Cisco invente le réseau intuitif qui s'occupe de tout

Cisco vient de renforcer son offre de gestion et sécurisation du réseau des entreprises. L'équipementier américain a annoncé une évolution de son réseau en lui ajoutant une dose « d'intuition ». Autrement dit, mettre en œuvre différents outils d'analyse pour déterminer les risques d'infection et d'attaques transportés par le réseau, que ce soit des charges précédemment identifiées ou nouvelles, et reconfigurer l'infrastructure en conséquence.

« Notre solution s'appuie sur la cyber□intelligence Talos de Cisco pour identifier les signatures d'attaques connues, même en trafic chiffré, pour une sécurité qui ne sacrifie rien à la confidentialité », avance David Goeckeler, vice□président et directeur réseau et sécurité de Cisco. Talos, la cellule d'identification des menaces du fournisseur, a pour avantage de pouvoir s'appuyer sur les routeurs et switches de l'Américain disséminés partout sur la planète, et par lesquels transite une bonne partie du trafic mondial, pour effectuer ses analyses et identifier les paquets menaçants. Et en proposer les résultats aux responsables sécurité informatique des entreprises afin d'anticiper les attaques et autres intrusions.

Une approche intuitive

Cette approche « intuitive » se concrétise dans une nouvelle famille de produits que Cisco rassemble derrière la Digital Network Architecture (DNA). A commencer par la nouvelle gamme de switches Catalyst 9000. Dotés de nouveaux Asics (processeurs spécialisés) et de l'OS maison IOS XE, les commutateurs seront taillés pour répondre aux évolutions des besoins, notamment avec l'essor de la mobilité, le Cloud, l'Internet des objets (IoT) et, bien sûr, la sécurité.

Celle-ci passera par Encrypted Traffic Analytics, une solution de Talos qui permet d'analyser les schémas de trafic de métadonnées à coup de cyber-veille et de machine learning. *« Le réseau identifie l'empreinte digitale des menaces connues, même en trafic chiffré, sans déchiffrer le contenu ni compromettre la confidentialité de la data »*, assure Cisco qui avance un taux de précision d'identification des menaces de 99% pour moins de 0,01% de faux positif.

Tableau de bord centralisé et automatisation des accès

DNA s'accompagne également de DNA Center, un tableau de bord qui centralise la gestion des fonctions et offre une visibilité sur l'intégralité du réseau. L'outil entend *« offrir aux équipes IT une approche intentionnelle englobant conception, dimensionnement, politique et assurance »*. Par ailleurs, Network Data Platform and Assurance, une plate-forme d'analytique prédictive, permettra de tirer au mieux parti de la valeur des données.

Enfin, DNA s'accompagne de Software□Defined Access (SD□Access), une solution de SD-WAN pour

automatiser les tâches répétitives dans l'optique de simplifier l'accès des utilisateurs, équipement et objets au réseau. Selon les premières remontées avancées par l'équipementier, SD-Access permettrait de réduire de 67% le délai de dimensionnement du réseau (par rapport à la précédente solution Cisco, suppose-t-on), d'augmenter de 80% la résolution des problèmes, de réduire l'impact des brèches de sécurité de 48% et les dépenses opérationnelles de 61%. Des chiffres que les utilisateurs auront l'occasion d'en vérifier la justesse (ou pas).

Une intégration en quelques heures

« Le nouveau réseau offre un monde où vous pouvez connecter des milliards de périphériques, les identifier presque instantanément, savoir ce qui est digne de confiance et ce qui ne l'est pas, et tirer une valeur exponentielle des connexions – et vous pouvez le faire en quelques heures au lieu de semaines ou de mois », résume Chuck Robbins, le CEO de Cisco, sur son blog. Autrement dit, un réseau automatisé qui, une fois en place, se passe quasiment de l'intervention humaine. Du moins sur le papier.

Ces nouveautés seront rendues disponibles au fil des prochains mois, à commencer par les boitiers Catalyst en juin et juillet, suivis de DNA Center et SD Access en août tandis qu'il faudra attendre septembre pour Encrypted Traffic Analytics et novembre pour Network Data Platform et Assurance.

Lire également
Cisco recule sur le marché des switches et routeurs, Huawei en profite
Cisco panse les switches vulnérables aux zero days de la CIA
SD-WAN : Cisco s'empare de son concurrent Viptela