IDC TECHNOLOGY SPOTLIGHT

Réinventer le réseau en le faisant détecteur de menaces et outil de sécurisation

Octobre 2015

Adapté de la publication *Worldwide Enterprise Network Infrastructure Forecast*, 2015–2019 de Nolan Greene, Rohit Mehra, Rich Costello et autres, IDC #258012

Sponsorisé par Cisco

Aujourd'hui, le réseau occupe une place plus importante que jamais sur la liste des objectifs de l'entreprise. De ce fait, la quantité de données sensibles qui traversent les réseaux filaires et sans fil ne cesse d'augmenter. Cette abondance de données stratégiques pour l'entreprise attire de plus en plus de hackers et d'applications malveillantes. Si l'intelligence et le caractère distribué du réseau profitent aux cybercriminels qui y trouvent une mine d'informations, ils permettent également de faire du réseau un outil de sécurité proactif. Aujourd'hui, grâce à la visibilité et à la segmentation du trafic, le réseau peut devenir un détecteur de menaces et un outil de sécurisation de l'entreprise.

Introduction

L'avènement de ce qu'IDC appelle la « 3e plate-forme » a fait naître un modèle de technologies et d'applications reposant sur le cloud, la mobilité, le Big Data et les médias sociaux. Le réseau occupe aujourd'hui un rôle majeur dans les décisions stratégiques en matière d'innovation. Cette transition s'explique notamment par l'accès 24 h sur 24 et 7 jours sur 7 à des applications stratégiques que permet la 3e plate-forme, ce qui a favorisé la collaboration, a éliminé les obstacles spatio-temporels et a accéléré l'innovation. Avec l'arrivée massive de nouveaux appareils et de nouvelles applications dans l'entreprise, des données plus sensibles traversent le réseau, ce qui intensifie les exigences de sécurité du cœur jusqu'à la périphérie. Dans les faits, 80 % des entreprises payent le prix d'une faille dans la sécurité. Même si l'on exclut les incidents majeurs, 1,3 million de dollars partent en fumée chaque année suite à des attaques qui aboutissent.

En un mot, les réseaux d'entreprise n'ont jamais été aussi compliqués à gérer qu'aujourd'hui. Chaque nœud, chaque application, chaque certificat, chaque cloud, chaque appareil, chaque utilisateur qui accède au réseau est une proie potentielle. S'il n'est pas immédiatement détecté et éliminé, un programme malveillant ou un vecteur d'attaque peut se propager très rapidement, indépendamment de son point d'entrée sur le réseau. Pourtant, les mêmes ressources qui sont intelligemment connectées et dont profitent les hackers constituent paradoxalement l'une des plus grandes richesses du réseau. En effet, les informations collectées sur le réseau peuvent être exploitées pour détecter proactivement les différents types d'attaques et y remédier. Grâce aux progrès réalisés en matière d'intelligence du réseau, ce dernier peut servir de capteur pour détecter rapidement les menaces. En d'autres termes, il aide à définir l'activité normale et à identifier rapidement ce qui est anormal. Le réseau contribue ainsi à sa propre sécurité en se transformant progressivement en outil de sécurisation dont le rôle est de contrôler les accès pour anticiper les attaques.

Une cible qui bouge

Dans de nombreuses entreprises, le BYOD et la généralisation de la mobilité continuent à accroître le nombre d'appareils présents sur le réseau. L'utilisation des appareils personnels utilisés pour le travail (BYOD) complique la sécurisation du réseau et peut même faire exploser la quantité de données sensibles qui le traversent. De surcroît, chaque périphérique accédant au réseau de l'entreprise est un terminal à protéger. Parallèlement, l'utilisation par les employés de leurs propres appareils mobiles pour effectuer des tâches essentielles a donné naissance à un écosystème florissant d'applications cloud pour le mobile. Celles-ci compliquent davantage les flux du trafic réseau dans la mesure où leur hébergement, et celui des données qu'elles génèrent, peut être interne ou externe, dans des clouds publics ou privés. Ces applications sont ensuite distribuées à divers endroits sur le réseau de l'entreprise, du siège aux succursales et même jusqu'aux télétravailleurs se connectant via leurs appareils mobiles. Elles représentent de nouvelles surfaces d'exposition aux attaques qui contiennent de vastes quantités de données sensibles ou non et peuvent également constituer des points d'intrusion sur le réseau.

L'adoption grandissante de l'Internet des objets (IoT) dans l'entreprise accentue encore la complexité du réseau. L'IoT est un réseau de réseaux de terminaux (ou objets) identifiables de manière unique et qui communiquent sans interaction humaine, à l'aide d'une connectivité IP, à l'échelle locale ou internationale. IDC estime que près de 30 milliards d'appareils IoT seront déployés d'ici 2020. Ces terminaux ou capteurs rendent le réseau encore plus vulnérable. À ce stade encore embryonnaire de l'évolution de l'IoT, les interfaces de sécurité ne sont pas toujours simples à configurer et sont même parfois difficiles à intégrer à l'infrastructure de sécurité globale. Face à la problématique de sécurisation de l'IoT, l'incertitude inquiète. L'intérêt de l'IoT réside essentiellement dans les données que les appareils/capteurs peuvent collecter. Il est à cet égard difficile d'en imaginer le volume, l'ampleur et la profondeur. Aujourd'hui, de nombreux environnements accueillent déjà des appareils IoT qui collectent en masse d'importantes données structurées ou non, dont la sécurité et la confidentialité posent problème. Pour tirer le meilleur parti de l'Internet des objets, il faut intégrer étroitement la sécurité du réseau.

Compte tenu de l'évolution constante de la mobilité dans l'entreprise, du déploiement d'applications hébergées dans le cloud public pour améliorer la productivité et de l'adoption généralisée de l'IoT, le service informatique de l'entreprise doit réévaluer son approche en matière de sécurité du réseau. Les décideurs experts en sécurité des réseaux en sont d'ailleurs bien conscients. En fait, une récente étude menée par IDC auprès de professionnels de la sécurité révèle que 52 % des sondés craignent que les employés sous-estiment l'importance des politiques de sécurité. Près de 45 % des personnes interrogées se montrent inquiètes face à la complexité grandissante des attaques. Par ailleurs, elles sont nombreuses (38 %) à penser que leurs budgets sont trop maigres pour relever ces nouveaux défis.

Ces défis ne font que s'intensifier au côté de problèmes de financement et de support liés à la sécurisation du réseau. Dans ces conditions, le service informatique de l'entreprise peine à détecter les attaques, à y remédier et à appliquer les mesures nécessaires pour éviter que ces incidents ne se reproduisent. L'étude d'IDC montre qu'il faut parfois plus d'une année pour que l'adoption d'une infrastructure de sécurité, type 3e plate-forme avec solutions de sécurisation des terminaux et de gestion des utilisateurs, soit généralisée dans l'entreprise. À l'ère de la 3e plate-forme, il est impératif de déployer une architecture de sécurisation du réseau qui soit adaptative, intelligente et évolutive, et qui se présente sous la forme d'une plate-forme entièrement intégrée dans l'infrastructure de réseau existante. Ce type de modèle de sécurisation, qui tire parti de l'intelligence distribuée intrinsèque du réseau, lui permet de se défendre contre les intrusions au lieu d'être une surface d'exposition aux attaques passive. Les hackers avancent rapidement, d'où la nécessité d'un réseau capable de réagir à la même vitesse.

Le réseau, une ressource pour la sécurisation

Avec la standardisation de la gestion des réseaux, les entreprises disposent d'une excellente visibilité sur leurs réseaux, du data center jusqu'à la périphérie, en passant par les différents sites géographiquement dispersés. Cette visibilité concerne les appareils, les utilisateurs et les applications. Grâce à la collecte de ces données et aux outils analytiques de plus en plus avancés, les réseaux sont aujourd'hui capables de détecter les activités anormales et douteuses. Les intrusions de programme malveillant sur le réseau, les flux de trafic anormaux, l'utilisation non autorisée d'applications, les autres infractions aux règles d'utilisation et les appareils et points d'accès sans fil non approuvés sont plus faciles à identifier, à écarter et à contrer grâce à l'intelligence du réseau.

Exploiter efficacement le réseau pour le sécuriser implique de le percevoir et de s'en servir comme un détecteur de menaces et un outil de sécurisation agissant sur l'ensemble du réseau, notamment dans les data centers, les succursales et les campus, et sur tous les terminaux et applications qu'il rencontre. L'utilisation de l'infrastructure de réseau comme outil de sécurisation ne remplace pas les fonctionnalités de sécurité du réseau, comme les services de pare-feu et celles permettant une protection avancée contre les programmes malveillants. Au contraire, elle les complète. Le paragraphe suivant explique comment la solution de sécurité globale de Cisco peut être déployée dans cette optique.

Envisager la solution Cisco

La gamme Cisco de solutions de sécurisation du réseau repose sur un principe : la sécurité doit être intégrée en tout point du réseau. Il est possible de sécuriser le réseau en toute transparence, depuis l'infrastructure jusqu'à l'utilisateur final. Il convient pour cela d'utiliser NetFlow (qui permet au réseau de jouer le rôle d'un détecteur de menaces) et de l'intégrer à Cisco ISE (Identity Services Engine) pour bénéficier d'un contrôle plus granulaire, ainsi qu'à TrustSec pour segmenter le réseau. Les outils présentés dans ce paragraphe permettent l'utilisation du réseau dans son ensemble comme ressource de sécurisation.

NetFlow et Lancope

L'approche Cisco consistant à utiliser le réseau comme un détecteur de menaces repose sur un outil clé : NetFlow. Il est capable de créer des enregistrements continus de tous les échanges transmis à travers les routeurs et les commutateurs Cisco et à travers certains équipements Cisco sans fil. Chaque session de communication sur un appareil NetFlow offre d'excellents niveaux de visibilité et d'analyse, notamment sur six activités souvent très importantes, à savoir l'analyse du réseau, la détection de botnets, le déni de service, les attaques par fragmentation, le changement de réputation d'hôte et la propagation des vers.

Les données peuvent être stockées pour une utilisation ultérieure, ce qui fait de NetFlow un outil essentiel dans l'identification des intrusions. Des investigations poussées et des journaux de communication globaux renseignent amplement sur les activités douteuses et permettent de détecter et d'éliminer les menaces plus efficacement. Ensemble, NetFlow et Lancope StealthWatch offrent une visibilité sur le réseau avancée et des alertes en temps réel pour identifier les menaces. L'intégration de Lancope StealthWatch avec Cisco ISE permet de corréler le contexte d'un appareil (utilisateur, type et emplacement, moment et mode d'accès) avec le trafic réseau et d'isoler rapidement les appareils infectés.

ISE (Identity Services Engine)

Identity Services Engine est la plate-forme de gestion des politiques de sécurité de Cisco. Elle simplifie et homogénéise l'attribution des contrôles d'accès sécurisé sur l'ensemble des réseaux filaires et sans fil, et pour toutes les connexions VPN. Avec Cisco ISE, l'accès sécurisé des utilisateurs commence par leur authentification et la classification de leurs appareils. Cisco ISE fournit des informations contextualisées pour optimiser le processus décisionnel et s'assurer que le niveau adéquat de contrôle d'accès est accordé dans chaque situation donnée. Grâce à des informations contextuelles plus granulaires comme le rôle, l'emplacement et le moment, Cisco ISE peut décider d'accorder un accès plus restreint au réseau. Tous les aspects de l'accès sécurisé sont donc maîtrisés. En fonction de critères liés aux politiques de sécurité, Cisco ISE propose des options d'accès selon l'utilisateur et l'appareil. Une politique de sécurité unifiée sur l'ensemble du réseau améliore l'efficacité opérationnelle puisqu'il n'est plus nécessaire de gérer et d'appliquer séparément plusieurs politiques, et parce que l'on dispose d'une visibilité sur l'application des politiques.

Segmentation définie par logiciel TrustSec

Cisco TrustSec est une technologie intégrée aux commutateurs, aux routeurs, aux périphériques sans fil et aux dispositifs de sécurité Cisco. Elle permet aux entreprises de réaliser une segmentation du réseau définie par logiciel. TrustSec applique les contrôles d'accès en fonction des rôles définis dans Cisco ISE pour sécuriser l'accès à des ressources du réseau ultrasensibles, d'après le rôle et l'identité de l'utilisateur. TrustSec simplifie la configuration et la gestion des politiques de sécurité qui régissent les échanges sur le réseau, l'accès aux ressources et les modes de communication entre les systèmes. L'application des politiques de sécurité commence dans le data center et s'étend jusqu'à la périphérie et aux VPN distants.

Les bénéfices d'un réseau servant d'outil de sécurisation

Dans un contexte où les dépenses d'exploitation et d'investissement sont soumises à un examen minutieux, le service informatique a tout intérêt à justifier ses décisions d'investissement et à trouver des moyens de tirer pleinement parti du réseau. L'utilisation de l'infrastructure de réseau comme un détecteur de menaces et un outil de sécurisation permet d'exploiter les ressources déjà en place pour protéger le réseau contre des intrusions et éviter une interruption de l'activité et un manque à gagner. Une infrastructure de sécurité globale et intégrée, comme celle qu'offrent les solutions Cisco, tire parti des précieuses métadonnées pour accélérer la visibilité sur le trafic du réseau. L'utilisation conjointe de TrustSec et de Cisco ISE permet un contrôle granulaire des accès en fonction des politiques établies et une segmentation définie par le logiciel pour contrer les attaques et empêcher leur mouvement latéral sur le réseau. Ce type de sécurité est également très évolutif puisque NetFlow, ISE et TrustSec peuvent être déployés sur tout le réseau pour protéger les ressources qu'il connecte.

Challenges et opportunités

Percevoir le réseau de l'entreprise comme un outil de sécurisation à part entière traduit une rupture avec l'approche traditionnelle qui considère que la protection doit venir des ressources extérieures plutôt que du réseau lui-même. Comme dans tout changement radical concernant l'infrastructure informatique de l'entreprise, les décideurs doivent comprendre les tenants et les aboutissants de ce nouveau modèle et changer de mentalité au prix de certains efforts. Par ailleurs, dans les entreprises qui ont déjà développé des infrastructures de sécurisation complexes du réseau, les intéressés pourront être réticents à l'idée de repenser les systèmes en place (en particulier s'ils semblent fonctionner). Le service informatique de l'entreprise doit déjà négocier des virages serrés entre l'optimisation des investissements préexistants et l'adaptation de l'infrastructure actuelle face aux problématiques de demain. Or, cette situation n'est pas différente.

Toutefois, comme bien souvent, ces challenges peuvent se traduire par d'immenses opportunités. Comme nous l'avons expliqué, la mise en œuvre d'une architecture de réseau à laquelle sont étroitement intégrés des composants de sécurité peut représenter un investissement plus rentable qui éliminera les redondances d'une approche au coup par coup. Pouvoir démontrer l'efficacité opérationnelle et le retour sur investissement d'une solution de réseau qui sert de détecteur de menaces et d'outil de sécurisation est certainement la meilleure preuve de sa rentabilité.

Conclusion

À l'ère de la 3e plate-forme, les réseaux d'entreprise jouent un rôle prédominant dans les activités quotidiennes, dans l'engagement des clients et des employés, ainsi que dans la différenciation par rapport à la concurrence et dans l'innovation. Or, les vastes quantités de données sensibles qui traversent ces réseaux attirent de nombreux hackers et cybercriminels qui, en y accédant, peuvent porter préjudice aux clients et aux employés, mais aussi à la réputation de l'entreprise. Fort heureusement, on peut intégrer à ces réseaux des solutions de sécurité globales, pour les armer efficacement contre les attaques de demain. L'intégration étroite de fonctionnalités de sécurisation dans une infrastructure de réseau est fortement recommandée dans le contexte informatique actuel. Un ensemble de solutions comme celui que propose Cisco peut apporter une réponse concrète et pérenne aux entreprises.

Siège social : 5 Speen Street, Framingham MA 01701 États-Unis P.508.872.8200 F.508.935.4015 www.idc.com