Le vilain petit secret du Cloud public : le coût du déchiffrement !

La plupart des applications web sont aujourd'hui servies à travers une connexion HTTP sécurisée. Mais qui dit HTTP sécurisé dit cryptographie. Et qui dit cryptographie dit, du moins traditionnellement, impact sur les performances.

Heureusement, les processeurs modernes sont désormais largement capables d'absorber ce coût en termes de puissance, et de nombreux équipements (clients ou serveurs) intègrent maintenant l'équivalent des crypto-processeurs jadis réservés aux équipements les plus puissants. Ce qui fait qu'aujourd'hui la question de l'impact du chiffrement sur les performances brutes n'est plus vraiment un problème.

Mais cela ne signifie pas pour autant que le chiffrement n'est plus une source de coûts opérationnels supplémentaires.

Car servir une application moderne est loin de ressembler à une paisible ballade directe entre un serveur et son client !

Les données devront transiter par de nombreux relais avant d'atteindre leur destination. On parle ici d'équipements de sécurité et de contrôle d'accès, d'équilibrage de charge et de routage, parfois répartis à travers la planète. Et chacun de ces intermédiaires devra inspecter les données – déchiffrées, évidemment – afin de pouvoir remplir son rôle dans cette chaîne complexe que représentent les réseaux modernes.

Et c'est là que l'affirmation précédente – le chiffrement ne coûte pas cher et n'a plus d'impact sur les performances – commence à s'effondrer !

Bien entendu, en tant que tel, un seul de ces relais n'introduit qu'un très léger retard dans la chaîne. Mais lorsque cela est répété à de nombreuses reprises sur le chemin, ces délais successifs peuvent non seulement commencer à peser, mais -dans le Cloud Public notamment- aussi alourdir significativement la facture.

Car le chiffrement est par nature une opération coûteuse en puissance de calcul. Cela signifie qu'il faut dépenser beaucoup plus de cycle CPU pour chiffrer ou déchiffrer un message qu'il n'en faudra pour exécuter les autres tâches régulières de l'application. Et dans le Cloud public, chaque cycle CPU est une dépense sonnante et trébuchante. Bien entendu, ce coût est généralement parfaitement accepté, car il s'agit de déplacer une charge de capital (l'achat de matériel) par une charge d'exploitation.

Mais si l'on commence à chiffrer et déchiffrer les messages à plusieurs reprises (à différents endroits, par exemple), alors ce coût va très vite grimper. Vous vous retrouvez finalement à devoir payer plusieurs fois pour exactement la même tâche. Ainsi, un traitement qui coûtait un centime coûte désormais cinq centimes, car il est exécuté cinq fois. Multipliez cela par plusieurs centaines de milliers de transactions sur la journée (ou l'heure) et le surcoût devient colossal.

Et puis il faut aussi réaliser que chaque cycle CPU consommé par une opération cryptographique est un cycle perdu pour l'application elle-même, c'est-à-dire pour faire ce pour quoi elle a été conçue : créer de la valeur. Cela peut sembler insignifiant au début, mais à terme cela signifie qu'il faudra augmenter la puissance de calcul louée à votre fournisseur de Cloud plus tôt que prévu.

Bref, vous comprenez maintenant que le slogan populaire de « SSL Everywhere » (SSL partout) ne doit surtout pas donner lieu à des architectures de type « déchiffrez partout » !

Déchiffrement unique : une bonne fois pour toutes

Afin de réduire les coûts et maximiser la rentabilité des cycles CPU que vous payez, prenez le temps de concevoir vos architectures Cloud selon le principe du déchiffrement unique.

Le principe du déchiffrement unique (« Decrypt Once ») dit que vous devriez chercher à réduire le nombre de relais qui ont besoin de chiffrer / déchiffrer les messages en transit.

Évidemment, cela exige une bonne dose de préparation, afin de prendre en compte toutes les applications et tous les services sur lesquels vous vous appuyez pour protéger votre trafic et vos données. Mais si vous n'êtes pas soumis à une réglementation qui exige un trafic chiffré de bout en bout, vous devriez concevoir votre flux de données pour que celles-ci soient déchiffrées au plus tôt afin d'éviter tous les cycles successifs. Si en revanche vous êtes contraints de respecter le chiffrement de bout en bout, il peut malgré tout être intéressant pour vous de réorganiser certains services afin de les regrouper et les faire bénéficier ainsi d'un déchiffrement unique mutualisé.

Associer certains services connexes sur une même plateforme – par exemple l'équilibrage de charge et le pare-feu applicatif web – permettra de réduire sensiblement le nombre d'opérations de déchiffrement sur le chemin des données. Et, accessoirement, de réduire également le nombre de connexions et le temps de transit sur le réseau, ce qui se traduit là aussi par un gain de performances. Mais le vrai gain, évidemment, sera réalisé en matière de cycles CPU économisés.

Toutes les applications peuvent être concernées par cette stratégie, et pas uniquement les plus sollicitées. Il peut certes sembler illusoire d'essayer de réaliser quelques économies aujourd'hui sur une application qui reçoit un faible trafic. Mais les applications grandissent, et leur trafic augmente au cours de leur existence. Ces quelques centimes économisés au début peuvent déboucher, en fin de vie, sur des économies substantielles.

Et, tout comme les centimes, les microsecondes s'additionnent ! Ainsi, en prenant soin des conditions de déchiffrement sur tout le chemin de vos données, vous pourrez contribuer à réaliser des bénéfices à la fois pour vos bilans annuels, mais aussi pour vos utilisateurs.