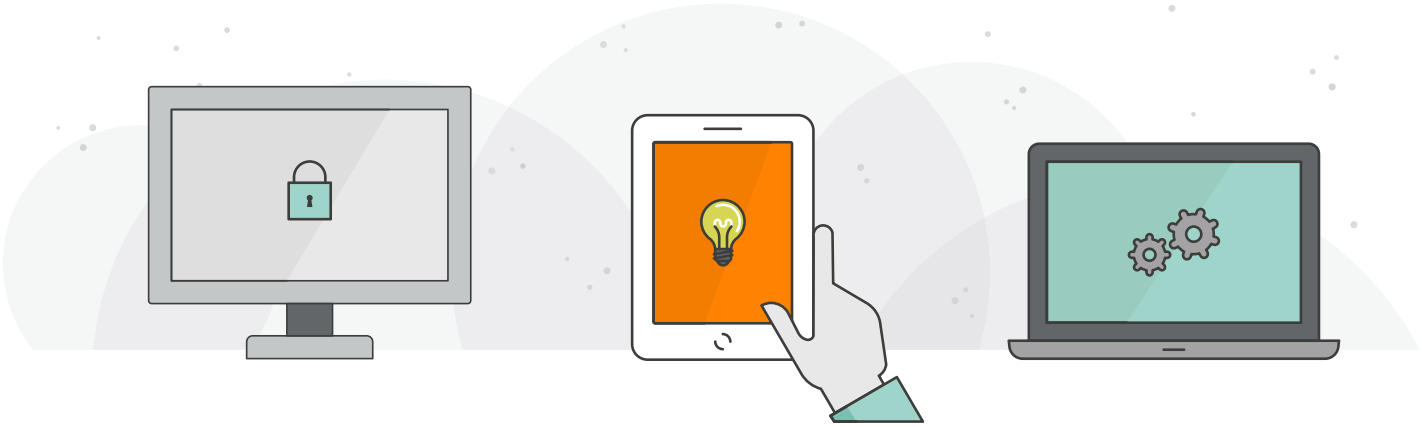
CINQ RÈGLES SIMPLES POUR UN RÉSEAU PLUS PERFORMANT



En suivant ces cinq règles simples, vous disposerez à coup sûr d'un réseau basé sur le cloud à la fois intelligent, fiable et sécurisé, grâce auquel votre entreprise restera dans le coup.

1. RENDEZ LA GESTION PLUS FLEXIBLE, PLUS ÉVOLUTIVE ET PLUS SIMPLE

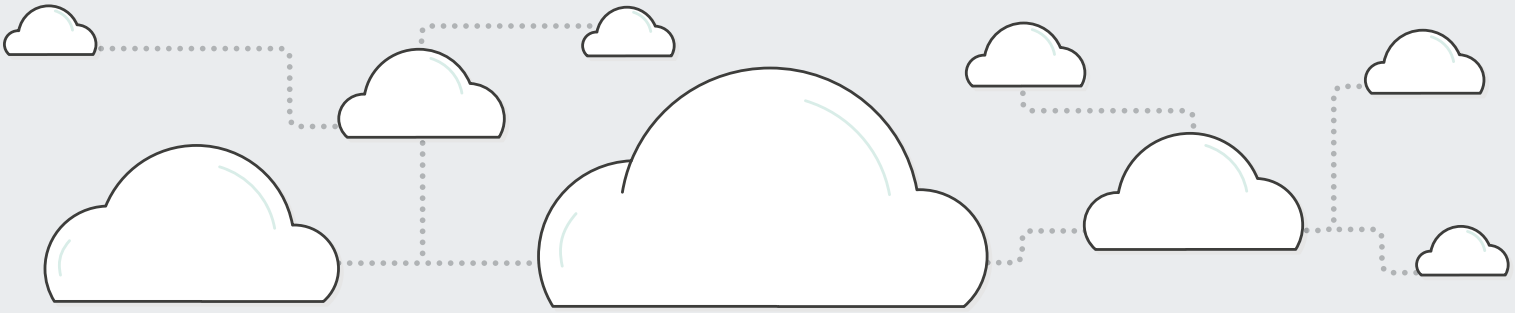
Avec un réseau géré dans le cloud, vous avez la possibilité d'adapter facilement les ressources à mesure que votre entreprise évolue. Vous devez en outre tirer profit de solutions Web et mobiles grâce auxquelles vous pouvez, le cas échéant, centraliser ou distribuer facilement des tâches de gestion. Cela vous évite de dépendre d'un seul système de gestion limitant votre flexibilité et votre capacité à ajouter les fonctionnalités avancées que peut exiger un réseau en pleine croissance. Veillez également à utiliser des outils de machine learning, capables d'identifier les problèmes réseau et d'optimiser les performances.

2. GARANTISSEZ UNE CAPACITÉ ET UNE COUVERTURE SUFFISANTE

À quel rythme votre réseau actuel évolue-t-il ? Quels seront vos besoins futures en disponibilité ? Aujourd'hui, la plupart des gens utilisent plusieurs devices – souvent simultanément. Le nombre d'utilisateurs et la quantité de trafic ne cessent d'augmenter, et il en sera de même pour le nombre de points d'accès (PA) requis pour que tous les utilisateurs restent connectés sur chaque device. Si les PA peuvent prendre en charge plus de 200 devices par radio, vous devez, de votre côté, vous préparer à gérer cette capacité en disposant d'au moins 60 clients actifs par radio. Le but : garantir une expérience utilisateur transparente à chaque utilisateur du réseau.

Identifiez les zones où la densité d'appareils est la plus forte, ainsi que les zones inactives. Découvrez où et comment optimiser votre réseau afin de bénéficier d'un meilleur débit grâce à des PA supplémentaires. Fournissez une couverture Wi-Fi là où se trouvent vos utilisateurs actuels, mais également là où l'accès sera nécessaire dans le futur. Enfin, prévoyez assez tôt comment vous couvrirez les lieux difficiles, par exemple ceux pouvant nécessiter six PA Wi-Fi pour satisfaire les besoins de communautés denses et exigeantes.

aruba
a Hewlett Packard Enterprise company



3. PROPOSEZ UNE SÉCURITÉ ADAPTÉE AUX ENJEUX ACTUELS ET FUTURS

Les pirates affinent leurs méthodes jour après jour. Aussi, vous devez vous préparer non seulement à répondre à leurs attaques actuelles, mais aussi à parer, à l'avenir, leurs tentatives de pénétration de votre réseau. Les outils de détection d'intrusion sont indispensables pour identifier et bloquer les utilisateurs non autorisés ainsi que les attaques par malware.

Utilisez des mesures de sécurité telles que l'AES (Advanced Encryption Standard), un pare-feu de niveau 7 et une protection contre les intrusions Wi-Fi pour vous protéger face aux risques d'intrusion dans les transactions financières, les données de santé et les institutions gouvernementales.
Recherchez des solutions de sécurité dotées de contrôles automatiques et d'application intégrée, dont l'efficacité augmente au fil de l'évolution de votre réseau, comme le contrôle d'accès réseau (NAC), afin de protéger les devices IoT en croissance rapide.

4. PRENEZ EN CHARGE LES APPLIS DONT LES CLIENTS ONT BESOIN ET LES SLA SUR LESQUELS ILS PEUVENT COMPTER

Les clients attendent toujours plus de la part de leurs fournisseurs, qu'il s'agisse d'une meilleure bande passante pour un meilleur streaming vidéo ou d'outils de collaboration plus complets. Point commun de ces attentes : un accès facile à des applications nouvelles et améliorées. Votre réseau doit pouvoir offrir la visibilité et les fonctionnalités de gestion requises pour prendre en charge et enrichir les applications nouvelle génération. Cette prise en charge doit s'appuyer sur des accords de niveau de service (SLA) grâce auxquels les clients bénéficient des performances et de la protection attendues – qu'il s'agisse d'une bande passante à la demande ou d'une résolution des incidents proactive permettant de résoudre les problèmes avant même que les utilisateurs ne les détectent.

5. RÉDUISEZ LES TEMPS D'ARRÊT AU STRICT MINIMUM AVEC UN RÉSEAU 100 % REDONDANT

Seuls les administrateurs doivent pouvoir déceler les temps d'arrêt. Et encore, ces mêmes administrateurs doivent être mis au courant uniquement après l'auto-correction du problème par le réseau ! Avec les solutions de redondance actuellement disponibles sur le marché, il n'y a plus aucune raison de tolérer le moindre temps d'arrêt. La clé du succès repose dans la mise en place — au sein de votre réseau — de fonctionnalités stratégiques qui maintiennent la connectivité même en cas de défaillance d'un commutateur, lien ou point d'accès.

Ces cinq règles simples vous mettront sur la bonne voie pour créer un réseau adapté aux enjeux actuels et futurs. Besoin d'une solution à la fois simple, intelligente et sécurisée ? Parlons-en ensemble. Contactez Aruba dès aujourd'hui.

aruba
a Hewlett Packard Enterprise company

3333, SCOTT BLVD | SANTA CLARA, CA 95054 (ÉTATS-UNIS)
+1 844 473 27 82 | Tél. : +1 408 227 4500 | Fax : +1 408 227 4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com

030920