Cryptage, confidentialité et protection des données: un acte d'équilibre

Les mandats d'entreprise, de confidentialité et de sécurité pour une inspection SSL / TLS complète

zscaler™

Sommaire

Le chiffrement à clé publique SSL / TLS est la norme de l'industrie en matière de protection des données et il est utilisé pour sécuriser les transactions Web pour la majeure partie d'Internet. Son chiffrement sécurisé protège les données confidentielles en transit et offre aux utilisateurs la confiance et l'anonymat. Mais il offre également une protection contre les personnes malveillantes, qui utilisent SSL / TLS pour exploiter cette confiance et cet anonymat afin de camoufler leurs activités.

Les responsables informatiques des entreprises doivent utiliser des méthodologies complètes d'inspection SSL / TLS pour atténuer les risques cachés derrière le trafic crypté. Ce livre blanc examine le risque que représentent les menaces cryptées; considère les implications pour l'entreprise, la vie privée et la sécurité de la gestion de ce risque; et présente des mesures constructives pour équilibrer les besoins de sécurité avec le droit à la vie privée des employés. Au final, le meilleur moyen pour les responsables informatiques de garantir les droits de chaque employé consiste à protéger l'entreprise contre les menaces et les attaques.

Par le passé, Internet était beaucoup plus simple — un terrain de jeu ouvert pour une élite experte en technologie...

De nos jours, il est devenu la plate-forme où convergent la vie normale et la plupart des affaires modernes complexes. Avec cette omniprésence, arrive un nouveau risque. De par sa nature même, un « Internet pour tous » inclut un refuge pour les personnes malveillantes déterminées à tirer profit de ceux parmi nous qui l'utilisent pour faire des affaires et mener leur activité quotidienne.

Les données personnelles doivent être protégées, en particulier lorsqu'elles sont en transit. Le chiffrement est la meilleure façon d'y parvenir. Les données cryptées avec les protocoles de sécurisation standard SSL / TLS ne peuvent pratiquement pas être décodées par une personne malveillante qui les intercepte. (Voir Figure 1 et se référer à l'encadré « Transport Layer Security [TLS] and Secure Sockets Layer [SSL] ».) Le chiffrement aide également à établir la confiance et à préserver l'anonymat. C'est cette combinaison de fonctionnalités qui rend idéal le chiffrement SSL / TLS pour protéger la communication sur Internet, de la simple navigation aux achats en ligne.

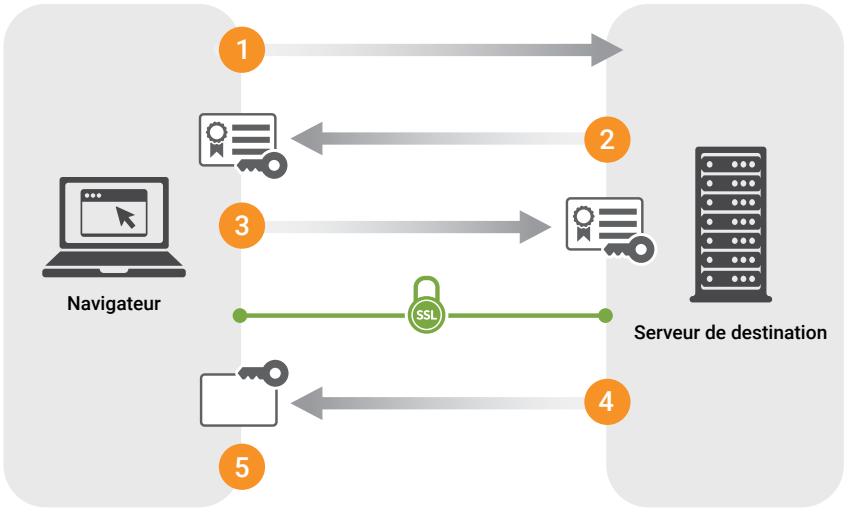
Dans les environnements professionnels de nos jours, il est primordial de protéger les ressources de l'entreprise *et* de préserver la vie privée des individus. Le chiffrement SSL / TLS sert ces deux missions apparemment opposées. Mais dans de mauvaises mains, les technologies SSL / TLS peuvent être extrêmement dangereuses. Que se passe-t-il lorsque des personnes malveillantes l'utilisent pour crypter des logiciels malveillants et masquer leurs activités? Comment les entreprises modernes peuvent-elles combattre cette menace?

De l'ouvert au sécurisé: comment le chiffrement SSL / TLS rend possible la protection en ligne

Internet a évolué. Par le passé, la navigation — que ce soit vers Yahoo, Google, Microsoft ou le site Web de votre université locale — n'exigeait aucune confidentialité ou protection. Saisir l'URL dans la barre d'adresse du navigateur vous menait directement au site, sans cookies ni détours, et avec peu voire aucune donnée potentiellement exploitable partagée sur le trajet. De nos jours, il est devenu courant de partager à la fois des informations personnelles et privées et de mener des affaires sur le même réseau. Nous *vivons* sur Internet. Même nos habitudes de navigation en elles-même sont devenues de précieuses données. Ce changement exige un moyen plus privé et sécurisé de s'engager dans les services Web.

Entrez dans la technologie du chiffrement. Le chiffrement Secure Sockets Layer (SSL) (et son successeur Transport Layer Security, ou TLS) établit *des tunnels sécurisés* entre un navigateur et un site de destination en utilisant des certificats de « clé publique » validés par des tiers. Ces certificats, de même que les relations qu'ils établissent, créent un ensemble de *chaînes de confiance* : « Je vous fais confiance parce que quelqu'un à qui je fais confiance vous fait confiance. » Lorsqu'une entreprise achète un tel certificat auprès d'un fournisseur de confiance reconnu par son navigateur (par exemple: Verisign, Thawte), cette entreprise devient un membre de confiance de cette chaîne. Lorsque vous naviguez sur un site protégé par SSL / TLS, votre navigateur et le site Web échangent des références (le certificat) et des paramètres de manière à ce que la communication subséquente soit cryptée. Cette communication, même si elle devait être interceptée, est incompréhensible pour quiconque, à l'exception du navigateur et du serveur de site Web. Les protocoles SSL et TLS fournissent cette capacité de chiffrement depuis plusieurs décennies.

Comment SSL / TLS fonctionne dans une connexion navigateur - serveur



1. Un utilisateur ouvre un navigateur et envoie une demande HTTPS.
2. Le serveur de destination renvoie une clé publique chiffrée en même temps qu'un certificat SSL / TLS.
3. Le client du navigateur valide le certificat, crée et renvoie au serveur de destination une clé chiffrée. (Si le certificat du serveur n'est pas validé, la communication prend fin.)
4. Le serveur de destination déchiffre la clé reçue et fournit au client le contenu (et la clé) chiffrés.
5. Le client déchiffre le contenu.

Figure 1. Comment SSL / TLS fonctionne dans une connexion du navigateur au serveur de destination.

SSL / TLS offre trois fonctionnalités importantes pour la navigation sur le Web :

Confidentialité

Les données contenues dans le tunnel sécurisé ne peuvent être vues ou partagées avec un tiers.

Confiance

Il y a validation que le navigateur est bien en relation avec le serveur / site web souhaité.

Anonymat

Les habitudes de navigation de l'utilisateur sont cachées à toutes les parties situées entre l'utilisateur et le serveur.

Transport Layer Security (TLS) et Secure Sockets Layer (SSL)[1] sont des protocoles de réseau destinés à créer un tunnel sécurisé entre deux appareils en se servant de la cryptographie. Cela assure des communications sécurisées sur ce qui autrement serait un réseau informatique public. SSL / TLS protège les données grâce aux méthodes de cryptographie qui utilisent à la fois des clés publiques et privées pour le chiffrement et le déchiffrement, et s'appuie sur les certificats pour authentifier les parties communicantes.

1 https://en.wikipedia.org/wiki/Transport_Layer_Security

L'anonymat protège les informations sur le navigateur et la personne derrière celui-ci, mais pas les adresses IP du navigateur et du serveur. Cette lacune a été comblée avec l'avènement de l'anonymisation des proxies[2] et des réseaux d'anonymat comme TOR.[3]

Premier risque lié au chiffrement: les personnes malveillantes exploitent la confiance

Le chiffrement SSL / TLS offre l'assurance de la confidentialité: personne entre votre navigateur et votre destination ne sait ce que vous consultez, ni quelles données vous partagez. Mais, rappelez-vous la chaîne de confiance — les personnes malveillantes cherchent à exploiter la confiance (Voir Figure 1), et elles ont rendu la confiance inhérente à SSL / TLS encore plus importante que les capacités de confidentialité et d'anonymat du tunnel.

Figure 2. Exemples de la manière dont les personnes malveillantes exploitent la confiance via des diffusions cryptées SSL / TLS.

Par exemple, une simple recherche sur Internet pourrait ne pas nécessiter un chiffrement, mais Google le fait de toute façon. Bien que les données ne soient pas forcément sensibles, la *certitude* de savoir que c'est Google qui sert la page fournit cet élément essentiel de confiance. Ce même chiffrement dans la chaîne de confiance fournit cette validation. Comme la plupart des sites Web modernes, Google actuellement sert toutes ses pages via SSL / TLS avec des URL « HTTPS ». L'ère de la navigation à texte ouvert « en

https://en.wikipedia.org/wiki/Anonymizer

https://en.wikipedia.org/wiki/Tor_(anonymity_network)

clair » touche à sa fin. (Chez Zscaler, nous sommes dans une position unique qui nous permet d'observer les tendances du trafic Internet, et plus de 83% du trafic de données transitant par Zscaler est maintenant chiffré via SSL / TLS.[4])

Le modèle de tunnel sécurisé est, de par sa conception, sécurisé. Mais il reste exploitable, particulièrement en ce qui concerne la confiance de l'utilisateur. Chaque organisation (et même une personne) peut acheter un certificat SSL / TLS. Cette organisation peut utiliser ce certificat pour coopter ou reproduire des destinations Internet légitimes (ou même des composants d'une page Web légitime), compromettant efficacement un site ayant un certificat légitime. De cette façon, les personnes malveillantes trompent l'utilisateur derrière son ordinateur, et accèdent à ses importantes données qu'elles peuvent décoder, *même si ces données sont chiffrées en transit.* Les personnes malveillantes se présentent comme une entité digne de confiance. Étant donné que le trafic est crypté, leur collecte de données n'est pas détectée, et elles contournent les contrôles ou outils mis en place par l'entreprise pour les stopper.

Deuxième risque lié au chiffrement: les personnes malveillantes dissimulent des programmes malveillants

La recrudescence des attaques par hameçonnage, usurpation d'identité, et ransomware a érodé la confiance dans l'Internet: comment savoir si je consulte un site légitime? Comment savoir si quelque chose sur le site (annonce, article, élément) n'est pas compromis? Comment savoir si ce site apparemment légitime ne contient pas de programme malveillant crypté?

Les personnes malveillantes compromettent souvent (ou usurpent l'identité) des fournisseurs tiers tels que Content Delivery Networks (CDN) qui fournissent du contenu à des sites légitimes, diffusant ainsi des programmes malveillants sur un site légitime qui, à toutes fins pratiques, est pourtant « sécurisé » par HTTPS.

Les personnes malveillantes utilisent le chiffrement SSL / TLS pour masquer leur activité, et la menace qu'elles représentent s'aggrave progressivement. Ceci n'est pas une nouvelle menace. Ces personnes malveillantes ont toujours eu l'opportunité de dissimuler des logiciels malveillants dans un code sécurisé. C'est l'économie qui a changé. Au cours des dernières années, des certificats SSL / TLS *gratuits* sont devenus facilement disponibles, réduisant considérablement le coût et l'effort liés au chiffrement de logiciels malveillants.

Chez Zscaler, nous avons vu au cours des dernières années le volume de menaces véhiculées par les tunnels cryptés augmenter de façon exponentielle. Plus de 54% de menaces avancées détectées sont désormais diffusées via des canaux cryptés SSL / TLS.[5] Plus inquiétant encore, en 2018 les attaques par hameçonnage cryptées avec SSL / TLS ont augmenté de 300%.[6]

---

https://www.zscaler.com/threatlabz/encrypted-traffic-dashboard

https://www.zscaler.com/resources/solution-briefs/add-advanced-threat-protection-to-close-your-security-gaps.pdf

https://www.zscaler.com/blogs/research/february-2018-zscaler-ssl-threat-report

Les cybercriminels utilisent les mêmes protocoles SSL / TLS pour crypter la source de leurs logiciels malveillants (par exemple, un « drive-by », site crypté spécialement conçu pour héberger des programmes malveillants) et le flux sortant de communications qui en découle. Ce chiffrement présente l'illusion de données « fiables », donnant aux personnes malveillantes un laissez-passer gratuit pour infiltrer les entreprises, accéder aux ressources et masquer une exfiltration de données.

Troisième risque lié au chiffrement: les personnes malveillantes masquent l'exfiltration de données

Si une personne malveillante extérieure parvient à s'infiltrer dans un réseau d'entreprise avec l'intention de voler des ressources numériques, elle doit relever le défi consistant à obtenir des données en dehors du périmètre de sécurité de l'entreprise. Le même problème se pose lorsqu'il s'agit d'un acteur interne: comment obtenir des informations protégées en dehors de l'organisation?

Les cybercriminels cachent des programmes malveillants dans le flux entrant de données cryptées. Dans certains cas, ce programme malveillant explose à l'intérieur d'une organisation, infectant les systèmes internes, puis contacte des serveurs de commande et de contrôle externes (C & C) afin d'exfiltrer de précieuses données d'entreprise en dehors de l'organisation.

Le chiffrement peut masquer une malicieuse perte de données et même les occasionnelles et accidentelles pertes. En l'absence d'une inspection SSL / TLS de flux sortant, comment un responsable informatique peut-il déterminer si les données confidentielles le demeurent? L'inspection SSL / TLS doit traiter à la fois le trafic de données entrant (bloquer l'accès aux personnes malveillantes) et sortant (empêcher la fuite d'informations confidentielles). Dans le cas du flux sortant, l'inspection SSL est essentielle pour prévenir la perte de données et pour identifier et corriger les vulnérabilités d'exfiltration de données en cas d'attaque zero-day.[7]

---

https://searchsecurity.techtarget.com/definition/zero-day-vulnerability

Équilibrer l'accès et la sécurité dans une nouvelle ère de confidentialité

L'évolution de la connectivité Internet annonce une ère nouvelle en matière de confidentialité — du texte clair à la transmission de données chiffrées, de la confiance implicite à la confiance explicite. Cela se voit non seulement à la demande des consommateurs en matière de gestion des données privées, mais aussi dans les lignes directrices réglementaires définissant le droit à la vie privée de l'utilisateur, telles que le Règlement général sur la protection des données (RGPD) de l'Union européenne[8], la Loi du Canada sur la Protection des renseignements personnels et les documents électroniques[9], et plusieurs lois existantes (Californie, Maine, Nevada) et proposées (Hawaii, Illinois, Massachusetts, Mississippi, Nouveau-Mexique, New York, Rhode Island, Texas et Washington) des États américains sur la protection de la vie privée.

Toute navigation ou trafic Internet ne sont pas égaux. Dans la plupart des cas, la protection de la vie privée est une affaire personnelle. Un utilisateur occasionnel dans un état démocratique est susceptible de naviguer en privé, alors qu'un internaute dans une localité soumise à un régime autoritaire pourrait utiliser un réseau anonyme comme Tor pour protéger les communications de la visibilité de la censure afin de communiquer avec sa famille à l'étranger. Dans chacun des cas, les données sont celles de l'utilisateur, et peu sont ceux — sauf exception éventuelle de ce gouvernement autoritaire — qui s'opposeraient à la protection du droit à la vie privée de chaque utilisateur. Les deux utilisateurs assument le risque d'une perte ou d'une interception de données, un risque qui est limité à leurs propres domiciles et appareils.

C'est une toute autre histoire au sein d'une entreprise ou avec une connexion Internet fournie par le gouvernement. La plupart seront d'avis que les utilisateurs d'entreprises devraient bénéficier d'un certain droit à la vie privée sur Internet — il y a peu de raisons justifiant le fait que les habitudes d'achat d'un utilisateur, ses choix de destination de vacances, ses passe-temps, ou les sites Web qu'il visite soient visibles aux collègues. Les diverses lois régissant la vie privée dans de nombreux cas vont dans ce sens. SSL / TLS a rendu possible cette confidentialité, et même la navigation anonyme, pendant des années.

Toutefois, cette confidentialité escomptée entraîne des coûts et des risques: pouvons-nous continuer à jouir de celle-ci si des personnes malveillantes peuvent aussi l'exploiter à leur avantage ? Dans un contexte d'entreprise, le risque ne concerne plus uniquement un employé, mais l'ensemble de l'entreprise. Dans le contexte des capacités de la technologie de chiffrement, les responsables informatiques des entreprises modernes doivent peser le risque de menaces entrantes avec la promesse de confidentialité — un délicat jeu d'équilibriste entre les droits de chaque employé et le devoir de l'entreprise de se protéger.

---

https://eugdpr.org/

https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

Dans une organisation, l'idée d'un droit à la vie privée absolue est moins claire. Toute entreprise connectée — et avouons-le, c'est le cas de toutes les entreprises — a la responsabilité envers ses employés, ses actionnaires et ses clients de se protéger et d'adhérer aux directives juridiques et réglementaires. Les responsables informatiques ont recours à des contrôles techniques et procéduraux pour prévenir et détecter les attaques et les comportements à risque. Pour réduire les risques et protéger l'organisation, ces contrôles doivent être appliqués à tout le trafic de données interne entrant et sortant.

L'environnement réglementaire peut rendre plus complexe la gestion des données d'entreprise. Certaines juridictions européennes exigent des sociétés qu'elles protègent les données personnelles de leurs employés pour en assurer la confidentialité et, dans certains cas, l'anonymat de la navigation personnelle. Par exemple en Allemagne: "Das Telekommunikationsgesetz"[10] (la « Loi sur les télécommunications », ou TKG) est généralement considérée comme s'appliquant aux sociétés fournissant aux employés un accès à Internet pour leur usage personnel. La TKG exige expressément des utilisateurs qu'ils se soumettent au « secret des télécommunications ». Elle exige également qu'une organisation protège convenablement le service des dommages et/ou interceptions, ET protège correctement les données de navigation des utilisateurs. Les entreprises qui se conforment à la TKG doivent concilier le « secret des télécommunications » des utilisateurs et la protection des actifs.

Selon un récent Rapport de transparence de Google,[11] jusqu'à 93% du trafic du navigateur Chrome est crypté. Avec des personnes malveillantes qui présentent des menaces avancées via des canaux cryptés pour échapper aux contrôles de sécurité de l'entreprise, comment une société peut-elle à la fois se protéger et protéger ses données, tout en préservant les droits des employés à la confidentialité, dans le respect des réglementations relatives à la protection des données?

Ouverture du tunnel — déchiffrement et inspection SSL / TLS

Dans une entreprise, un logiciel malveillant ne se limite pas uniquement à un individu. Une fois qu'un hacker accède à la machine d'un employé, cet intrus peut généralement se déplacer ailleurs (« Est / Ouest[12]») dans le domaine de cet employé, et infecter d'autres systèmes et ordinateurs au sein du réseau d'entreprise.

Les contrôles de cybersécurité peuvent facilement inspecter les communications à texte ouvert entrant ou sortant d'une entreprise, mais le chiffrement SSL / TLS des données entrantes ou sortantes complique

---

https://germanlawarchive.iuscomp.org/?p=692

https://transparencyreport.google.com/https/overview?hl=en

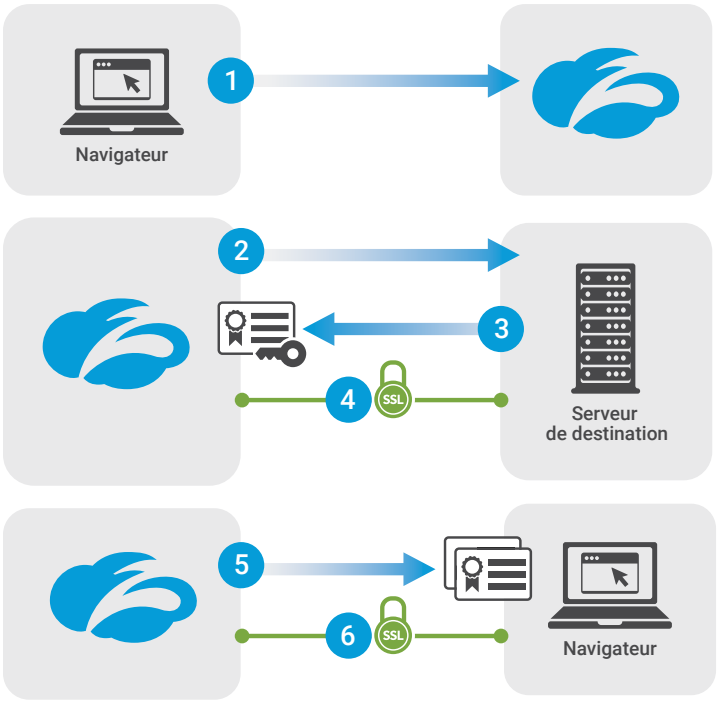
https://searchnetworking.techtarget.com/definition/east-west-traffic

l'inspection. La confidentialité présumée d'un tunnel sécurisé peut-elle être préservée si les menaces cryptées présentent un tel danger à la fois pour l'utilisateur individuel *et* pour l'entreprise plus étendue?

La réponse est OUI. La lutte contre le risque de menaces cryptées destructrices commence par l'inspection des données SSL / TLS. Une entreprise a l'obligation institutionnelle et légale de protéger ses actifs, ce qui inclut la protection des communications de ses employés.

Pour inspecter les données SSL / TLS, l'organisation doit efficacement dévier cette chaîne de confiance de communication, l'interrompant avec un tunnel entre le navigateur et le dispositif d'inspection, puis un tunnel subséquent entre le dispositif d'inspection et la destination.

Comment Zscaler inspecte les données cryptées SSL / TLS — fonctionnement



1. Un utilisateur ouvre un navigateur et envoie une demande HTTPS.
2. Le service Zscaler intercepte la demande HTTPS. Grâce à un tunnel SSL différent, le service envoie sa propre requête HTTPS au serveur de destination et mène les négociations SSL.
3. Le serveur de destination envoie au service Zscaler son certificat avec sa clé publique.
4. Le service Zscaler et le serveur de destination terminent la négociation SSL. Les données d'application et les messages suivants sont envoyés via le tunnel SSL.
5. Le service Zscaler conduit les négociations SSL avec le navigateur de l'utilisateur. Il envoie au navigateur le certificat intermédiaire Zscaler ou la racine intermédiaire personnalisée de votre organisation ainsi qu'un certificat de serveur signé par l'autorité de certification intermédiaire Zscaler. Le navigateur valide la chaîne de certificats dans la liste de certificats du navigateur.
6. Le service Zscaler et le navigateur terminent la négociation SSL. Les données d'application et les messages suivants sont envoyés via le tunnel SSL.

Une fois la négociation terminée, le moteur de politique Zscaler évalue les règles de politique SSL / TLS, applique les blocages / contournements généraux, vérifie les certificats des émetteurs non fiables et affiche les notifications (le cas échéant).

Figure 3. Processus par lequel Zscaler inspecte les données cryptées SSL / TLS.[13]

Dans cet exemple, l'inspection ne brise pas la relation de confiance entre l'individu et la source. L'employé fait confiance à l'organisation qui fournit le dispositif de navigation plutôt qu'à la source de données. Le dispositif d'inspection « verra » la destination et le contenu des données.

13 https://help.zscaler.com/zia/about-ssl-inspection

La question demeure donc: *une organisation peut-elle assurer cette essentielle fonction protectrice tout en respectant les deux autres caractéristiques du chiffrement, l'anonymat et la confidentialité?* Fait correctement, absolument. La menace posée par le logiciel malveillant crypté fait de l'inspection SSL / TLS un mandat de contrôle de la cybersécurité pour l'entreprise moderne, et les organisations doivent équilibrer leurs besoins en matière de sécurité avec les droits de leurs employés à la vie privée. Une organisation qui n'inspecte pas le trafic SSL / TLS s'expose à d'inutiles risques, notamment la perte d'informations personnelles identifiables, le vol de propriété intellectuelle, l'espionnage industriel ou même les infections de ransomware. (Le pourcentage d'organisations inspectant des données cryptées a augmenté: parmi les entreprises clientes de Zscaler — dont près de la moitié sont basées en Europe — 72% inspectent le trafic SSL/TLS.)

Dans une entreprise, l'anonymat individuel en ligne peut être préservé... dans une certaine mesure

Lors de l'évaluation des modèles d'inspection SSL / TLS, nous devons d'abord examiner l'anonymat. Dans certaines organisations, la fourniture d'accès à Internet est un droit accordé et régi par un contrat avec l'employé, établi et contrôlé par une politique de la même manière que le comportement de l'employé sur le lieu de travail est régi par une politique.

L'application de cette politique exige un suivi. Un tunnel SSL / TLS expose déjà sa source et sa destination à tout et à n'importe qui, entre le navigateur et le serveur. L'enregistrement de ces transactions est essentiel pour l'analyse comportementale et la détection des incidents. L'examen des journaux peut aider à assurer le respect des politiques et contribuer à l'amélioration continue de leur efficacité. (L'analyse rétrospective des journaux est même souvent utilisée dans les enquêtes criminelles.)

Avec un protocole d'inspection SSL / TLS installé sur le lieu de travail, les employés ne devraient pas s'attendre à l'anonymat complet pendant leur navigation en ligne, dans la mesure où l'accès à Internet est un privilège accordé à ses employés par l'organisation et régi par le contrat de travail de chaque employé. Pour protéger les actifs de l'entreprise, l'organisation peut choisir de suivre les URL de destination d'un utilisateur, son comportement de navigation et son accès aux appareils. La politique d'entreprise d'une organisation établit des barrières de sécurité pour cette utilisation d'Internet, ainsi que des retombées en cas de violation de cette politique.

Pour être clair, l'inspection SSL / TLS ne signifie pas la fin de l'anonymat individuel en ligne. Les entreprises peuvent équilibrer les exigences de confidentialité des employés avec des mesures de cybersécurité à jour. Une surveillance complète des données est requise pour une inspection SSL / TLS efficace, mais l'accès aux données résultant de cette inspection peut être limité. Les employés peuvent rester anonymes tout au long de l'analyse des journaux, même pendant les enquêtes et le verdict (par exemple, l'examen et la réaction aux

violations potentielles de la politique) jusqu'à ce qu'il soit nécessaire de s'engager. Cette anonymisation est généralement désignée comme indexation des journaux ou obfuscation.

Parfois, les responsables informatiques doivent inspecter et analyser les journaux en entier. Par exemple, un responsable de la cybersécurité examinera régulièrement les journaux pour identifier les rappels de logiciel malveillant via le tunnel SSL / TLS. Lorsqu'il en trouve un, la sécurité informatique doit déclencher un flux de travail de nettoyage de la machine, en s'engageant avec l'employé à éliminer le logiciel malveillant de l'appareil infecté (ou même le reformater ou alors le détruire). Ce processus peut être mis en œuvre pour soutenir une approche à « quatre yeux[14] », avec à la fois un administrateur de la sécurité et un représentant des travailleurs (par exemple, un dirigeant d'une association d'employés, ou peut-être un avocat extérieur) qui examineront les journaux de la console en même temps.

Lorsque les journaux identifient une infection, un utilisateur d'entreprise individuel ne peut garder l'anonymat, et doit être « désobfusqué » pour révéler son identité afin que la sécurité informatique puisse remédier à la menace avant qu'elle n'affecte pas l'organisation dans son ensemble.

L'exfiltration des données — la « fuite » indésirable des données d'une organisation — représente une autre situation pouvant exiger une désobfuscation. En règle générale, un processus d'examen des journaux peut déterminer que le trafic SSL / TLS précédent, non filtré, peut en fait être destiné à un site Web de destination criminelle ou non agréée. Dans ce cas, des forces de l'ordre pourraient être engagées, et les données désobfusquées pour appuyer l'enquête.

Les employés doivent s'attendre à ce que la navigation soit anonyme pour les pairs de l'entreprise, la direction, et même les équipes de sécurité de l'entreprise... jusqu'à ce qu'un risque ou une menace pour les organisations entraîne la nécessité de supprimer cet anonymat. Dans les situations susmentionnées, il est essentiel que l'organisation ait un *besoin justifié* de désobfusquer au moyen d'une politique d'utilisation acceptable (PUA) qui serait souvent intégrée au contrat de travail de l'employé. L'utilisation d'Internet par l'intermédiaire de dispositifs ou de réseaux d'entreprise ne devrait être autorisée que si l'employé y consent (généralement au début de l'emploi).

Sécurisation des données: déchiffrement SSL / TLS dans un environnement régi par le RGPD

Au premier abord, « ouvrir » le tunnel de communication chiffré SSL / TLS pour l'inspection des données et l'application des politiques semble faire en sorte que les données ne soient plus privées. Il s'agit d'une préoccupation commune soulevée par les services juridiques des entreprises et les défenseurs de la vie

[14] https://whatis.techtarget.com/definition/four-eyes-principle

privée. Certains pointent le RGPD comme base pour soutenir que le RGPD interdit à une organisation de décrypter et d'inspecter les données personnelles cryptées via SSL / TLS. À notre avis, c'est incorrect.

Même les sessions normales et non cryptées exigeront que les mêmes obligations soient appliquées à toutes les parties (ISP, fournisseurs de réseau, proxy de mise en cache) entre le navigateur et le serveur. Les directives RGPD exigent *toujours* que chaque partie traite les données personnelles avec le même degré de sensibilité. Le chiffrement ne modifie pas les obligations imposées à un responsable du traitement des données, ou même à un sous-traitant. Pour réduire davantage l'argument erroné, les données personnelles sont traitées par l'appareil fourni par l'entreprise de l'employé d'une manière non cryptée, *même en utilisant un tunnel crypté.* Il ne peut y avoir aucune garantie absolue de confidentialité dans ce contexte d'entreprise.

L'inspection SSL / TLS est utilisée pour appliquer la politique et identifier les potentielles menaces cachées dans le trafic de données cryptées. Afin d'identifier les menaces, un dispositif d'inspection décrypte les données, les compare à un ensemble de signatures « de mauvaise réputation », et inspecte le flux de données pour déterminer les risques de menace tels que les logiciels malveillants entrants ou des données d'entreprise qui sortent de façon inappropriée. Au cas où les données ne présentent aucune menace, elles sont reconditionnées et acheminées. Réalisée de cette manière, l'inspection SSL / TLS ne porte pas atteinte à la vie privée des employés. Les données ne sont ni partagées avec des tiers, ni utilisées de manière à enfreindre les droits de la personne concernée. Le processus d'inspection SSL / TLS protège les ressources d'une organisation des menaces d'attaques, sans empiéter sur les droits individuels à la vie privée.

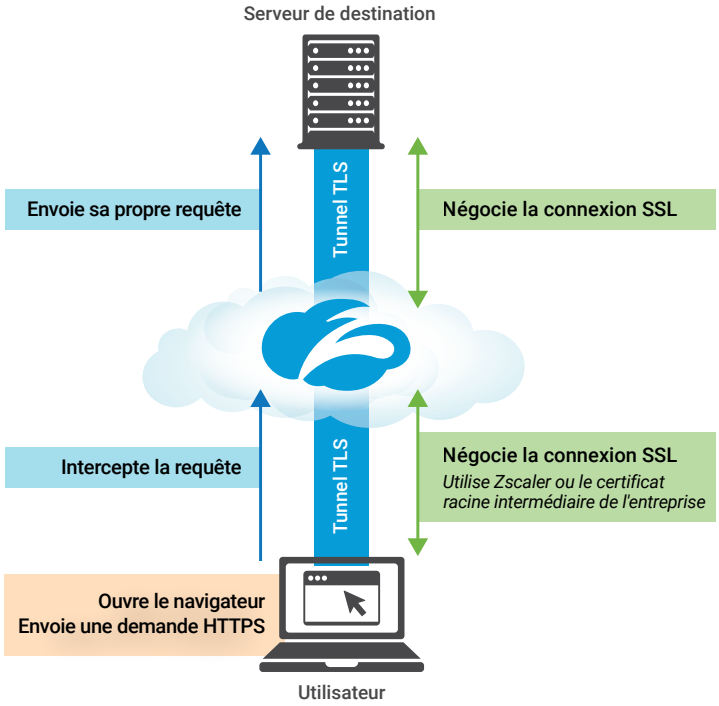
Zscaler offre des capacités complètes d'inspection SSL / TLS pour protéger le trafic de données des clients et offrir une « parfaite confidentialité persistante » (perfect forward secrecy ou PFS).[15]Zscaler ne stocke jamais les données sur le disque: une fois l'inspection des données achevée, le flux de données continue sans entraves, et aucun enregistrement des données sources n'est conservé au-delà du journal de transaction. En plus de protéger les données en transit, Zscaler protège toutes les clés SSL / TLS pendant l'inspection. Reportez-vous aux Figures 3 et 4 pour savoir comment Zscaler inspecte les données chiffrées SSL / TLS. Pour en savoir plus sur la façon dont Zscaler sécurise toutes les données et toutes les clés de chiffrement cliquez ici.[16])

---

https://www.zscaler.com/blogs/corporate/tls-13-busting-myths-and-debunking-fear-uncertainty-doubt

https://help.zscaler.com/zia/safeguarding-ssl-keys-and-data-collected-during-ssl-inspection

Comment Zscaler inspecte les données cryptées SSL / TLS — fonctionnement



Zscaler sert de proxy SSL inline. Il met fin à la connexion SSL établie par le client et établit une nouvelle connexion SSL au serveur. Du point de vue d'un client, Zscaler devient le serveur et du point de vue du serveur SSL d'origine, Zscaler devient le client.

Inspection Zscaler SSL / TLS basée sur le cloud:

- Évolue pour inspecter tout le trafic
- Rationalise la gestion des certificats
- Simplifie l'administration du réseau
- Sécurise le trafic avec les chiffrements AES/GCM/ECDHE pour PFS
- Applique des contrôles efficaces de politique
- Conserve en sécurité les données de l'utilisateur (puisqu'elles restent éphémères, jamais stockées dans le cloud)

Figure 4. Modèle de proxy inline pour savoir comment Zscaler inspecte les données chiffrées SSL / TLS.[17]

Il est utile de considérer le droit à la vie privée comme un résultat et d'examiner la façon dont le résultat est atteint, plutôt que de désamorcer les étapes individuelles qui semblent avoir une incidence sur ce résultat. L'inspection du trafic et le résultat binaire du blocage ou non du blocage, n'est pas la même chose que l'accès, la surveillance ou le stockage des données cryptées.

Une inspection SSL / TLS complète renforce la conformité au RGPD d'une entreprise et la conformité globale à la confidentialité, car elle contribue à protéger la confidentialité de l'organisation, de ses employés, et de ses actifs. Sans inspection SSL / TLS, le risque d'exposer des données personnelles internes / IPI est plus élevé, exposant alors l'organisation à un grand risque de non-conformité.

[17] https://help.zscaler.com/zia/about-ssl-inspection

Les règlements sur la protection des données appuient la protection de la vie privée *et la* sécurité

Les réglementations sur la confidentialité des données — en particulier les législations européennes comme le RGPD,[18]le règlement 2018 du Royaume-Uni sur les réseaux et les systèmes d'information (NIS)[19], et le règlement TKG[20]— ont été mises en place pour s'assurer que les organisations protègent les données personnelles tout en préservant un accès libre et équitable à Internet. Ces réglementations établissent un équilibre entre les droits des particuliers et les exigences selon lesquelles les sociétés doivent mettre en œuvre des mesures de sécurité pour protéger les systèmes et les données. Par exemple, le règlement TKG exige que les organisations appliquent des « précautions techniques de protection[21] » pour éviter la perte de données et repousser les attaques externes. Le NIS stipule explicitement qu'une organisation doit mettre en place des mesures de sécurité appropriées pour s'assurer que les systèmes (et les données qu'ils contiennent) ne peuvent être compromis. Et l'article 5 du RGPD[22] stipule que ces organisations doivent traiter les données

> *... d'une manière qui garantit une sécurité appropriée des données personnelles, y compris la protection contre le traitement non autorisé ou illicite, et contre toute perte, destruction ou détérioration accidentelle, au moyen de mesures techniques ou organisationnelles appropriées.*

De plus, l'article 32 du RGPD (Sécurité du traitement) impose aux organisations une obligation positive de mettre en œuvre des mesures de sécurité pour le traitement des données personnelles qui « assurent un niveau de sécurité proportionnel au risque. » Les inspections SSL / TLS sont très « appropriées », compte tenu de l'ampleur des risques de sécurité qu'elles visent à atténuer.

Les menaces se cachent dans le trafic crypté. Sans inspection, il n'existe aucun moyen pour les entreprises de distinguer les « bonnes » données cryptées SSL / TLS des « mauvaises ». Aucune entreprise ne peut à la fois remplir les obligations de confidentialité et de sécurité du TKG, du NIS et du RGPD — encore moins protéger ses employés et les intérêts de l'entreprise — sans une inspection complète du trafic de données chiffrées.

---

https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-gdpr/

http://www.legislation.gov.uk/uksi/2018/506/contents

https://germanlawarchive.iuscomp.org/?p=692

https://germanlawarchive.iuscomp.org/?p=692

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679#d1e1807-1-1

Points à retenir: comment implémenter l'inspection SSL / TLS dans votre entreprise

Les justifications de sécurité et de protection des données pour l'inspection SSL / TLS au sein de l'entreprise sont judicieuses et irréprochables. Les responsables informatiques doivent recourir à l'inspection SSL / TLS pour protéger les données et les actifs de leur organisation, ainsi que les employés. Une défaillance dans ce domaine pourrait causer des dommages irréparables et même constituer un manquement au devoir.

Les responsables informatiques qui veulent introduire l'inspection SSL / TLS au sein de leur organisation doivent prendre en compte plusieurs considérations importantes:

1. **Informer les employés.**
   - S'assurer qu'une Stratégie d'utilisation acceptable valide est en place et que ses politiques sont appliquées au niveau du filtre proxy / contenu.
   - S'assurer que la Stratégie d'utilisation acceptable est explicitement acceptée par tous les employés, généralement par le biais de leur contrat de travail.
   - S'assurer que les employés sont bien au courant de ce que constituent les données personnelles et pour combien de temps celles-ci sont conservées par l'organisation.
   - S'assurer que les employés sont clairement informés des données à inspecter de façon à ce qu'ils prennent des décisions éclairées quant à leur utilisation des ressources de l'entreprise.
   - Obtenir l'accord et le soutien des conseils de travailleurs et/ou des syndicats, démontrant que l'inspection SSL / TLS en fait profite aussi aux employés.
   - Socialiser ce qui est fait, ainsi que la façon de le faire.

2. **Choisir une base légale pour le traitement des données en accord avec le RGPD.** La réglementation n'est pas l'ennemie ici — si une entreprise est assujettie au NIS ou à un système similaire, la base légale est l'« obligation légale ». Et comme nous l'avons mentionné précédemment, une entreprise a un « intérêt légitime » à protéger l'organisation et ses actifs.

3. **Obtenir des conseils juridiques et en matière de protection de la vie privée auprès d'une équipe interne ou d'experts externes, mais être prêt à discuter de certains points.** Par exemple, certains avocats et professionnels de la protection de la vie privée peuvent ne pas bien comprendre les services proposés par les fournisseurs ni avoir le point de vue technique nécessaire pour juger si les mesures de sécurité sont appropriées au risque.

4. **S'assurer que les processus et les contrôles sont efficaces et appropriés.**
    - Obfusquer ou alors masquer les données des utilisateurs réguliers; s'assurer qu'elles ne sont disponibles que de manière sélective.
    - S'assurer qu'il existe un processus rigoureux et documenté d'examen des données personnelles.
    - Examiner et mettre en application ce flux de travail sur une base régulière.
    - Conserver les données pour la période déterminée, puis les supprimer par la suite.
    - Protéger les données pendant que l'entreprise les possède.

L'inspection SSL / TLS: la bonne façon d'assurer la conformité réglementaire

L'inspection SSL / TLS représente les « mesures de sécurité appropriées » pour protéger la confidentialité de l'entreprise, de ses actifs et même des employés. L'inspection SSL / TLS protège l'organisation des menaces d'attaques tout en équilibrant les droits individuels à la vie privée, renforçant de cette manière la conformité réglementaire de ces organisations.

Les menaces chiffrées sont tangibles, destructrices, virulentes et croissent (de façon exponentielle) en volume. Les responsables informatiques d'entreprise qui choisissent de ne pas déchiffrer le trafic mettent en danger à la fois la vie privée de leurs utilisateurs et les actifs de leur entreprise, tout en courant le risque d'être non conforme aux diverses réglementations relatives à la protection des données. En cette ère moderne, les responsables informatiques doivent utiliser l'inspection SSL / TLS pour combattre les risques de sécurité pour l'entreprise et préserver la vie privée de leurs employés et utilisateurs.

À propos de Zscaler

Zscaler a été fondé en 2008 sur un concept simple mais puissant: à mesure que les applications migrent vers le cloud, la sécurité doit également s'y déplacer. Aujourd'hui, nous aidons des milliers d'organisations mondiales à se porter vers des opérations basées sur le cloud.