Pare-feu : l'évolution des modèles d'utilisation d'Internet l'a-t-il rendu obsolète ?

Technologie de cybersécurité historique, le pare-feu est également l'une des technologies les plus largement connues au monde. Depuis « War Games » en 1983, il est même régulièrement mis en lumière au cinéma, contribuant ainsi à sa notoriété.

En effet, au cinéma, lorsqu'un pirate informatique doit infiltrer un ordinateur central, il est souvent confronté à un pare-feu, qu'il contourne généralement rapidement en tapant frénétiquement sur son clavier. Évidemment la fiction est souvent loin de la réalité, surtout sur des sujets aussi techniques.

Après « War Games » Il aura toutefois fallu attendre près d'une décennie pour que le terme pare-feu entre dans le lexique courant des professionnels de la cybersécurité. Des années 80 aux années 90, des experts tels que Jeff Mogul, Steve Bellovin et Bill Cheswick, Marcus Ranum et Nir Zuk ont fait progresser la technologie. Au milieu des années 90, il était normal pour les entreprises de se connecter à Internet, et le paysage des menaces s'est étendu. Le pare-feu est alors devenu une technologie extrêmement populaire et indispensable aux entreprises.

À l'époque, l'utilisation d'un pare-feu était tout à fait légitime, car l'Internet des années 90, avec ses centaines de serveurs (contre des dizaines de millions aujourd'hui), était plus simple et les menaces moins sophistiquées. Il y avait bien des pirates, mais il s'agissait en majorité de criminels solitaires, contrairement aux groupes, souvent soutenus par des États, que nous connaissons aujourd'hui.
Le pare-feu était donc la solution idéale pour séparer le mauvais trafic du bon : le réseau était sûr, Internet ne l'était pas, et le pare-feu protégeait les entreprises contre les dangers extérieurs.

L'évolution de l'utilisation d'Internet

Le mode d'utilisation d'Internet a radicalement changé depuis les années 90. Il ne s'agit plus uniquement d'un outil qui nous aide à accomplir notre travail au bureau, et de surfer à tire personnel lors de nos temps libres. Internet occupe aujourd'hui une part essentielle de nos existences. La menace ne vient plus des pirates, elle est intégrée dans les applications et les services que nous utilisons tous au quotidien, que ce soient les médias sociaux, les services de streaming ou toute autre application. Même les entreprises de confiance qui forment notre écosystème de fournisseurs sont désormais sources de menaces.

L'industrie du pare-feu n'est pas restée les bras croisés et a étendu les fonctionnalités de ses produits pour faire face à ces nouvelles menaces. Au-delà du filtrage des paquets, les pare-feux se sont dotés d'antivirus, de fonctions de prévention des attaques par déni de service (DoS/DDoS) et de détection des botnets, de VPN, etc.

Le phénomène s'est transformé en véritable course aux armements. Mais plus les fonctionnalités

se sont accumulées, plus la complexité, la latence et les coûts ont augmenté. Tous les contrôles étant regroupés au même endroit, le pare-feu est devenu le seul moyen de défense des entreprises, mais aussi le seul obstacle à contourner pour les pirates.

Même les défenseurs de la première heure du pare-feu ont commencé à remettre en question sa pertinence. En 2008, Cheswick et Bellovin ont qualifié le pare-feu de « solution économique à la faiblesse de la sécurité des hôtes » et de « contrôle d'accès bas de gamme pour des ressources de faible valeur ».

Le développement du Cloud

S'il est une évolution qui a sonné le glas du pare-feu, c'est bien le Cloud (et la mobilité à laquelle il donne accès). La pandémie de Covid a bien entendu accéléré la transition vers le Cloud et contribué à accélérer un peu plus le déclin du pare-feu. Aujourd'hui, les activités professionnelles ont lieu directement sur Internet, en dehors du réseau.

Bien que le pare-feu ait rendu de grands services à la cybersécurité, il s'agit d'une technologie dépassée, qui représente une architecture obsolète. Non seulement il date et multiplie les fonctionnalités, mais il repose en outre sur des notions de confiance archaïques. La mise en place d'un pare-feu suggère qu'un côté de la connexion est plus sûr que l'autre. Or, rien n'est moins vrai avec le trafic Internet qui circule des deux côtés. Cette confiance implicite peut même présenter plus de risques qu'elle n'en réduit.

Le pare-feu voulait que les entreprises fassent confiance au réseau et aux adresses IP alors que, dans le monde actuel, nous devons adopter une approche Zero Trust.

Un accès Zero Trust associe la validation de l'identité de l'utilisateur à l'application d'une politique d'entreprise fondée sur les données contextuelles de l'utilisateur, de l'appareil, de l'application et du contenu pour autoriser un accès direct aux applications et aux ressources. Il s'agit d'amener le trafic vers le contrôle, et non d'engorger le trafic en amenant le contrôle vers lui.

D'après une récente étude d'ESG, plus de 3/4 des équipes de sécurité informatique (77%) prévoient d'adopter un modèle de travail hybride qui nécessitera des exigences plus élevées en matière de sécurité. Un récent rapport que nous avons publié sur les risques liés aux VPN indique que 72 % des entreprises privilégient l'adoption d'un modèle Zero Trust, tandis que 59 % accélèrent leurs efforts en raison de la montée en puissance du télétravail.

Dans un monde où l'on travaille en tout lieu, les contrôles basés sur le périmètre, comme le pare-feu, deviennent rapidement obsolètes. L'approche Zero Trust utilise une architecture Cloud native pour disperser les contrôles de sécurité à des fins de performances et d'évolutivité. Elle constitue un moyen bien plus attractif et efficace pour protéger les entreprises. Avec le pare-feu, l'erreur a été de penser que nous avions besoin d'un meilleur outil, alors que nous avons en réalité besoin d'une meilleure architecture.