PERSPECTIVES

Les coûts (à peine) cachés du LAN :

favoriser la simplicité opérationnelle et des licences

Synthèse

Le réseau local (LAN) filaire et sans fil est la clé de voûte d'une infrastructure IT. Il permet des applications de nouvelle génération et dope la productivité des utilisateurs. En tant que tel, le LAN a un impact particulièrement positif sur l'expérience utilisateur. Le LAN est également le point d'origine et de fin de nombreux évènements de sécurité.

Les administrateurs IT actuels doivent concevoir des réseaux de nouvelle génération qui permettent une expérience utilisateur sécurisée et transparente. La commutation sur Ethernet et le Wi-Fi comptent parmi les technologies IT les plus matures. Cependant, face à une demande en croissance, les fournisseurs technologies ont introduit des coûts opérationnels dissimulés.

"78% des décisionnaires IT indiquent préférer opter pour une seule marque pour l'ensemble de leur matériel réseau, plutôt que d'associer des solutions provenant de multiples fournisseurs."[1]

Les tendances qui alimentent les coûts opérationnels

La complexité des environnements hétérogènes

Pour différentes raisons, les entreprises font appel à de multiples fournisseurs pour bâtir leur réseau filaire et sans fil. Les critères de choix varient : cycles de mise à jour, familiarité avec un fournisseur particulier, préférences qui évoluent, coûts et même le critère de disponibilité. Il en résulte des LAN hétérogènes qui creusent les coûts et nourrissent la complexité.

Chaque fournisseur dispose de sa propre interface de gestion, ce qui impose aux équipes IT de jongler entre différentes consoles pour connaître l'origine d'un incident identifié. Ces équipes sont également souvent contraintes de faire appel aux équipes de support de différents fournisseurs, des équipes qui ne sont pas vraiment motivées à collaborer entre elles pour traiter un incident.

La multiplication des licences

Le commutateur Ethernet et le point d'accès sans fil sont les éléments de base du LAN. Dans un passé pas si lointain, se procurer ces équipements faisait l'objet d'un investissement (CapEx). Le coût d'un commutateur Ethernet, hors support et maintenance, ne résumait à la somme réglée pour acquérir ce matériel. L'achat d'un point d'accès sans fil faisait également l'objet d'un investissement, jusqu'à l'avènement du contrôleur sans fil (WLC - Wireless LAN Controller). Ceci générait des licences par point d'accès sans fil dont le coût était souvent intégré à celui du WLC. Dans les deux cas, un administrateur IT pouvait budgétiser le coût du réseau sans fil en tant qu'investissement initial.

Les administrateurs IT doivent désormais gérer de multiples coûts de licence et abonnements pour leurs équipements et outils de gestion de leur réseau sans fil. Ces licences, et les coûts associés, portent sur des composantes basiques comme un système d'exploitation, ou plus complexes, comme une solution de visibilité sur les applications. Il est aujourd'hui commun qu'une commande soit assujettie à des termes et conditions complexes et peu compréhensibles qui régissent des fonctions auparavant incluses dans l'investissement matériel. Cette tendance a lourdement creusé les charges d'exploitation.

"69% des entreprises disposent de davantage objets connectés que d'ordinateurs sur leurs réseaux."[2]

3 erreurs à éviter en matière de licence

Gestion

Le cloud est devenu une plateforme de prédilection pour gérer le LAN. La dimension pervasive de cette option de gestion la rend particulièrement opportune. Cependant, la licence sous forme d'abonnement peut être source de confusion et coûteuse.

Ces licences peuvent présenter des coûts et fonctionnalités différents. Dans certains cas, le matériel acheté en investissement ne fonctionne pas en l'absence de licences. Pour maîtriser ces coûts d'exploitation, il s'agit de bien comprendre la nature des licences de gestion cloud de chaque fournisseur. D'autre part, une option de déploiement sur site doit être proposée, car importante lorsque les équipes IT souhaitent migrer hors du cloud sans subir de pénalités.

Visibilité sur les endpoints

Difficile de gérer un réseau sans savoir ce qui est connecté à ce réseau. Les systèmes d'authentification peuvent indiquer aux administrateurs les utilisateurs présents sur le réseau, mais pas forcément les dispositifs. Les équipes IT doivent donc identifier manuellement ces dispositifs connectés, une tâche chronophage, peu précise et coûteuse. Nombre de fournisseurs exigent une licence et/ou un abonnement pour offrir une visibilité sur les endpoints et, souvent, ceci n'inclut pas l'accueil sécurisé de ces endpoints sur le réseau. Ces besoins essentiels doivent être traités sans coûts supplémentaires.

Sécurité

De nombreux évènements de sécurité démarrent au niveau de l'edge filaire ou sans fil du LAN, le périmètre qui accueille les connexions des utilisateurs et des endpoints. Souvent, les réseaux filaires et sans fil ne sont pas conçus dans une optique de sécurité. La sécurité est souvent déployée en tant que couche supplémentaire, ce qui cloisonne davantage les fonctions et pèse sur l'efficacité de la protection. Pour les administrateurs IT et de sécurité, ce faible niveau d'intégration rallonge les délais pour détecter et résoudre les problématiques. Les charges d'exploitation s'envolent lors des évènements de sécurité tandis que ces retards accentuent les dommages résultant de l'attaque.

Comment choisir une solution LAN Edge intégrée ?

Une solution traditionnelle de LAN, qui implique un investissement en matériel et non un abonnement, ne relève pas forcément du passé. Recherchez des fournisseurs qui proposent les fonctionnalités clés requises. Une solution de LAN Edge doit offrir, à minima :

- Une gestion unifiée des réseaux filaires et sans fil, sur site ou dans le cloud
- Un matériel qui reste opérationnel même en cas d'expiration d'une licence
- Une veille pour identifier ce qui est connecté au LAN et capable de réagir face à des dispositifs prohibés.
- Une sécurité intégrée et efficace

Pour simplifier le déploiement et la gestion du LAN edge et optimiser le coût total de possession (TCO), une solution capable de faire converger sécurité et réseau est requise. Une architecture sécurisée et simple à gérer, disposant de l'ensemble des fonctionnalités clés, permet de maîtriser les dépenses opérationnelles tout en dopant les performances.

[1] "Networking Technology Trends in 2020 and Beyond," Spiceworks Ziff Davis, consulté le 1er février 2022.

[2] "How Prepared Is Your IT Department for Attacks on IoT Devices?" Virginia Business Systems, consulté le 1er février 2022.

FORTINET®

www.fortinet.com/fr

16. mai 2022, 13:21
1455202-0-1-FR