FORTINET

LIVRE BLANC

Livre blanc | Réseaux filaires et sans fil sécurisés : mode d'emploi

Principaux défis et solutions

Synthèse

Au sein d'un réseau corporate, la surface d'attaque la plus large est celle de la couche d'accès au réseau. Cette couche prend en charge toute la connectivité au réseau (filaire via des commutateurs Ethernet et sans fil via des points d'accès) des collaborateurs, des partenaires, des invités ou des objets connectés. Alors que les dispositifs sont toujours plus nombreux à se connecter au réseau chaque jour, sécuriser la couche d'accès devient critique. Compte tenu de la généralisation du télétravail suite à la pandémie de la COVID-19, une sécurité pertinente contre les attaques ciblant la couche d'accès n'a jamais été aussi importante.[1]

La mise à jour du réseau local permet d'actualiser un périmètre souvent négligé du réseau. Elle peut également mener à une gestion et une visibilité de bout en bout[3].

Les carences des infrastructures d'accès

Le Edge LAN constitue une cible potentielle pour les cybercriminels, surtout à un moment où la survie de nombre d'entreprises issues de différents secteurs d'activité dépend du réseau. De leur côté les attaques progressent : sur le seul premier trimestre 2020, les attaques par DDoS (distributed denial-of-service) qui cherchent à submerger les réseaux ont bondi de 542% par rapport au trimestre précédent (T4 2019).[2]

Les directions IT font face à nombre de défis dans la gestion de leur couche d'accès, parmi lesquels :

- Assurer la synchronisation des différentes configurations
- Disposer d'une visibilité sur l'ensemble du réseau
- Gérer différents niveaux d'accès
- Coût total de possession élevé

Pour mieux gérer un réseau sécurisé, les entreprises misent sur des approches de plateformes intégrées. Une solution, qui associe la gestion des réseaux filaires/sans fil et la sécurité, devient de plus en plus courante, alors que les directions IT visent à maîtriser les coûts opérationnels. Mais toutes les solutions réseau n'offre pas la simplicité, les fonctionnalités et les performances requises.

La complexité engendre des défis pour les réseaux locaux (LAN)

Les réseaux LAN traditionnels gagnent en complexité alors qu'il s'étendent pour accompagner la croissance des entreprises et le nombre d'utilisateurs. Il en résulte que les administrateurs IT consacrent davantage de temps à assurer le suivi des flux entrants et sortants. Avec le déploiement de bureaux/sites distants et la progression du travail à domicile, l'exploitation du LAN gagne en complexité et se révèle coûteux.

Gérer les configurations

- Même dans le cas de très grandes entreprises informatisées, une seule petite modification peut perturber des composantes essentielles du réseau. Elles doivent s'assurer que tout changement ou mise à jour peut être tracé et géré pour garantir que tous les segments du réseau sont opérationnels et synchronisés les uns par rapport aux autres.
- Les environnements réseau sur les sites distants peuvent également présenter des problématiques de configuration. L'installation et le pilotage d'un standard sur de nombreux lieux et sur des topologies disparates sur les sites distants sont susceptibles de lourdement peser sur les ressources IT.

La visibilité du réseau

- Les réseaux des campus corporate évoluent en permanence, avec des dispositifs appartenant à des collaborateurs, des partenaires et des invités qui s'y connectent et se déconnectent en permanence.

- Les objets connectés posent un défi particulier en termes de visibilité. Alors que ces dispositifs se connectent au réseau, les équipes doivent pouvoir concrétiser les cas d'utilisation envisagés, sans pour autant mettre la sécurité du réseau en péril. Sur les sites ne disposant pas d'équipes IT, cet objectif est plus complexe à tenir, puisque la seule information sur un dispositif en particulier est celle fournie par l'interface de la couche d'accès.

Coût total de possession (TCO) élevé

- Les LAN modernes ont tenté d'apporter des solutions à leur problématique de complexité, en investissant dans de nouvelles licences ou abonnement pour répondre aux différentes besoins des équipes IT. En intégrant l'ensemble de ces fonctionnalités, le coût total de la solution a été multiplié par deux, si ce n'est trois par rapport au coût initial du réseau.
- De plus, alors que de nouveaux systèmes et outils se connectent en ligne pour gérer et sécuriser l'edge du LAN, les équipes de sécurité se voient contraintes de se former à différentes interfaces solution, déconnectées les unes par rapport aux autres.

Les LAN ont souvent été négligés du point de vue de la sécurité et ne disposent donc pas toujours de fonctionnalités essentielles comme le chiffrement, le contrôle d'accès et la visibilité granulaire. Les cybercriminels se rendent ainsi compte que le LAN est souvent vulnérable.[4]

Sécurité

- Alors que les réseaux LAN gagnent en complexité, la sécurité des points entrants sur le réseau pour les utilisateurs autorisés peut également gagner en complexité. Bon nombre d'entreprises déploient des produits de sécurité ciblés pour restaurer les failles de sécurité identifiées, l'une après l'autre. Cette approche peu organisée est préjudiciable. Une seule erreur de configuration au sein d'un outil de sécurité LAN peut aboutir à un incident réseau critique.

Les critères pour évaluer une solution pertinente

Lors de la mise à jour d'un réseau LAN filaire et ou sans fil, les entreprises sont invitées à se pencher sur les critères décisionnels suivants :

- ✓ **Structure de la topologie.** Pour déployer un LAN sécurisé, un élément important est la nature des sites qui accueilleront le réseau. S'agit-il de plusieurs campus d'envergure ou plutôt de petits sites distants ? Des travailleurs distants auront-ils besoin de connectivité ? Très souvent, la solution devra répondre à plusieurs exigences opérationnelles. Chaque topologie présente ses propres défis, contraintes, et la solution retenue doit donc se montrer évolutive pour pouvoir accompagner les différents scénarios opérationnels.
- ✓ **Dispositifs connectés.** Quels seront les profils d'équipements connectés au réseau ? Qui seront les différents utilisateurs ? Le LAN doit rester sécurisé lorsque les invités et partenaires auront besoin de se connecter avec leurs dispositifs extérieurs. Une solution Edge LAN pertinente doit pouvoir prendre en charge tous les types de dispositifs et d'utilisateurs qui se connectent, sans faire constamment appel aux équipes IT. Les technologies d'agrégation de liens offrent aux architectes réseau un moyen simple de répondre à une demande croissante de bande passante des dispositifs.[6]
- ✓ **TCO faible.** Si une solution est capable d'offrir l'ensemble des fonctionnalités ci-dessus, les coûts cumulés de licence, de formation et d'abonnement à des fonctions à la carte peut se révéler important. Les décisionnaires en matière de réseau doivent prendre en compte le nombre de systèmes et de solutions à acheter pour que la fonctionnalité souhaitée soit opérationnelle sur l'ensemble de l'organisation, ainsi que le nombre de licences et des abonnements récurrents potentiels à des fonctionnalités clés.

  D'autre part, le coût total de possession va au-delà des investissements et des abonnements. Le temps consacré par les équipes pour déployer et maintenir une solution peut également varier de manière importante. Les décisionnaires doivent s'interroger sur le niveau de complexité de la solution en matière de gestion. La solution est-elle prête à l'emploi ou faut-il l'associer à de nombreux autres modules pour assurer un fonctionnement pérenne ?
- ✓ **Sécurité intégrée.** Nombre de solutions LAN ne disposent pas de sécurité intégrée. Ceci implique de rajouter une couche de sécurité en aval du déploiement, ce qui est source de coût et de complexité. Parfois des fonctions de sécurité sont proposées mais elles ne sont pas intégrées au Edge LAN. Ceci peut entraîner des failles qui sont autant d'opportunités pour les cybercriminels de perpétrer leurs exactions. Les réseaux doivent être conçus et opérés dans un contexte de sécurité pour assurer la meilleure des protections possible avec un impact minimal sur la gestion globale de l'infrastructure LAN.

Un accès sécurisé exige une solution transparente

Les réseaux LAN filaires et sans fil constituent le backbone de toutes les entreprises, mais ils représentent également un investissement important en temps et en budget pour les directions IT. Choisir la bonne solution aide les équipes IT à mener à bien et concrétiser les projets d'entreprise.

Il existe de nombreux fournisseurs d'équipements réseau aujourd'hui sur le marché et les décisionnaires IT doivent évaluer toutes les options pour identifier une solution qui offre de la flexibilité en matière de déploiement au niveau de la couche d'accès, ainsi qu'une sécurité intégrée, afin d'assurer la pérennité des opérations.

[1] "In addition to traditional DDoS attacks, researchers see various abnormal traffic patterns," Help Net Security, 21 juillet 2020.

[2] Ibid.

[3] Andrew Froehlich, "A Network's Weakest Link May be Different Than you Think," Network Computing, 26 novembre 2019.

[4] Ibid.

[5] Ibid.

762006-0-1-FR

mars 5, 2021 12:50 PM

wp-FA-challenges-to-achieving-secure-wired-and-wireless-solution-A4_FR