pour évaluer l'état de l'entreprise.** Dans un réseau distribué, la périphérie est la seule région offrant une visibilité sur l'ensemble du trafic de données, puisqu'il est possible d'y collecter des données pour les analyser. Grâce aux données concernant les utilisateurs, les applications, les appareils, et les menaces, les entreprises peuvent obtenir des informations qui les aideront réellement à prendre de meilleures décisions pour accompagner leurs collaborateurs, réduire les risques et les coûts, et fournir des informations à leur public cible. Si leur précision est insuffisante ou irrégulière, ces données seront faussées et non fiables.

La standardisation des périphéries représente-t-elle une évolution positive ?

De nombreuses solutions pour les périphéries de réseau participent à cette standardisation en recourant à des composants largement disponibles pour créer des appareils de réseau en appliquant des conceptions calquées sur les normes du secteur. On procède généralement ainsi pour réduire les coûts d'ingénierie et de production de l'équipement en exploitant des conceptions existantes fournies par les fabricants des composants. Ceci contribue à accroître la standardisation des périphéries. Le principe consistant à faire passer les coûts et la gestion avant la volonté de livrer des innovations majeures pour la croissance et la sécurité expose votre entreprise à des risques plus importants.

Quels sont les risques ?

Les composants et leur conception ne sont pas exclusivement réservés aux fabricants d'appareils. Ils peuvent parfois tomber entre les mains d'individus recherchant des moyens d'infiltrer les réseaux. Chaque appareil connecté au réseau constitue un point d'infiltration potentiel. Aujourd'hui, les entreprises utilisent un nombre toujours plus grand d'appareils mobiles ou IoT (Internet des objets) sur leurs réseaux pour développer leur activité. Elles doivent rechercher des solutions permettant de sécuriser les accès, de la périphérie aux data centers, en contrôlant le trafic entre chaque relais.

Il existe également le risque de devoir revoir l'ingénierie du réseau lorsque l'entreprise se trouve face à un nouvel impératif commercial. Les solutions toutes prêtes sont conçues pour répondre à un nombre important d'utilisations, mais elles ne sont ni flexibles ni faciles à personnaliser. Elles sont également peu adaptées en cas d'évolutions imprévues de votre réseau. Les plates-formes de réseau doivent être capables de s'adapter aux évolutions rapides du paysage numérique actuel.

La majorité des solutions prêtes à l'emploi sont calquées sur les normes du secteur, ce qui est important si l'on veut répondre à des exigences basiques et à offrir les fonctionnalités les plus courantes, mais ces normes peuvent changer. Le processus d'élaboration des normes est souvent long, tandis que les exigences des fabricants, des développeurs d'applications et des utilisateurs ne cessent de changer. Les partisans d'une approche standardisée peuvent être mis en difficulté face à des utilisateurs plus exigeants. Il arrive qu'une solution commence par suivre la norme tout en étant capable de s'enrichir de nouvelles fonctionnalités si nécessaire. Ce type de solution répond aux exigences du monde numérique sans être entravée par les normes, dont la modification et l'officialisation peuvent prendre des années.

L'intégrité des appareils risque également d'être compromise. Des organisations malveillantes peuvent intercepter les appareils expédiés à travers le monde pour en modifier certaines composantes, par exemple en remplaçant les processeurs ou en installant des mouchards pour obtenir des données sensibles.

Quel est le véritable coût de l'uniformisation ?

La standardisation de solutions de périphérie est souvent liée à une volonté de réduire les coûts d'ingénierie et de production. Elle permet aussi à certaines solutions d'être vendues à bas prix. Cependant, on ne saurait évaluer le coût en fonction des dépenses d'exploitation et d'investissement sans tenir compte du coût associé au risque. Chaque entreprise est différente : il ne serait pas réaliste de fixer des coûts réels représentant chacune d'entre elles. Il faut tenir compte des éléments suivants :

- Le coût d'une faille de sécurité Beaucoup d'entreprises vivent de leur propriété intellectuelle et des ressources que représentent leurs données. Quelles seront les conséquences si celles-ci se retrouvent entre les mains de hackers ? Les organisations malveillantes savent très bien monétiser la propriété intellectuelle en pratiquant le rançonnement, l'extorsion ou la revente au plus offrant. Selon certaines études, des dossiers médicaux ont fait l'objet de rançons d'un montant de $40 par dossier. Détenteurs de milliers de dossiers, les hôpitaux peuvent ainsi devoir payer des sommes conséquentes pour récupérer ce qui leur appartient.
- Le coût d'une application essentielle non adoptée par les collaborateurs. De nombreuses entreprises consacrent une large part de leur budget à de nouvelles applications et de nouveaux systèmes afin d'améliorer leur productivité. Si les collaborateurs sont déçus de ces applications ou services, ils les abandonneront et le retour sur investissement chutera.
- Le coût lié aux occasions manquées. Si vous travaillez dans les secteurs du commerce ou de l'hôtellerie, vous devez interagir avec vos clients via leurs appareils mobiles. Mais chaque fois que l'un de vos clients rencontre des difficultés pour se connecter, votre entreprise perd une occasion d'interagir avec ce client et d'influencer son comportement.

- Le coût du manque de visibilité. La périphérie de réseau recèle une quantité d'informations importantes sur les utilisateurs, leurs appareils, les applications qu'ils utilisent, les lieux où ils se rendent, sans oublier les informations sur les sites susceptibles de contenir des menaces. Sans cette visibilité, votre entreprise peut passer des heures à tenter de comprendre comment ses utilisateurs interagissent avec leur environnement, comment ils accèdent à l'information et la consomment, voire manquer de détecter une menace potentielle qui aurait pu être éliminée très rapidement.

L'intelligence en périphérie avec Cisco

Cisco présente une approche opposée à la standardisation des périphéries. Nous investissons énormément dans le développement d'innovations visant à aider les entreprises à s'engager dans l'ère du numérique. Nous concentrons tous nos efforts sur la défense des ressources les plus importantes, la prise en charge d'une sensibilité plus élevée aux appareils et aux applications, et la livraison d'informations plus riches et plus rapides. Cisco aide votre entreprise à s'adapter à mesure qu'elle évolue et se prépare à relever les défis à venir. Pour y parvenir, nous concevons de nouvelles fonctionnalités uniques dès le départ ou nous améliorons celles de composants éprouvés. Cisco vous donne les moyens de répondre aux exigences actuelles et futures de la périphérie du réseau.

La défense des ressources essentielles en périphérie

La périphérie du réseau est le premier point d'entrée des éléments non autorisés ou hostiles, car c'est là que sont ajoutés les nouveaux utilisateurs et appareils. Elle doit être fiable pour permettre l'identification et le contrôle des éléments intégrés aux réseaux.

Accepter la standardisation de la sécurité en périphérie revient à déclarer que les solutions de sécurité prêtes à l'emploi sont efficaces. Si c'était le cas, comment expliquer le fait que le vol d'informations, l'extorsion et les rançons dégagent des revenus approchant mille milliards de dollars ?

Les approches actuelles de sécurité en périphérie sont inefficaces. En tant que leader du marché, Cisco dispose des technologies innovantes nécessaires pour identifier les programmes et leurs auteurs, et évaluer leur intégrité avant de les autoriser à entrer et à circuler dans vos réseaux.

Voici quelques-unes des innovations pour la sécurité en périphérie de réseau de Cisco® dont bénéficient nos clients :

- **L'identité et l'intégrité des appareils et des utilisateurs**. Nos appareils pour la périphérie disposent des technologies les plus complètes pour analyser les profils des terminaux. En outre, Cisco AnyConnect® effectue une vérification d'intégrité tenant compte de l'approche et des politiques en vigueur avant d'autoriser l'accès au réseau. Cette précision dans la vérification d'identité permet de prévenir tout accès au réseau par des appareils non autorisés ou corrompus (infectés par des malwares) jusqu'à ce que ces derniers démontrent qu'ils sont autorisés et non compromis.
- **Des autorisations d'accès selon l'indice de dangerosité**. L'intégration de Cisco ISE (Identity Services Engine) permet une modification automatique des autorisations d'accès des utilisateurs et des appareils en cas de changement de leur indice de dangerosité STIX ou de leur indice de vulnérabilité CVSS. Les indices STIX et CVSS sont utilisés par l'ensemble du secteur pour évaluer les niveaux de menace et les vulnérabilités.
- **L'intégration d'une segmentation logicielle**. Il est souvent d'autant plus difficile de créer et de gérer les segmentations avec des LAN virtuels et des listes de contrôle d'accès (ACL) que ces segmentations deviennent plus importantes pour sécuriser les opérations de l'Internet des objets. Nos appareils pour la périphérie bénéficient d'une segmentation logicielle TrustSec® intégrée à leur système d'exploitation et d'un ASIC (circuit intégré spécialisé) pour garantir une identification et une segmentation faciles et performantes depuis le point d'accès aux applications du data center.
- **Le réseau comme exécuteur**. Cette segmentation logicielle et intégrée aux équipements de périphérie garantit l'application instantanée et fiable des politiques de sécurité visant à contrôler l'accès et à isoler les menaces. Grâce à l'intégration de Cisco ISO, Cisco StealthWatch et des technologies Cisco Security Technology Associate, les solutions peuvent utiliser les politiques pour isoler les menaces depuis une interface unique ou un même produit.
- **Le réseau comme détecteur**. Bénéficiez d'une visibilité totale avec NetFlow et de l'interprétation de ces données par Cisco Stealthwatch. Étant donné que tous les appareils Cisco pour la périphérie comprennent Flexible NetFlow, vous disposez d'une visibilité totale sur les flux pour détecter les comportements anormaux. Les solutions standardisées ne vous permettent pas de visualiser les comportements des utilisateurs au sein de votre réseau ou sur Internet.

- **L'intégration de Stealthwatch Learning Network**. Cette innovation permet à tous les appareils des succursales de transmettre des données sur les comportements et de développer une reconnaissance intelligente des comportements autorisés, ce qui les rend à la fois plus rapides, plus simples et plus évolutifs.
- **La mise en application instantanée des politiques indexées sur des niveaux d'alerte**. Vous pouvez définir des politiques par avance pour répondre à des événements d'une gravité exceptionnelle, tels qu'un malware zero-day ou une attaque à propagation rapide. Un simple clic vous permettra d'appliquer des modifications de politiques d'accès à tous les appareils présents sur le réseau afin de restreindre ou d'interrompre toute communication jusqu'à ce que la menace soit éliminée.
- **La segmentation automatique et l'identification des terminaux relevant de l'Internet des objets (IoT)**. Les capteurs dont disposent les appareils de périphérie Cisco permettent de reconnaître le plus grand nombre d'appareils médicaux de l'Internet des objets à ce jour, et cette technologie est en passe de gagner de nombreux secteurs supplémentaires. Grâce à l'intégration des technologies de pointe comme la solution ISE (Identity Services Engine), les appareils de la périphérie de réseau seront à même de mieux identifier et de segmenter automatiquement les terminaux les plus rares et de les ajouter automatiquement à des segments de réseau isolés pour les protéger contre les attaques. Ainsi, chaque fois qu'un collaborateur ajoute un appareil au réseau, cet appareil est détecté, classé et placé dans le segment de réseau correspondant à sa catégorie de sécurité.
- **L'isolation rapide des menaces**. Les appareils de périphérie Cisco fonctionnent avec ISE et TrustSec. Ainsi, lorsqu'une attaque est détectée par Cisco ou un partenaire technologique, le terminal concerné peut être placé dans un segment de réseau par les services informatiques ou de façon automatique. Les menaces sont détectées plus rapidement et leur isolation est instantanée.
- **La détection de malwares dans un trafic chiffré**. Face à des hackers qui inventent sans cesse de nouvelles méthodes pour accéder aux réseaux sans être détectés, nous exploitons notre capacité à analyser des trames du réseau pour identifier les programmes malveillants, et ce même si le trafic est chiffré.
- **La protection contre les malwares, les ransomwares et les autres attaques visant le cloud**. L'intégration avec les solutions Cisco Umbrella en succursale permet aux appareils de périphérie Cisco de jouer un rôle essentiel face aux ransomwares. Umbrella interdit aux collaborateurs l'accès aux sites suspects, compromis ou infectés de malwares. Il empêche également les bots de malwares et de ransomwares d'atteindre leurs parents, bloquant ainsi leur activation.
- **La protection des collaborateurs mobiles**. Les collaborateurs mobiles constituent sans doute l'un des principaux points d'infiltration de logiciels malveillants, car ils disposent généralement d'un accès libre à Internet lors de leurs déplacements. L'agent de sécurité Cisco AnyConnect avec VPN peut être complété par Cisco Advanced Malware Protection et les solutions Cisco Umbrella pour protéger les collaborateurs mobiles hors du réseau. Il permet également de se connecter, via un VPN, à de nombreux appareils de périphérie de réseau Cisco. Aucun de ces agents individuels de sécurité pour les appareils mobiles ne fonctionnera dans un environnement standardisé.
- **L'intégrité des appareils de réseau**. L'exploitation de vulnérabilités dans les applications et dans les systèmes d'exploitation ne constitue pas le seul moyen dont les hackers disposent pour pénétrer dans des réseaux et compromettre leur intégrité. Ils attaquent la pile logicielle et matérielle d'appareils de réseau, qu'il est donc indispensable de sécuriser pour une protection efficace. Comme cela se produit pour les systèmes d'exploitation et les applications, de nouvelles vulnérabilités seront certainement découvertes pour les appareils réseau. Nous appliquons des règles très strictes pour le développement de logiciels et de matériel, incluant même des tests de régression pour garantir à nos clients une totale fiabilité de leur réseau.

Des données plus complètes et des informations plus rapides

Les solutions de périphérie Cisco vous fournissent une grande quantité d'informations sur l'activité effective de votre entreprise, c'est-à-dire sur vos utilisateurs, les appareils dont ils se servent et les applications auxquelles ils ont accès. Elles sont capables d'apprendre en analysant l'activité des appareils du réseau et ainsi s'adapter automatiquement aux changements et à l'évolution des besoins. Les données de localisation qu'elles fournissent permettent de mieux comprendre la façon dont les utilisateurs interagissent avec l'environnement et d'optimiser la prise de décision. Les solutions de périphérie Cisco peuvent également effectuer une analyse approfondie de la circulation d'une menace pour vous aider à anticiper la façon dont votre entreprise peut être infiltrée.

Avec les fonctions de fog computing de Cisco IOX, les solutions en périphérie peuvent déterminer l'emplacement optimal pour le traitement de ces données, que ce soit localement ou dans le cloud, ce qui permet à l'entreprise d'améliorer ses

performances et de réduire ses coûts. Le traitement analytique des données de localisation de la solution de mobilité connectée Cisco CMX offre des analyses détaillées basées sur le Wi-Fi et un module BLE (Bluetooth Low Energy) pour obtenir une vue concrète de la façon dont les individus interagissent avec l'environnement.

Les entreprises B2C des secteurs du commerce, de l'hôtellerie et de la formation ont pu obtenir une géolocalisation au mètre près en s'appuyant sur les données Wi-Fi et BLE, ce qui leur a permis de faire croître leurs revenus directs. Par exemple, l'hôtel Hyatt Regency a connu une croissance de 20 % de ses revenus hors chambres avec un triplement de la durée de séjour ; le centre commercial Stary Browar a vu une amélioration de l'expérience de ses clients de 80 %, tout ceci grâce à des offres mobiles personnalisées.

En outre, Cisco Prime™ offre une visibilité globale sur vos utilisateurs, leurs appareils et les applications utilisées sur le réseau. Cette visibilité facilite la planification de l'infrastructure de réseau, augmente la précision des données sur l'adoption des applications et permet de réduire les coûts.

L'automatisation pour suivre l'évolution de votre entreprise

Avec la multiplication du nombre d'utilisateurs, d'appareils et de lieux à gérer, il devient indispensable d'automatiser les processus et les nouveaux services en offrant des fonctionnalités dès l'installation et la mise en service. Qu'il s'agisse d'un environnement filaire ou sans fil, un fabric comprenant un campus et un data center dotés d'une solution logicielle indépendante exécutée en superposition sur des circuits intégrés propres à une application (ASIC) offre les avantages suivants :

- Élargissement des capacités
- Garantie de service
- Sécurité
- Autres services pour les appareils, applications et utilisateurs physiques ou virtuels

La virtualisation du réseau permet la mise en place rapide d'une gestion du réseau et des politiques par type d'utilisateur. Elle facilite également la personnalisation des applications et l'isolation rapide des menaces. Elle représente une approche centralisée pour le déploiement sécurisé de nouveaux sites distants en quelques minutes plutôt qu'en plusieurs jours, quel que soit le type de connexion.

Le module Cisco Application Policy Infrastructure Controller Enterprise (APIC-EM) offre des fonctionnalités prêtes à l'emploi contrôlées de façon centralisée et une qualité de service conçues pour un déploiement automatisé à la périphérie. Il permet également la hiérarchisation dynamique de vos applications essentielles.

La solution logicielle de Cisco offre l'agilité nécessaire pour s'adapter aux besoins de chaque entreprise. Une association étroite des plates-formes logicielle et matérielle nous permet d'offrir des avantages significatifs à votre entreprise, en particulier en périphérie WAN et en périphérie d'accès. Les composants adaptés au WAN comprennent des circuits intégrés ASIC rapides, et le logiciel de gestion de cloud fait de la solution Cisco de virtualisation des fonctions de réseau pour les entreprises (Enterprise NFV), une réalité en vertu de laquelle il vous est possible d'activer des services en quelques minutes, plutôt qu'en plusieurs mois. La virtualisation des fonctions de réseau fournit les fonctionnalités de traitement, de stockage et de gestion, ainsi que l'infrastructure de réseau et les garanties nécessaires pour mettre en œuvre des services réseau en réduisant la complexité au niveau des succursales et en proposant de nouveaux services à la demande en périphérie.

Grâce à la fonctionnalité prête à l'emploi du module APIC-EM, certaines entreprises ont constaté une réduction de 79 % de leurs coûts de déploiement, tandis que les applications de WAN intelligent sur le APIC-EM peuvent accélérer de 85 % les provisionnements.

Du fait du nombre élevé d'utilisateurs et d'appareils se connectant depuis une grande variété de sites, la périphérie du réseau peut se trouver dans de vastes campus ou dans des sites distants de taille modeste. Des vues topologiques globales dotées de fonctionnalités automatisées prêtes à l'emploi réduisent sensiblement les coûts liés à l'intégration de nouveaux appareils ou à leur mise à jour, qu'il s'agisse de commutateurs, de routeurs ou de points d'accès. Les applications supplémentaires sur le contrôleur permettent le provisionnement de la qualité de service (QoS) sur l'ensemble du réseau, ce qui facilite une protection rapide du trafic essentiel à l'activité en cas de consommation de bande passante non essentielle. Grâce aux applications spécialisées comme le WAN intelligent Cisco (IWAN), vous pouvez assurer le provisionnement, le suivi et les dépannages liés à la sécurité, au chiffrement, à l'acheminement ainsi que la visibilité sur les applications et leur contrôle depuis le WAN.

Par ailleurs, le logiciel Cisco ONE™ offre un moyen efficace et flexible pour vous procurer des logiciels destinés à la périphérie de votre réseau. À chaque étape du cycle de vie du produit, le logiciel Cisco

ONE facilite l'acquisition, la gestion et la mise à niveau de votre infrastructure. Réalisez un excellent ROI à mesure que vous investissez dans l'innovation, les mises à jour et les mises à niveau de vos machines virtuelles et physiques.

La sensibilité aux applications et aux terminaux

Cisco est le seul fournisseur travaillant en partenariat avec Apple, un leader mondial du secteur des appareils mobiles, pour offrir une meilleure expérience de mobilité. Ce partenariat stratégique pour les deux entreprises permet d'exploiter les informations collectées au niveau du réseau pour offrir la meilleure expérience Wi-Fi à travers une itinérance optimisée. En d'autres termes, ce partenariat ouvre une voie rapide aux applications essentielles de l'entreprise installées sur les appareils Apple iOS sur le lieu de travail afin d'améliorer la productivité des collaborateurs.

Les entreprises peuvent espérer une itinérance jusqu'à huit fois plus rapide, des appels Wi-Fi plus fiables à 66 %, une réduction de 50 % des coûts fixes de gestion du réseau suite à la diminution du nombre de SSID, et enfin une utilisation de la batterie des appareils réduite de 30 %.

Depuis de nombreuses années, Cisco offre des innovations Wi-Fi dépassant les standards en vigueur et qui servent de référence aux standards futurs. La technologie sans fil Cisco Aironet® offre des expériences haute densité innovantes qui améliorent les ondes radio, les performances des appareils et l'utilisation des applications. Cisco a également mis au point la technologie Flexible Radio Assignment qui optimise les performances du réseau Wi-Fi sans limiter la disponibilité des ondes radio. Cela permet aux points d'accès sans fil d'identifier les besoins de bande passante sans fil non planifiés et d'adapter automatiquement le réseau pour y répondre. Cette fonctionnalité est essentielle dans les lieux où de nombreux utilisateurs sont rassemblés et se disputent la bande passante sans fil disponible.

L'entreprise numérique dépend des applications qu'elle utilise pour augmenter la productivité et interagir avec les clients. Cisco offre une visibilité et un contrôle sur les applications permettant de détecter les applications à la périphérie du réseau filaire et sans fil. Nous utilisons un contrôle intelligent de l'acheminement pour sélectionner le meilleur chemin sur votre WAN tout en optimisant la circulation sur votre LAN filaire ou sans fil afin que vos utilisateurs puissent utiliser leurs applications dans les meilleures conditions possible.

Les entreprises peuvent bénéficier d'une visibilité totale sur plus de 1 200 applications et hiérarchiser les applications essentielles d'un simple clic grâce au module APIC-EM et à Cisco Prime Infrastructure.

La périphérie permet de gérer et d'améliorer l'expérience des collaborateurs dans l'espace physique. Le plafond numérique de Cisco permet d'étendre les avantages de l'Internet des objets en faisant converger les réseaux de plusieurs bâtiments. Ces avantages concernent notamment :

- L'éclairage
- Le chauffage et la climatisation
- La vidéo IP
- Les capteurs de l'Internet des objets
- Et bien davantage, via une plate-forme réseau intelligente et sécurisée.

Un plafond numérique améliore l'expérience des collaborateurs et leur productivité tout en réduisant les coûts d'exploitation des installations.

Une solution pour répondre aux défis à venir

Conçue pour le futur, sans système d'exploitation Cisco IOS-XE dont la programmabilité est basée sur des modèles standardisés, la solution de périphérie de Cisco prépare le réseau à accueillir de nouvelles fonctionnalités et à s'adapter aux évolutions de l'environnement, de l'activité et du secteur. La périphérie du réseau devient ainsi ouverte, programmable et extensible.

La périphérie effectue actuellement une transition, passant d'un modèle qui s'adapte à chaque appareil, et où la segmentation et le contrôle d'accès sont ajoutés sur une configuration de réseau, à une solution entièrement constituée de politiques automatisées. À l'avenir, il ne sera plus nécessaire de provisionner directement les réseaux. Vous pourrez définir vos politiques sous forme de simple intention. De plus, vous pourrez définir des utilisateurs ou des groupes d'utilisateurs ayant accès à certains ensembles d'applications ou de données à caractère confidentiel, que ceux-ci soient hébergés localement ou dans le cloud. Le réseau sera provisionné automatiquement pour mettre en œuvre les politiques définies, tout en conservant une flexibilité exceptionnelle permettant d'assurer la surveillance, les dépannages, les résolutions ou l'application de services supplémentaires à certains types de trafic.

La périphérie devient aussi entièrement programmable. Les solutions d'orchestration peuvent communiquer avec la périphérie à l'aide d'API standard basées sur des modèles, de scripts Python ou d'autres outils de type Linux. Ceci simplifiera les méthodes actuelles d'intégration de la périphérie dans le développement de logiciels et permettra d'offrir une agilité et une adaptabilité sans précédent.

L'innovation continue à la périphérie du réseau

Face à l'explosion annoncée de la connectivité et à toutes les opportunités qu'elle fera naître, de plus en plus d'entreprises admettent actuellement que cette transformation entraînera nécessairement un bouleversement de leur infrastructure de réseau et de leurs capacités de gestion et d'analyse de données. Nous ouvrons la voie de cette transformation en innovant dans les domaines des infrastructures de réseau, de la gestion de cette infrastructure et du traitement analytique des données en vue d'en extraire des informations exploitables.

La démarche de Cisco vise à passer d'une approche réactive du dépannage à une approche proactive et à réduire les délais de résolution de plusieurs jours à quelques minutes. C'est pourquoi nous attribuons à chaque appareil du réseau un rôle de détecteur tout en le faisant contribuer au traitement décentralisé des données. Le fait de collecter des données depuis les appareils de la périphérie et de les traiter au plus près de leur point de collecte nous permet d'offrir une analyse en temps réel et de générer des informations exploitables grâce à l'apprentissage automatique.

Forts de la plus importante base installée de clients et du plus grand nombre de solutions ASIC adaptées à des réseaux existants, nous sommes parfaitement positionnés pour concevoir un matériel et des logiciels optimisés pour l'analytique. Vous pouvez exploiter la puissance de la base installée. L'association du filaire et du sans fil dans un même réseau signifie que l'intelligence en périphérie peut vous aider à résoudre les problèmes, qu'ils se produisent à la périphérie ou non, en quelques secondes. Au fil du temps, certains problèmes pourront même être corrigés avant de se manifester. Ceci aidera les départements IT à assurer la qualité de service qui sera exigée quant aux performances des réseaux et des applications de demain.

Conclusion

Étant donnée l'importance prise par la périphérie du réseau, la standardisation des réseaux LAN et WAN filaires et sans fil présente des risques qui pourraient entraîner des failles de sécurité, des pertes de productivité et de revenus, des pertes d'opportunités et un manque de visibilité. La périphérie du réseau de Cisco permet aux entreprises de ne pas s'en tenir à une approche standardisée et limitée par les standards en vigueur pour bénéficier, en périphérie, d'une intelligence à haute valeur ajoutée.

Cette approche permet aux entreprises de :

- Protéger l'activité grâce à une première ligne de défense solide
- Fournir des applications en toute confiance aux utilisateurs
- Proposer une expérience transparente à leurs collaborateurs, où qu'ils se trouvent
- Faciliter les interactions avec les clients pour générer de nouvelles sources de revenus
- Gérer de meilleure façon les appareils connectés à l'Internet des objets et proposer un environnement physique optimisé
- Permettre une visibilité optimale sur l'activité effective au sein de l'entreprise

Informations complémentaires

Pour en savoir plus, visitez le portail dédié à nos solutions d'accès unifié à l'adresse http://www.cisco.com/c/en/us/solutions/enterprise-networks/unified-access/index.html.

C11-737691-00 08/16