SOPHOS
Cybersecurity evolved.

Le chiffrement a-t-il rendu votre pare-feu actuel obsolète ?

Cinq fonctions d'inspection TLS à avoir dans votre prochain pare-feu

Un livre blanc Sophos. Juin 2021

Cinq fonctions d'inspection TLS à avoir dans votre prochain pare-feu

La part de trafic chiffré sur les réseaux s'est rapidement accrue, mais la plupart des pare-feux Next-Gen sont incapables de l'inspecter, ce qui pose un sérieux problème de sécurité.

Sur la plupart des réseaux, plus de 90 % du trafic est chiffré et il traverse le pare-feu sans être filtré. Cela n'est pas dû au fait que les équipes informatiques ne souhaitent pas l'inspecter, mais que la plupart des pare-feux ne sont tout simplement pas à la hauteur de la tâche. Et même si le pare-feu est en mesure d'inspecter le trafic chiffré, il arrive trop souvent que la solution d'inspection TLS soit mal implémentée, et son utilisation aura pour effet de casser de nombreux sites Web et offrira une mauvaise expérience aux utilisateurs.

Naturellement, les hackers n'ont pas attendu pour exploiter ce défaut de visibilité dans la sécurité des organisations, et profitent de cette vulnérabilité pour introduire des menaces dans les réseaux et les y maintenir.

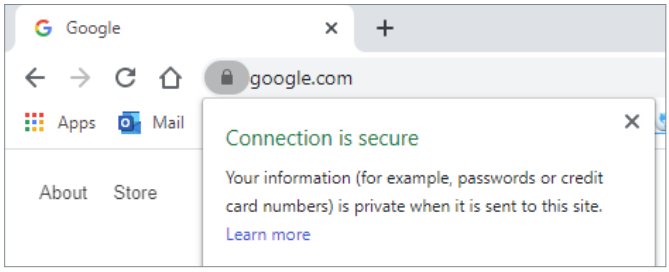
Ce livre blanc vous permettra de comprendre comment le chiffrement a rendu la plupart des pare-feux Next-Gen obsolètes, et vous découvrirez également quels sont les défis de l'inspection TSL et les cinq fonctions d'inspection SSL dont vous avez besoin pour combler cette faille de sécurité.

Le chiffrement assure la confidentialité, pas la sécurité

Souvent, les utilisateurs pensent que les connexions Internet sont « sécurisées » parce qu'elles sont chiffrées. Mais « sécurisées » contre quoi exactement ?

La norme TLS ou Transport Layer Security est la norme de chiffrement utilisée sur Internet aujourd'hui. Les acronymes SSL ou TLS sont souvent utilisés de manière interchangeable. En réalité, SSL est une ancienne norme qui s'est vue éclipsée par TLS ; mais SSL reste le terme le plus couramment utilisé. Retenons simplement que la plupart des gens font référence à TLS lorsqu'ils parlent de SSL.

La norme TLS a été conçue pour assurer confidentialité et authenticité, en chiffrant la communication entre deux parties et en vérifiant que le serveur est bien celui qu'il prétend être sur la base de son certificat et de son émetteur.



Le symbole du cadenas dans votre navigateur indique que la connexion est chiffrée — à des fins de confidentialité.

Mais le chiffrement TLS NE sécurise PAS le contenu de la page Web et il n'en donne aucune garantie. Un site hébergeant des charges utiles de malwares peut avoir une connexion chiffrée et « sécurisée » parfaitement valide.

Lorsqu'un utilisateur affirme que sa connexion à un serveur Web est sécurisée, il veut simplement dire qu'elle est protégée contre l'espionnage (même si ce n'est pas toujours le cas). C'est pourquoi il est primordial d'inspecter le trafic chiffré.

L'inspection TLS des flux chiffrés, une tâche difficile

Le défi de l'inspection TLS est que TLS est un protocole très complexe. Il faut échanger différents certificats et les suites de chiffrement à utiliser doivent être négociées afin de déterminer comment la connexion doit être chiffrée. Qui plus est, il existe plusieurs versions de TLS, et bon nombre d'applications et de services Web n'utilisent pas les mêmes.

Résultat : il est très probable que, malgré l'existence de normes rigoureuses, les choses soient incompatibles. Cela pose d'énormes problèmes aux diverses solutions de sécurité qui tentent de s'injecter dans le processus afin d'inspecter et de sécuriser le contenu échangé.

L'importance de TLS 1.3 et la fin de certains mythes

La bonne nouvelle est que la dernière norme TLS, TLS 1.3, offre un certain nombre d'avantages par rapport aux versions précédentes en termes de performances, de confidentialité et de traitement des vulnérabilités.

L'adoption de TLS 1.3 sur les serveurs n'en est qu'à ses débuts, mais tous les principaux navigateurs prennent désormais en charge cette norme. Toutefois, un grand nombre de pare-feux dotés de l'inspection TLS aujourd'hui disponibles sur le marché ne prennent pas pleinement en charge la norme 1.3, en raison de la complexité et de l'effort de R&D nécessaires à sa mise en œuvre. Au lieu de cela, ils imposent de revenir à la version TLS 1.2. Les connexions se retrouvent donc exploitables et exposées aux attaques en raison des vulnérabilités existantes.

Comme pour beaucoup de nouvelles technologies, il existe un certain nombre de mythes ou de malentendus assez courants sur l'inspection TLS 1.3. L'un d'entre eux est qu'il n'est pas possible d'inspecter le trafic TLS 1.3. Cela est faux. S'il est vrai que l'inspection TLS passive, qui se faisait en marge, n'est plus possible, avec la participation d'un terminal coopérant (comme c'est le cas sur un réseau d'entreprise), l'inspection reste tout à fait possible.

Un autre mythe est qu'en inspectant les flux de trafic chiffrés, vous les rendez en quelque sorte moins sécurisés. Cela est vrai si vous passez d'une connexion TLS 1.3 à une connexion TLS 1.2, comme le font aujourd'hui de nombreuses solutions d'inspection TLS. Les failles de TLS 1.2 ouvrent la voie aux attaques malveillantes de type man-in-the-middle (MITM). La version TLS 1.3 a été conçue pour remédier à ces vulnérabilités. L'inspection du trafic sans baisse des performances de la connexion n'introduit donc aucun risque.

Enfin, certains prétendent que l'épinglage des certificats rend l'inspection TLS impossible. Bien que cela soit vrai pour certaines applications avec des certificats codés en dur, la plupart des applications utilisent une approche d'épinglage qui respecte le certificat démissionnaire et continuent de fonctionner avec les solutions d'inspection SSL.

L'importance de la validation des certificats

La validation des certificats est un élément fondamental du protocole TLS, car elle permet au client (ou au dispositif d'inspection comme le pare-feu) de prouver l'identité du serveur d'où provient la communication.

Toutefois, pour fonctionner, cette validation doit être implémentée correctement. Si ce n'est pas le cas, les pare-feux et les terminaux auxquels ils sont connectés peuvent être « trompés » en croyant communiquer avec un serveur qui ne l'est pas, ce qui peut ouvrir la voie à une attaque MITM malveillante.

Un équilibre entre performances, confidentialité et protection

À toutes ces complexités techniques liées aux flux de trafic chiffré TLS, viennent s'ajouter des contraintes liées aux politiques et aux règlementations qui doivent également être prises en compte et respectées. Par ailleurs, le trafic des applications d'entreprise et les médias en streaming peuvent représenter une bonne partie du trafic chiffré TLS qui ne nécessite pas nécessairement d'inspection.

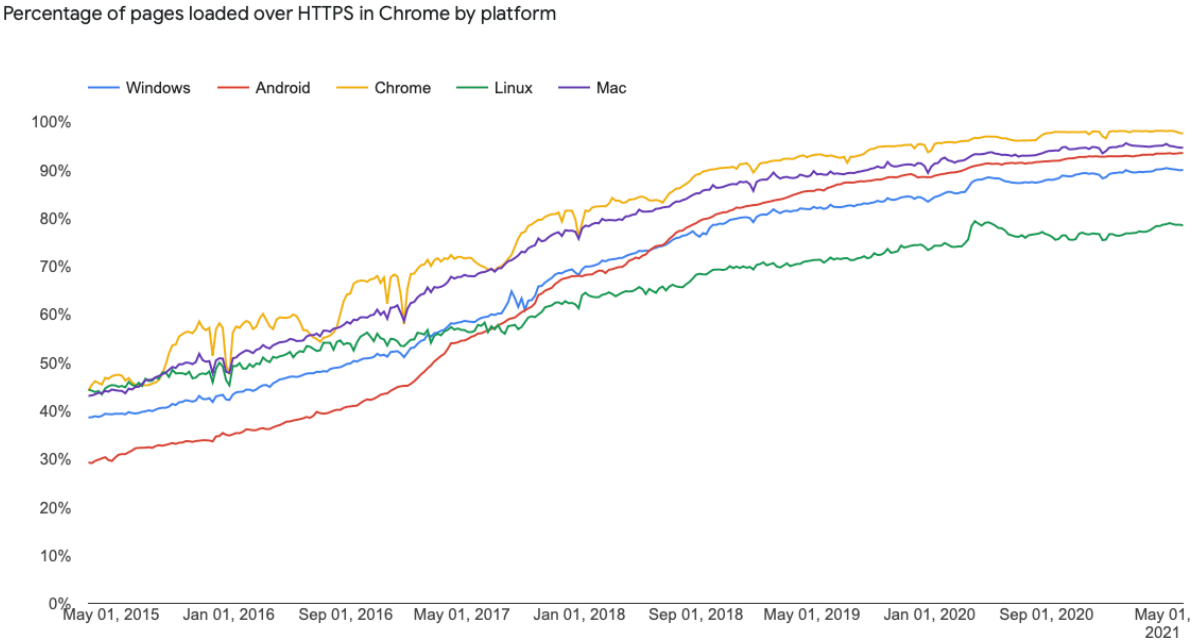
La conclusion est que tout le trafic chiffré ne peut pas ou ne doit pas être traité de la même manière. C'est une question d'équilibre : vous devez trouver la bonne mesure entre confidentialité, sécurité, conformité et performances. Cet équilibre peut vous être dicté par certaines règlementations, ou bien vous devrez trouver vous-mêmes le bon équilibre pour votre organisation.

Malheureusement, les limites des solutions d'inspection TLS dans la plupart des pare-feux actuellement sur le marché obligent les organisations à adopter une approche très déséquilibrée : les besoins en matière de sécurité et de conformité sont sacrifiés pour fournir des performances et une interopérabilité indispensables.

Le volume du trafic chiffré avoisine les 100 %

La plupart des connexions Internet sont désormais entièrement chiffrées. En fait, selon le rapport de transparence de Google, plus de 90 % des sessions Web sont désormais chiffrées, ce qui représente une hausse spectaculaire par rapport aux 60 % d'il y a deux ans.

Rapport de transparence de Google



Le volume du trafic chiffré a augmenté de façon spectaculaire au cours des deux dernières années et atteint presque les 100 %.

Le chiffrement a-t-il rendu votre pare-feu obsolète ?

Cette croissance considérable du trafic chiffré a généré un énorme défaut de visibilité en matière de sécurité pour la plupart des organisations. Leurs pare-feux actuels ne sont tout simplement pas en mesure d'inspecter ce fort volume de connexions chiffrées. Le chiffrement TLS a rendu la plupart des pare-feux obsolètes, car ils n'ont plus de visibilité sur la majorité du trafic qui transite sur le réseau.

Les menaces cachées dans le trafic chiffré : le véritable danger

Avec la croissance explosive du chiffrement TLS ces dernières années, il n'est pas étonnant que les hackers et les attaquants s'emparent de cette tendance et l'exploitent pour introduire des malwares sur les réseaux sans être détectés — et les y maintenir.

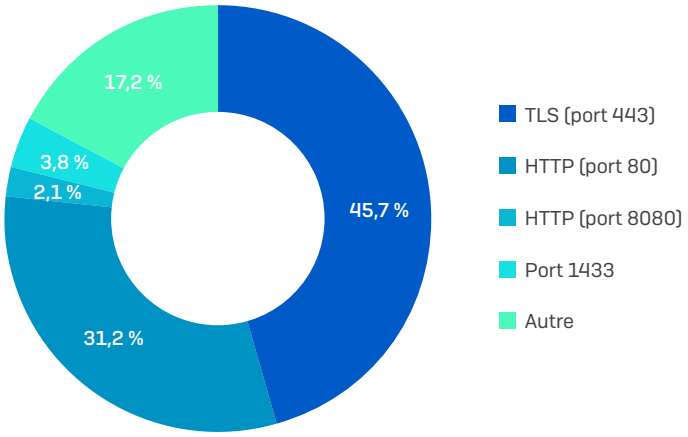
L'an dernier, nous avons constaté une augmentation de l'utilisation du TLS dans les attaques de ransomware, notamment pour les ransomwares déployés manuellement, qui s'explique en partie par le fait que les attaquants recourent à des outils modulaires qui exploitent le chiffrement. Mais la majorité du trafic TLS malveillant provient de malwares de compromission initiale : chargeurs, droppers et programme d'installation de documents qui reviennent sur des pages Web sécurisées pour récupérer leurs paquets d'installation.

Presque toutes les menaces pénètrent désormais sur les réseaux via des connexions chiffrées

Une fois qu'une menace est entrée sur le réseau, elle utilise tous les stratagèmes possibles pour ne pas être détectée. L'utilisation du TLS permet aux commandes envoyées au client par les serveurs de contrôle de ne pas être détectées, tout en dissimulant les informations collectées sur le réseau ainsi que toute autre charge utile téléchargée sur l'hôte compromis.

Il n'est pas étonnant que les malwares utilisant le TLS pour dissimuler leurs communications aient connu une croissance spectaculaire l'an dernier. En 2020, 23 % des malwares que nous avons détectés et qui communiquaient avec un système distant sur Internet utilisaient le TLS ; aujourd'hui, ils sont près de 46 %.

Communications C&C des malwares : comparatif des différents protocoles, 1er trimestre 2021

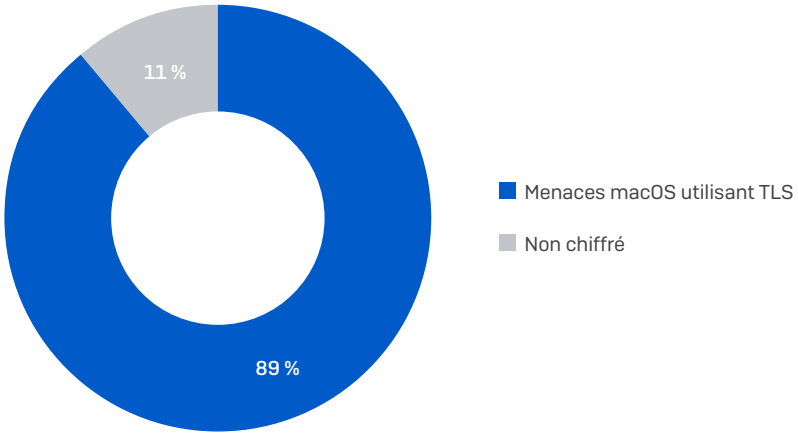


Répartition des communications sortantes des malwares

Il existe également une portion importante de communications TLS qui utilisent un port de protocole Internet autre que 443 — comme les malwares utilisant un proxy Tor ou SOCKS sur un numéro de port non standard.

Les pirates commencent également à héberger des contenus malveillants sur des services de partage légitimes comme Discord, Github et Google Cloud, qui utilisent le chiffrement TLS pour garantir la confidentialité du contenu. Cette pratique aide à dissimuler parfaitement les malwares, ce qui permet aux menaces de pénétrer dans la plupart des réseaux sans être détectées.

Les menaces ne sont pas les seules à utiliser le chiffrement pour ne pas être détectées. Les applications potentiellement indésirables comme les spywares, les adwares et les barres d'outils des navigateurs, ainsi que les clients de partage de fichiers peer-to-peer et les outils d'évitement de proxy utilisent également le chiffrement pour échapper à la détection des pare-feux. Cela est particulièrement vrai sur la plateforme macOS, où plus de 89 % des menaces macOS avec des communications C&C ont recours au TLS pour effectuer des « call home » ou récupérer du code nuisible supplémentaire.



La plupart des organisations sont impuissantes à agir

Comme nous l'avons vu, l'inspection TLS est complexe et demande beaucoup de ressources. Avec plus de 90 % du trafic réseau désormais chiffré, peu de pare-feux sont à la hauteur pour une inspection efficace.

En réalité, la plupart des pare-feux actuels ne disposent pas des fonctionnalités d'inspection TLS appropriées. Ils sont incapables de déterminer intelligemment ce qui doit être inspecté et ce qui ne doit pas l'être. Et tout déchiffrer représente une énorme charge qu'ils ne peuvent pas gérer. Leurs moteurs de traitement des paquets et d'inspection profonde des paquets (DPI) ne sont pas conçus pour traiter efficacement l'inspection TLS. De plus, implémenter un inspection de mauvaise qualité, qui ne prend pas en charge les dernières normes, entraîne une baisse de la sécurité, ce qui expose les organisations à des vulnérabilités tout en créant de très mauvaises conditions d'utilisation.

La progression rapide du trafic réseau chiffré et l'incapacité de la plupart des pare-feux Next-Gen à l'inspecter correctement donnent lieu à une véritable crise dans la sécurité réseau.

Cinq fonctionnalités à rechercher dans votre prochain pare-feu

Pour minimiser les risques liés au trafic réseau chiffré, assurez-vous que votre prochain pare-feu inclut ces 5 principales fonctions d'inspection TLS :

1. Un moteur d'inspection en streaming moderne et performant qui prend en charge les dernières normes telles que TLS 1.3 et fonctionne efficacement sur tous les ports/protocoles pour identifier le trafic à risque et les menaces.
2. Des listes d'exclusion intelligentes et prédéfinies qui sont mises à jour de manière dynamique, afin d'éviter de planter Internet pour les sites et les services ne prenant pas en charge ou ne nécessitant pas de déchiffrement.
3. Une visibilité dans le tableau de bord sur vos flux de trafic chiffré et les problèmes éventuels liés aux sites et aux services non compatibles, ce qui vous permet d'ajouter des exceptions au fur et à mesure avant que la situation ne s'aggrave.
4. Une validation solide des certificats capable de gérer les certificats invalides, autosignés, révoqués ou non approuvés pour éviter les attaques malveillantes de type Man-in-the-Middle (MITM).
5. Des outils de politique qui vous permettent de prendre en compte la confidentialité des utilisateurs, la sécurité de l'organisation et les performances du réseau afin de trouver l'équilibre parfait répondant à vos besoins.

Sophos Firewall, conçu pour l'Internet chiffré moderne

La toute nouvelle architecture Xstream de Sophos Firewall et les appliances de la série XGS offrent la meilleure solution d'inspection TLS disponible dans un pare-feu. Elles vous permettent d'éliminer les problèmes de défaut de visibilité du chiffrement TLS sans impacter les performances. Ses avantages :

- De hautes performances : un moteur de streaming léger et repensé offrant une connexion haut débit.
- Un tableau de bord offrant une visibilité inégalée sur les flux de trafic chiffrés et les problèmes éventuels, avec la possibilité d'ajouter des exclusions en deux clics seulement.
- Une sécurité optimale, prenant en charge le protocole TLS 1.3 et toutes les suites de chiffrement modernes avec une fonction robuste de validation des certificats.
- Une inspection de tout le trafic, indépendamment de l'application et du port utilisés.
- Une vaste liste d'exclusions intégrée pour garantir des performances optimales et une expérience utilisateur de qualité, avec une interopérabilité étendue pour éviter de casser Internet.
- Des outils puissants de création de politiques de sécurité offrant l'équilibre parfait entre performances, confidentialité et protection.

Pour en savoir plus, consultez notre présentation de la solution Sophos Firewall ou lancez une démonstration instantanée en ligne sur www.sophos.com/firewall.

Essayez-le gratuitement

Essayez Sophos Firewall en ligne gratuitement sur sophos.fr/demo

Sophos France
Tél. : 01 34 34 80 00
Email : info@sophos.fr

21-06-17 FR (DD)

SOPHOS