Pratiques exemplaires en matière de déchiffrement

Version 10.0 (EoL)

techDOCS paloalto NETWORKS

Contact Information

Corporate Headquarters:
Palo Alto Networks
3000 Tannery Way
Santa Clara, CA 95054
www.paloaltonetworks.com/company/contact-support

About the Documentation

- To ensure you are viewing the most current version of this document, or to access related documentation, visit the Technical Documentation portal: docs.paloaltonetworks.com.
- To search for a specific topic, go to our search page: docs.paloaltonetworks.com/search.html.
- Have feedback or questions for us? Leave a comment on any page in the portal, or write to us at documentation@paloaltonetworks.com.

Copyright

Last Revised

October 28, 2020

Table of Contents

Pratiques exemplaires en matière de déchiffrement

Vous ne pouvez pas protéger votre réseau des menaces que vous ne pouvez pas voir ni inspecter. Gartner prédit que, en 2020, plus de 70 % des nouvelles campagnes de logiciels malveillants utiliseront diverses formes de chiffrement. Le rapport Google Transparence montre que, quelle que soit la manière donc vous analysez le trafic Web Google, la plupart du temps, plus de 90 % de ce trafic est chiffré. Déchiffrez ce trafic pour protéger votre réseau contre les menaces cachées.

Ce document se veut une liste de contrôle simplifiée des pratiques exemplaires avant le déploiement, pendant le déploiement et après le déploiement que vous pouvez suivre pour mettre en œuvre le déchiffrement. Chaque section comprend des liens vers des informations détaillées contenues dans le guide de l'administrateur de PAN-OS, y compris les profils et règles de politique de déchiffrement.

- Planifier votre déploiement de déchiffrement SSL exemplaire
- Déployer le déchiffrement SSL au moyen des meilleures pratiques
- Suivre les pratiques exemplaires en matière de déchiffrement SSL après le déploiement

Planifier votre déploiement de déchiffrement SSL exemplaire

Préparez-vous à déployer le déchiffrement en concevant une stratégie de décryptage et un plan de déploiement. L'activation du déchiffrement pourrait modifier la manière dont les utilisateurs interagissent avec certaines applications et avec certains sites Web. Pour assurer la réussite du déploiement, il est donc essentiel de planifier, de tester et d'informer les utilisateurs.

STEP 1 | Fixez des objectifs.

- ❑ Prévoyez de déchiffrer autant de trafic non privé ou non sensible que vous le permettent les ressources de votre pare-feu. Cela permet de réduire la surface d'attaque en révélant et en empêchant les menaces chiffrées. Comprenez les lois et les règlements locaux relatifs au trafic que vous pouvez légalement déchiffrer et les exigences en matière d'envoi d'avis aux utilisateurs.
- ❑ Passez de règles de politique de sécurité basées sur des portes à des règles de politique de sécurité basées sur des applications avant de créer et de déployer des règles de politique de déchiffrement. Si vous créez des règles de décryptage basées sur une politique de sécurité basée sur des ports, puis que vous passez à une politique de sécurité basée sur les applications, le changement pourrait pousser les règles de décryptage à bloquer le trafic que vous cherchez à autoriser, car les règles de politique de sécurité risquent d'utiliser les ports par défaut des applications pour empêcher le trafic d'utiliser des ports non standard. En migrant vers des règles basées sur l'App-ID avant de déployer le décryptage vous permettra, lorsque vous testerez votre déploiement de décryptage, de découvrir les mauvaises configurations de la politique de sécurité et de les régler avant de procéder au déploiement à la population d'utilisateurs générale.

STEP 2 | Travaillez avec les parties prenantes, comme les services juridiques, les finances, les ressources humaines, les cadres supérieurs, la sécurité, les technologies de l'information et le soutien pour développer une stratégie de déploiement du déchiffrement, et informez-les.

- ❑ Obtenez les approbations nécessaires pour déchiffrer le trafic et ainsi sécuriser l'entreprise.
- ❑ Identifiez et hiérarchisez le trafic à déchiffrer :
  - Décidez des applications à déchiffrer (approuvées et non approuvées). N'autorisez pas les applications non approuvées qui sont chiffrées.
  - Décidez des périphériques à déchiffrer (entreprise, BYOD, mobiles, etc.).

    

    Les entreprises ne contrôlent pas les périphériques BYOD. Si vous autorisez les périphériques BYOD sur votre réseau, déchiffrez leur trafic et soumettez-le à la même politique de sécurité que vous appliquez à tout autre trafic sur le réseau. Pour ce faire, redirigez les utilisateurs BYOD via un portail d'authentification, montrez-leur comment télécharger et installer le certificat de l'autorité de certification et informez-les clairement que leur trafic sera déchiffré. Informez les utilisateurs BYOD du processus et incluez-le dans la politique d'utilisation des ordinateurs et dans la politique de confidentialité de votre société.
  - Décidez si vous souhaitez utiliser la même politique de déchiffrement pour différents groupes, comme différents groupes d'employés, d'agents contractuels, de partenaires et d'invités.
- ❑ Identifiez le trafic que vous ne pouvez déchiffrer :
  - Le trafic qui interrompt le déchiffrement pour des raisons techniques, comme l'épinglage de certificats, des suites de chiffrement non prises en charge ou l'authentification mutuelle.
  - Le trafic que vous choisissez de ne pas déchiffrer, comme le trafic relatif aux services financiers, à la santé ou au gouvernement ainsi que les autres catégories sensibles, dont des utilisateurs ou des groupes spécifiques comme les dirigeants.

- Comprenez pleinement le trafic que vous excluez du décryptage. Vous n'avez aucune visibilité du trafic chiffré, et le pare-feu ne peut appliquer des profils de prévention contre les menaces au trafic chiffré.

- ❑ Préparez les politiques relatives à l'utilisation des ordinateurs par les RH et les services juridiques pour les distribuer à tous les employés, sous-traitants, partenaires, invités et les autres utilisateurs du réseau. Ainsi, lorsque vous déployez le déchiffrement, les utilisateurs comprennent que leurs données peuvent être déchiffrées et qu'elles peuvent faire l'objet d'une analyse visant à y déceler des menaces.
- ❑ Décidez comment vous souhaitez gérer la vérification des certificats. Votre modèle d'affaires vous forcera peut-être à faire des compromis entre la sécurité et l'expérience de l'utilisateur. Lorsque vous comprenez comment vous voulez gérer la vérification des certificats, cela vous permet de déterminer la manière dont vous configurez les profils de déchiffrement de proxy de transfert SSL.
- ❑ Identifiez le trafic que vous souhaitez journaliser. Soyez au courant des différences propres aux lois et aux exigences réglementaires locales et de l'incidence qu'elles ont sur le trafic que vous pouvez journaliser et sur l'endroit où stocker les journaux.

Positionnez les pare-feu de manière à ce qu'ils puissent voir tout le trafic du réseau et ainsi veiller à ce qu'aucun trafic non chiffré ne puisse obtenir accès à votre réseau en contournant le pare-feu.

STEP 3 | Concevez un plan de déploiement de votre Public Key Infrastructure (infrastructure à clé publique ; PKI)).

- ❑ Si vous disposez d'une PKI d'entreprise existante, générez le certificat de l'autorité de certification d'approbation de transfert SSL à partir de votre CA racine d'entreprise en tant que certificat subordonné. Cela facilite le déploiement, car les périphériques réseau approuvent déjà la CA racine d'entreprise, vous évitez donc tout problème de certificat. Si vous ne disposez pas d'une CA racine d'entreprise, songez à en obtenir une.

  Vous pouvez également générer un certificat CA racine auto-signé sur le pare-feu et créer un certificat CA d'approbation de transfert subordonnés sur ce pare-feu à installer sur les périphériques réseau. Les certificats auto-signés conviennent mieux aux petites entreprises qui ne possèdent pas de CA racine d'entreprise et pour les essais proof-of-concept (preuve de concept ; POC).

  Tout comme c'est le cas pour les périphériques BYOD, les entreprises ne contrôlent pas les périphériques des invités. Si vous autorisez les périphériques invités sur votre réseau, déchiffrez leur trafic et soumettez-le à la même politique de sécurité que vous appliquez à tout autre trafic sur le réseau. Pour ce faire, redirigez les utilisateurs invités via un portail captif, montrez-leur comment télécharger et installer le certificat de l'autorité de certification et informez-les clairement que leur trafic sera déchiffré. Incluez le processus dans la politique d'utilisation des ordinateurs et dans la politique de confidentialité de votre société.
- ❑ Générez des certificats CA d'approbation de transfert et des certificats de non-approbation de transfert *distincts*. N'utilisez pas la même CA subordonnée de PKI pour les deux certificats et ne signez pas le certificat de non-approbation de transfert avec la CA racine de confiance ! Le certificat de non-approbation de transfert avertit les utilisateurs que le certificat signant le serveur n'est pas légitime et qu'ils ne doivent pas accéder au site. Si la CA racine de confiance signe le certificat de non-approbation, les clients font confiance aux certificats qui ne sont pas approuvés, car ils font confiance à la CA racine.
- ❑ Générez un certificat CA d'approbation de transfert subordonné distinct pour chaque pare-feu. L'utilisation de CA subordonnées distinctes vous permet de révoquer un certificat lorsque vous mettez un appareil (ou une paire d'appareils) hors service sans affecter le reste du déploiement et réduit l'impact si vous avez besoin de révoquer un certificat. Des certificats d'autorité de certification distincts aident le soutien technique à régler les problèmes auxquels les utilisateurs sont confrontés, car le message d'erreur renvoyé par le certificat comprend des informations sur le pare-feu que

le trafic a traversé. Bien qu'il soit plus facile de déployer un seul CA d'approbation de transfert subordonné sur tous les pare-feu, l'utilisation d'un certificat distinct sur chaque pare-feu procure une meilleure sécurité.

- ❑ Si vous avez besoin d'une sécurité supplémentaire pour vos clés privées, envisagez de les stocker dans un HSM.

STEP 4 | Effectuez une mesure de référence de la performance du pare-feu afin de comprendre la consommation de ressources et les ressources du pare-feu qui sont disponibles pour pouvoir comparer la performance après le déploiement du décryptage, puis estimez la taille du déploiement de pare-feu nécessaire pour prendre en charge la quantité de trafic que vous souhaitez déchiffrer.

- ❑ Travaillez avec votre SE/CE de Palo Alto Networks pour dimensionner votre déploiement de pare-feu et éviter les erreurs de dimensionnement.
- ❑ Prenez note des ressources de pare-feu actuellement disponibles. En général, plus votre sécurité est stricte, plus de ressources du pare-feu sont consommées par le décryptage. Voici certains facteurs qui influent sur la quantité de trafic que vous pouvez déchiffrer :
  - La quantité de trafic SSL que vous souhaitez déchiffrer.
  - La version du protocole TLS.
  - La taille de la clé.
  - L'algorithme d'échange de clés. Des algorithmes éphémères de Perfect Forward Secrecy (Confidentialité de transmission parfaite ; PFS) comme DHE et ECDHE consomment plus de ressources que RSA, mais offrent une sécurité accrue, car le pare-feu génère une nouvelle clé de chiffrement pour chaque session. Si un pirate compromet une clé de session, PFS empêche le pirate de l'utiliser pour déchiffrer d'autres sessions entre le même client et le même serveur, ce que RSA ne fait pas.
  - Authentification du certificat. L'authentification du certificat par RSA (qui n'est pas l'algorithme d'échange de clés RSA) consomme moins de cycles du processeur que l'authentification du certificat par ECDSA, mais ECDSA procure le niveau le plus élevé de sécurité.
  - Algorithme de chiffrement. L'algorithme d'échange de clés détermine si l'algorithme de chiffrement est PFS ou RSA.
  - Le modèle et les ressources du pare-feu. Les nouveaux modèles de pare-feu ont plus de ressources que les anciens modèles.
- ❑ La taille des transactions influe sur la performance. Mesurez la taille des transactions moyennes de tout le trafic, puis mesurez la taille des transactions moyennes du trafic sur le port 443 (le port par défaut pour le trafic HTTPS crypté) pour connaître la proportion de trafic crypté qui passe par le pare-feu par rapport à votre trafic total et aux tailles des transactions moyennes.

La combinaison de ces facteurs détermine la consommation des ressources de traitement du pare-feu par le déchiffrement. Si les ressources du pare-feu sont un enjeu, utilisez un déchiffrement plus fort pour le trafic de priorité absolue et de risque plus élevé et utilisez un déchiffrement moins exigeant pour le processeur pour déchiffrer et inspecter le trafic de moindre priorité jusqu'à ce que vous puissiez accroître les ressources disponibles.

Dimensionnez le pare-feu de manière à laisser place à la croissance quant à la quantité de trafic que vous déchiffrez, car la quantité de trafic chiffré croit jour après jour.

STEP 5 | Prévoir un déploiement hiérarchisé et organisé.

- ❑ Identifiez les premiers utilisateurs pour promouvoir le déchiffrement et veiller à l'adhésion des directeurs de service au plan.
- ❑ Établissez des POC pour tester la stratégie de déploiement avant de la déployer à l'ensemble de la population d'utilisateurs générale. Mesurez la manière dont le déploiement des POC de décryptage affecte l'utilisation du processeur et de la mémoire du pare-feu pour vous aider à comprendre si

le dimensionnement du pare-feu est bon. Les POC peuvent également révéler les applications qui interrompent le déchiffrement techniquement.

- Informez les participants à la POC des changements et de la manière de communiquer avec le soutien technique.
- Établissez un POC de soutien technique pour les POC de déchiffrement afin que le soutien ait l'occasion de développer les meilleurs moyens de soutenir le déploiement.
- Déployez le déchiffrement. Prévoyez de déchiffrer le trafic le plus à risque dans un premier temps (catégories d'URL les plus susceptibles de contenir du trafic malveillant, comme les jeux ou à risque élevé), puis d'en déchiffrer davantage lorsque vous acquérez de l'expérience. Vous pouvez éventuellement déchiffrer les catégories d'URL qui n'affectent pas votre entreprise dans un premier temps (si quelque chose ne se passe pas comme prévu, cela n'affecte pas l'entreprise), par exemple, de nouveaux flux d'informations. Dans les deux cas, déchiffrez quelques catégories d'URL, tenez compte des commentaires des utilisateurs, exécutez les rapports et vérifiez les journaux de décryptage pour vous assurer que le déchiffrement fonctionne comme prévu, puis déchiffrez progressivement quelques catégories d'URL supplémentaires, etc. Planifiez de faire des exclusions de déchiffrement pour exclure les sites du déchiffrement, si vous ne pouvez les déchiffrer pour des raisons techniques ou parce que vous choisissez de ne pas les déchiffrer.
- Évaluez le succès des POC et peaufinez les pratiques de déploiement.

- ❑ Informez la population d'utilisateurs avant le déploiement général. Les POC permettent de déterminer les points les plus importants à communiquer.
- ❑ Distribuez des politiques d'utilisation juridiques et de ressources humaines des ordinateurs mises à jour à tous les employés, sous-traitants, partenaires, invités et autres utilisateurs du réseau. Assurez-vous que tous comprennent que leurs données peuvent être déchiffrées et analysées pour détecter les menaces lorsque vous déployez le décryptage dans chaque service ou groupe.
- ❑ Créez des calendriers réalistes qui donnent le temps d'évaluer chaque étape du déploiement.

Déployer le déchiffrement SSL au moyen des meilleures pratiques

STEP 1 | Générez et distribuez les clés et les certificats des politiques de déchiffrement.

- Si vous disposez d'une PKI d'entreprise, générez le certificat de l'autorité de certification d'approbation de transfert pour le trafic de proxy de transfert depuis votre autorité de certification racine d'entreprise. Sinon, générez un certificat AC racine auto-signé sur le pare-feu, créez une CA subordonnée sur le pare-feu, puis diffusez le certificat auto-signé à tous les systèmes clients. Les certificats auto-signés sont conçus pour les essais en laboratoire, les petits déploiements et les tests de Proof-Of-Concept (preuve de concept ; POC).
- Générez un CA d'approbation de transfert subordonné pour chaque pare-feu (ou un CA d'approbation de transfert subordonné pour tous les pare-feu, en fonction de votre planification – il est plus facile de déployer un certificat unique, mais l'utilisation de certificats distincts offre la meilleure sécurité et d'autres avantages). Des plateformes de PKI distinctes possèdent des caractéristiques différentes pour la mise à l'échelle de la gestion des certificats.
- Si vous n'utilisez pas de CA d'entreprise, importez le CA d'approbation de transfert dans le stockage approuvé de la CA dans les systèmes client.
- N'importez pas le certificat CA de *non-approbation* de transfert dans le stockage approuvé de la CA des systèmes client. Autrement, le certificat de non-approbation ne fera pas office d'élément déclencheur pour les sites non approuvés. (Cependant, si la CA racine auto-signée du pare-feu n'a pas été installée en tant qu'émetteur de confiance sur les systèmes client, vous pouvez utiliser un certificat de non-approbation de transfert auto-signé.)
- Utilisez une méthode automatisée pour distribuer les certificats d'approbation de transfert aux périphériques connectés, comme le portail GlobalProtect de Palo Alto Networks, les Services de certificats Active Directory de Microsoft (au moyen d'objets de politique de groupes), les outils commerciaux ou les outils libres.
- Si vous générez le certificat à partir de votre CA racine d'entreprise, importez le certificat sur le pare-feu.
- Sauvegardez la clé privée du certificat CA d'approbation de transfert du pare-feu (pas la clé principale du pare-feu) dans un registre sécuritaire. Ainsi, en cas de problème, vous pouvez toujours accéder au certificat CA d'approbation de transfert.
- Si vous générez des certificats et des clés privées à partir de votre CA racine d'entreprise, bloquez l'exportation de clés privées. (Vous pouvez les installer sur les nouveaux pare-feu et Panoramas à partir de votre CA d'entreprise, de manière à ne pas avoir besoin de les exporter à partir de PAN-OS.)
- Si vous prévoyez de faire des appels pour utiliser un HSM, stockez les clés privées sur le HSM.

STEP 2 | Configurez des protocoles de contrôle pour contrôler les protocoles, la vérification des certificats et la gestion des échecs.

- Les profils de déchiffrement du proxy de transfert SSL contrôlent la vérification des certificats du serveur, les modes de session et les vérifications d'échec pour le trafic sortant. Bloquez les sessions comportant des certificats expirés, des émetteurs non approuvés ainsi que des versions et des suites de chiffrement non prises en charge. Bloquez les sessions avec authentification du client, sauf si une application importante l'exige. Dans un tel cas, vous devez créer un profil de déchiffrement distinct qui permet l'authentification du client et l'appliquer uniquement au client qui doit faire l'objet d'une authentification du client.
- Les profils d'inspection SSL entrante contrôlent les modes de session et les vérifications d'échec pour le trafic entrant. Bloquer les sessions avec des versions et des suites de chiffrement non prises en charge.

- Les paramètres du protocole SSL contrôlent les éléments des suites de chiffrement, les versions du protocole, les algorithmes d'échange de clés, les algorithmes de chiffrement et les algorithmes d'authentification pour le trafic de proxy de transfert SSL et d'inspection SSL entrante. Utilisez les chiffrements les plus forts possibles. Pour le proxy de transfert, définissez la **Min Version** (Version min.) du protocole sur **TLSv1.2** et la **Max Version** (Version max.) sur **Max** pour bloquer les protocoles faibles. Pour l'inspection SSL entrante, créez des profils distincts avec des paramètres de protocole qui correspondent aux capacités des serveurs dont vous inspectez le trafic entrant.

  

  Utilisez la suite de chiffrements la plus forte possible. Créez des politiques et des profils de décryptage distincts pour optimiser la sécurité. Si d'anciens sites dont vous avez besoin à des fins professionnelles ne prennent en charge que des chiffrements plus faibles, créez un profil de décryptage distinct pour autoriser le trafic et appliquez-le dans une politique de décryptage uniquement aux sites nécessaires. Utilisez la même technique pour ajuster le rapport sécurité/performances pour différentes catégories d'URL.

  De nombreuses applications mobiles utilisent des certificats épinglés. Comme TLSv1.3 crypte les informations de certification, le pare-feu ne peut pas ajouter ces applications mobiles automatiquement à la liste d'exclusion de décryptage SSL. Pour ces applications, assurez-vous que la Max Version (Version maximale) du profil de décryptage est configurée sur TLSv1.2 ou appliquez une politique de non-décryptage pour le trafic.
- Les profils d'absence de déchiffrement contrôlent les vérifications de serveur pour le trafic que vous choisissez de ne pas déchiffrer. Bloquez les sessions aux certificats expirés et provenant de distributeurs non approuvés.

  

  N'appliquez pas d'absence de profil de décryptage au trafic TLSv1.3. Les informations du certificat sont cryptées, afin que le pare-feu ne puisse pas bloquer les sessions basées sur les informations de certificat.
- Pour le trafic de proxy de transfert SSL et d'absence de déchiffrement, configurez les vérifications de révocation de certificat de la Certificate Revocation List (liste de révocation de certificats ; CRL) et du Online Certificate Status Protocol (protocole de vérification des certificats en ligne ; OCSP) pour vérifier que les certificats du site n'ont pas été révoqués.
- Les profils de proxy SSH contrôlent les modes de session et les vérifications d'échec pour le trafic par tunnel SSH. Bloquer les sessions avec des versions et des algorithmes non pris en charge.

Les paramètres de profil de déchiffrement exemplaires pour le centre de données et pour le périmètre (passerelle internet) diffèrent légèrement des paramètres exemplaires généraux.

STEP 3 | Configurez les règles de politique de déchiffrement pour définir le trafic à déchiffrer et créer des exceptions basées sur la politique pour le trafic que vous ***choisissez*** de ne pas déchiffrer.

- Créez des règles de politique pour exclure des adresses IP de destination (par exemple, les serveurs financiers), des utilisateurs et groupes source (par exemple, les dirigeants ou le personnel des RH), des périphériques source et des ports d'application que vous choisissez de ne pas déchiffrer. Placez ces règles en haut de la base de règles de déchiffrement, devant les règles qui déchiffrent le trafic. Pour l'ensemble du trafic à l'exception du trafic TLSv1.3, associez-y un profil d'absence de déchiffrement pour appliquer des contrôles de vérification de certificat serveur SSL au trafic chiffre. Cette façon de faire vous empêche de déchiffrer par mégarde du trafic que vous ne voulez pas déchiffrer.
- Utilisez URL Categories (Catégories d'URL), Custom URL Categories (Catégories d'URL personnalisées) et External Dynamic Lists (EDL) (Listes dynamiques externes) pour spécifier les URL à ne pas déchiffrer, telles que les catégories de services financiers, santé et médecine, gouvernement et toute autre catégorie que vous ne souhaitez pas déchiffrer pour des raisons commerciales, juridiques ou réglementaires. Utilisez un EDL dans les environnements possédant des adresses IP qui changent

de manière dynamique (par exemple, Office 365) ou qui font l'objet de changements d'adhésion fréquents pour mettre à jour sans avoir besoin de valider.

Créez une Custom URL Category (Catégorie d'URL personnalisées) ou EDL contenant toutes les catégories que vous choisissez de ne pas déchiffré afin que vous n'ayez besoin que d'une seule règle de politique de déchiffrement pour elles.

Placez ces règles au-dessus des règles qui déchiffrent le trafic dans la base de règles de déchiffrement.

- Configurez le décryptage de journalisation et le transfert des journaux.
- Si vous utilisez la mise en miroir du déchiffrement pour copier et envoyer le trafic déchiffré à un outil de collecte du trafic, soyez à l'affût des règles relatives au respect de la vie privée locales qui peuvent interdire la surveillance ou le contrôle du trafic que vous pouvez mettre en miroir.
- Créez une politique pour déchiffrer le reste du trafic en configurant les règles de proxy de transfert SSL, d'inspection SSL entrante et de proxy SSH. Déchiffrez toujours les catégories de sauvegarde et stockage en ligne, messagerie Web, hébergement Web, sites personnels et blogues, réseaux de distribution de contenu ainsi que les catégories d'URL à risque élevé. Limitez le proxy SSH aux administrateurs qui gèrent des périphériques réseau, consignez tout le trafic SSH et configurez l'Authentification multi-facteurs pour empêcher tout accès SSH non autorisé.

STEP 4 | Ajoutez les sites à la liste d'exclusion du déchiffrement SSL (**Device (Périphérique)** > **Certificate Management (Gestion des certificats)** > **SSL Decryption Exclusion (Exclusion du déchiffrement SSL)**) s'ils interrompent le déchiffrement techniquement lors d'un test POC et s'ils ne figurent pas déjà sur la liste d'exclusion. (Le déchiffrement des sites qui bloquent le déchiffrement entraîne techniquement le blocage de ce trafic.)

STEP 5 | Dans la politique de sécurité, bloquez le protocole de connexions Internet UDP rapides (QUIC).

Chrome et certains autres navigateurs établissent des sessions au moyen du protocole QUIC au lieu du protocole TLS, mais QUIC utilise un chiffrement propriétaire que le pare-feu ne peut déchiffrer ; le trafic potentiellement dangereux peut alors entrer sur le réseau en tant que trafic chiffré. Créez deux règles, l'une pour bloquer l'application QUIC sur les ports standards et l'autre pour bloquer les ports UDP 80 et 443. En bloquant le protocole QUIC, vous forcez le navigateur à utiliser le protocole TLS.

STEP 6 | Transférez le trafic déchiffré à WildFire pour qu'il l'inspecte afin d'y déceler des fichiers malveillants.

STEP 7 | Déployez le déchiffrement lentement.

Déchiffrez quelques catégories d'URL, passez en revue les commentaires des utilisateurs, puis exécutez les rapports pour vous assurer que le décryptage fonctionne comme prévu. Déchiffrez graduellement un plus grand nombre de catégories d'URL et poursuivez jusqu'à ce que vous ayez atteint votre objectif. Commencez par le trafic de priorité absolue (les catégories d'URL les plus susceptibles de contenir du trafic malveillant, comme les jeux), puis déchiffrez-en davantage lorsque vous acquérez de l'expérience et affinez le processus. Une approche plus prudente consiste à déchiffrer les catégories d'URL qui n'affectent pas votre entreprise dans un premier temps, par exemple les fils d'actualité.

Suivre les pratiques exemplaires en matière de déchiffrement SSL après le déploiement

Après avoir déployé le déchiffrement, assurez-vous que tout fonctionne comme prévu et prenez les mesures nécessaires pour vous assurer qu'il continue à fonctionner comme prévu.

STEP 1 | Vérifiez que le déchiffrement fonctionne comme prévu.

STEP 2 | Mesurez la performance du pare-feu pour vous assurer qu'elle se situe dans les normes acceptables et pour comprendre l'effet du déchiffrement sur la performance.

Si vous souhaitez déchiffrer plus de trafic que les ressources du pare-feu prennent en charge, accroissez les ressources pour en posséder suffisamment pour déchiffrer tout le trafic que vous voulez déchiffrer et sécuriser votre réseau.

STEP 3 | Formez les nouveaux employés lorsque vous les embauchez afin qu'ils comprennent votre politique de décryptage et ne soient pas surpris s'ils ne parviennent pas à atteindre un site donné parce qu'il utilise des suites de chiffrement faibles.

STEP 4 | Revoyez périodiquement les profils et politiques de déchiffrement et mettez-les à jour.

STEP 5 | Utilisez des outils de dépannage du décryptage comme les widgets d'**activité SSL** du centre de commande d'application et le journal de décryptage (**Monitor [Surveillance]** > **Logs [Journaux]** > **Decryption [Décryptage]**) pour surveiller le trafic de décryptage et résoudre les problèmes de décryptage.

Des exemples de flux de production de dépannage de décryptage vous montrent comment utiliser les outils pour examiner les problèmes.

STEP 6 | Utilisez la documentation de Palo Alto Networks et d'autres ressources pour en apprendre davantage sur le déchiffrement et pour chercher des informations :

- Le Guide de l'administrateur de PAN-OS fournit des informations détaillées sur les pare-feu nouvelle génération Palo Alto Networks.
- La communauté en direct de Palo Alto Networks offre une liste de ressources relatives au déchiffrement qui comprend des articles qui portent sur la configuration, le paramétrage et l'administration du déchiffrement.
- Pour trouver les certificats intermédiaires manquants, visitez SSL Labs (Qualys).
- Pour savoir quelles suites de chiffrement sont prises en charge par un serveur, consultez la page de test SSL du serveur sur le site de Qualys SSL Labs.
- Pour consulter les statistiques à jour sur les pourcentages des différents chiffrements et protocoles utilisés sur les 150 000 sites les plus populaires du monde. Vous pouvez ainsi suivre les tendances et comprendre à quel point le support mondial est étendu pour des chiffrements et des protocoles plus sûrs, rendez-vous sur la page SSL Pulse de Qualys SSL Labs.