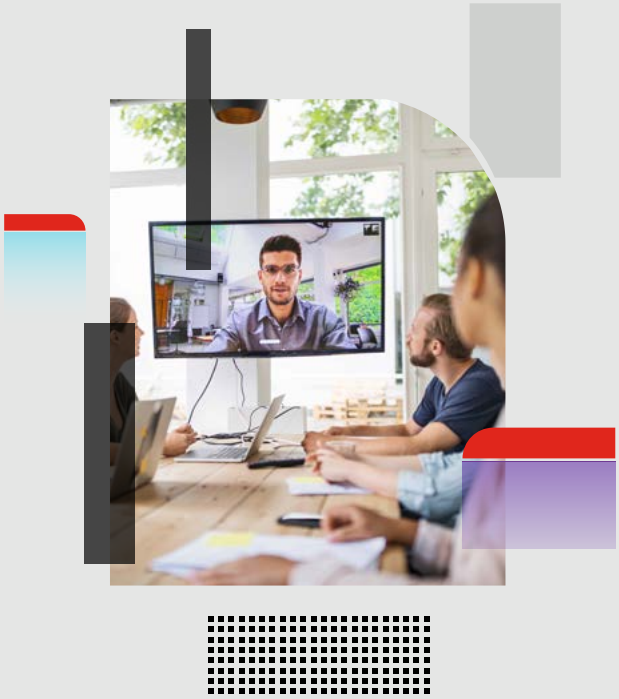
PERSPECTIVES

Sécurité des réseaux hybrides : cinq erreurs à proscrire



La majorité des entreprises actuelles dispose d'un réseau hybride. Selon Gartner, le récent passage forcé au télétravail a eu un impact durable sur les réseaux. « Jusqu'en 2024, les entreprises seront amenées à accélérer leurs projets de transformation digitale d'au moins cinq ans pour pouvoir s'adapter à un monde post-covid-19 qui se caractérise par un télétravail toujours plus important et de nouveaux points de contact numériques. »[1]

Cependant, les réseaux hybrides actuels ne facilitent en rien une visibilité et un contrôle centralisés, notamment pour les entreprises qui ne disposent pas d'une stratégie centrale de sécurité. Bien au contraire, les entreprises ont déployé, en moyenne, plus de 45 outils de sécurité sur leur réseau, souvent proposés par des éditeurs différents. D'autre part, chaque incident à traiter exige de coordonner 19 solutions différentes. Une telle complexité pèse sur la visibilité, limite le contrôle et induit des failles de sécurité qui ne demandent qu'à être exploitées.[2]

La consolidation et l'intégration de la sécurité et du réseau sont pertinentes pour répondre à des environnements aussi complexes. Le déploiement d'un pare-feu de nouvelle génération (NGFW), en tant que clé de voûte d'une stratégie unifiée de sécurité, aboutit à une visibilité de bout en bout, une gestion et un contrôle simplifiés et une application uniforme des règles sur l'ensemble du réseau. Cependant, choisir la bonne solution n'est pas simple, etle risque d'erreur existe.

Cinq erreurs classiques lors de la sécurisation des réseaux hybrides

Erreur 1—Adopter une solution de sécurité 100 % cloud. Certaines entreprises envisagent de remplacer leur sécurité traditionnelle par une solution SASE (secure access service edge). Cependant, peu d'entre elles disposent d'un environnement 100 % cloud. Dans la réalité, les réseaux sont hybrides. Ainsi, opter pour une stratégie de sécurité cloud-only peine à protéger des utilisateurs qui travaillent sur des sites d'entreprise en local.

Selon Gartner, les déploiements classiques de pare-feu en périphérie de data centers ne sont pas obsolètes et doivent être pérennisés pour sécuriser les flux de données entrants traditionnels et les connexions sortantes résiduelles des utilisateurs internes qui restent affectés sur site, au siège social ou sur les sites distants d'envergure.[3]

Erreur 2—Ignorer l'importance du data center sur site. Pour de multiples raisons, nombre d'entreprises ne peuvent migrer certains de leurs services sur site vers le cloud. Mais nombre de ces services doivent néanmoins se rendre disponibles à l'intention des clients externes et des utilisateurs corporate, ce qui rend les pare-feu sur site d'autant plus essentiels.

Le rapport de Gartner valide cette approche, tout en reconnaissant les défis liés aux solutions de sécurité des fournisseurs cloud. Une minorité non négligeable d'entreprises considère ces offres comme moins matures que celles d'éditeurs tiers spécialisés en sécurité et déploient parfois ces solutions tierces directement au sein d'instances IaaS dans le cloud public. Les opérateurs privés de clouds publics et privés offrent des solutions natives de pare-feu, WAF, anti-DDoS et ADC.»[4,5]

Les réseaux hybrides ont besoin d'une solution de sécurité qui fonctionne en natif dans tous les environnements et qui en protège l'ensemble des edges de manière cohérente. Ceci démarre par une plateforme commune de pare-feu réseau active sur chaque edge réseau : campus d'entreprise, data center, sites distants, clouds privés et publics. Ce service de pare-feu doit également protéger les collaborateurs distants et mobiles.

« Pour les applications accessibles au public et hébergées au sein de data centers privés, il est recommandé que les professionnels de l'IT envisagent un modèle traditionnel de pare-feu d'entreprise sécurisant l'edge du réseau ».[6]

Erreur 3—le mythe du "Best-of-Breed". L'erreur est de penser qu'une approche best-of-breed assure une meilleure sécurité de l'edge réseau. Au contraire, une telle approche entraîne souvent une prolifération de produits distincts, aboutissant à un réseau complexe et des architectures cloisonnées de sécurité, incapables de partager efficacement les informations de veille sur les menaces. Ceci remet en cause l'intérêt même de mettre en œuvre une posture robuste de sécurité : les solutions distinctes ne peuvent offrir le même niveau de sécurité et de visibilité que celles conçues pour collaborer entre elles. Seuls les écosystèmes intégrés de sécurité, bâtis dans l'optique de partager les données de veille sur les menaces, sauront assurer un traitement pertinent, coordonné et rapide des cyber-évènements.

Un système unifié est toujours plus sécurisé que la somme de ses composants individuels. À titre d'exemple, comment une approche « best-of-breed » gère-t-elle le cas d'un utilisateur disposant d'un PC portable conforme, mais qui y insère une clé USB non autorisée ? La majorité des dispositifs isolés de sécurité réseau ne saura détecter et répondre à cette menace. En revanche, une solution EDR (endpoint detection and response), conçue pour collaborer avec d'autres systèmes de sécurité, peut notifier le pare-feu NGFW de cette violation. Les règles applicables seront alors mises en oeuvre, donnant lieu, par exemple, à une mise en quarantaine du dispositif incriminé. Ceci n'est possible qu'au sein d'un écosystème de sécurité construit autour d'une plateforme de sécurité commune, capable de partager la veille sur les menaces avec tous les modules de sécurité. Les règles s'appliqueront sur l'ensemble des périmètres nécessaires.

Erreur 4—Ne pas penser de manière globale. Les architectures hybrides en évolution participent à étendre la surface d'attaque, à réduire à la visibilité et à renforcer les risques. Ce qui rend les choses plus complexes est que la part du trafic chiffré devrait atteindre 95 % dans un futur proche.[5] Pour autant, la majorité des pare-feu réseau sont incapables d'inspecter le trafic chiffré sans grever les performances attendues par les applications actuelles. Dans ce contexte, comment sécuriser un réseau lorsque votre visibilité n'est précise que sur 5 % de votre trafic ? D'où l'intérêt, pour les responsables informatiques, d'opter pour une solution NGFW, capable d'évoluer au rythme du réseau et de s'adapter aux opérations qui consomment des ressources importantes (déchiffrement des flux SSL, détection des menaces et remédiation automatisée).»

Cet objectif implique une solution conçue pour prendre en charge les normes les plus récentes de chiffrement, comme TLS 1.3, tout en assurant la fluidité des communications sous TLS 1.2. Au-delà de la visibilité, le vrai défi est de retenir une solution capable d'identifier et de s'adapter à l'état de ressources qui évoluent au fil du temps. Ceci est un vrai défi si votre stratégie de sécurité doit intégrer le multi-cloud. Il s'agit de comprendre comment les différents clouds sont conçus et configurés pour normaliser les règles de sécurité sur l'ensemble des fournisseurs de services cloud. Dans ce contexte, il s'agit de retenir une solution NGFW capable de suivre des ressources cloud publiques et privées en forte évolution, pour ensuite déployer une sécurité de bout-en-bout sur cette architecture IT hybride, ce qui permet d'optimiser la posture de sécurité.

Erreur 5—Le risque d'une confiance accordée par défaut. Traditionnellement, les réseaux plats ont pour ambition de prévenir les attaques provenant de l'extérieur, mais ils permettent à des attaques d'évoluer au sein d'un réseau qu'elles ont déjà infecté. Les entreprises doivent se pencher sur un NGFW capable de fournir une sécurité au-delà du edge, en réduisant la surface d'attaque grâce à la segmentation réseau, pour ainsi prévenir toute menace entrante. Parallèlement, c'est la micro-segmentation qui peut prévenir une propagation en interne des menaces.

Au-delà d'une segmentation dynamique du réseau qui prévient les mouvements internes, un NGFW doit également ajuster le niveau de confiance en surveillant les comportements grâce à des outils de type UEBA (user and entity behavior analytics). Ce pare-feu doit également révoquer la confiance d'un utilisateur ou dispositif qui commence à se comporter de manière suspecte.

Des solutions ZTA (zero-trust access) et ZTNA (zero-trust network access) doivent être déployés pour contrôler l'accès aux ressources réseau, jusqu'à assurer une segmentation par application. La prolifération des dispositifs headless (Internet des objets, Internet des objets industriels) doit également être maîtrisée, tout en assurant une intégration transparente avec une solution de contrôle d'accès réseau. Ceci assure que chaque dispositif, application ou transaction est pris en compte et sécurisé.

Les réseaux hybrides ont besoin d'un pare-feu conçu pour l'univers numérique actuel

Les réseaux hybrides exigent un pare-feu NGFW pour déployer une protection cohérente, une visibilité et un contrôle au sein d'environnements multisites et temps-réel. Il s'agit donc de retenir un pare-feu, proposé sous différents formats, qui sécurise tous les edges, qui s'intègre en toute transparence au réseau et qui offre une application cohérente des règles, une orchestration centralisée de celles-ci, un partage en temps réel des données de veille sur les menaces et une réponse corrélée aux menaces. En activant des règles de sécurité capables de suivre de bout en bout les applications et les workflows, les entreprises bénéficient d'une visibilité large sur leurs réseaux en évolution permanente, tout en optimisant l'expérience d'utilisateurs qui travaillent en différents lieux.»

[1] Gartner, "Forecast Analysis: Remote and Hybrid Workers, Worldwide," Ranjit Atwal, et al., 2 juin 2021. (P1).

[2] Kim Samra, "IBM Study: Security Response Planning on the Rise, But Containing Attacks Remains an Issue," IBM, 30 juin 2020.

[3] Gartner, "How the Shift From Firewall Appliances to Hybrid Cloud Firewalling Will Change Selection Criteria," Aaron McQuaid, 10 mars 2021. (P1).

[4] Idem (P5).

[5] Idem (P5).

[6] Idem (P11).

août 30, 2021 11:09 AM
745599-A-0-FR