paloalto TECHDOCS

Meilleures pratiques de déchiffrement

Version 10.2

docs.paloaltonetworks.com

Contact Information

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

About the Documentation

- For the most recent version of this guide or for access to 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

January 18, 2022

Table of Contents

Meilleures pratiques de déchiffrement

Vous ne pouvez pas protéger votre réseau contre des menaces que vous ne pouvez pas voir et inspecter. Gartner a noté qu'en 2020, environ 70 % des nouvelles campagnes de logiciels malveillants utilisaient diverses formes de cryptage. de Google Rapport de transparence montre que, quelle que soit la manière dont vous analysez le trafic Web de Google, dans la plupart des cas, jusqu'à 95 % de celui-ci est crypté. Décrypter ce trafic pour protéger votre réseau contre les menaces cachées.

Ce document est une liste de contrôle simplifiée des meilleures pratiques de pré-déploiement, de déploiement et de post-déploiement que vous pouvez suivre pour implémenter le déchiffrement. Chaque section comprend des liens vers des informations détaillées dans le Guide d'administration de PAN-OS, y compris comment configurer les règles et les profils de stratégie de déchiffrement.

- Planifiez votre déploiement des meilleures pratiques de déchiffrement SSL
- Déployer le décryptage SSL en utilisant les meilleures pratiques
- Suivez les meilleures pratiques de déchiffrement SSL post-déploiement

Planifier votre déploiement des meilleures pratiques de décryptage SSL

Préparer le déploiement du déchiffrement en élaborant une stratégie de décryptage et un plan de déploiement. L'activation du déchiffrement peut modifier la façon dont les utilisateurs interagissent avec certaines applications et certains sites Web, de sorte que la planification, les tests et la formation des utilisateurs sont essentiels à la réussite du déploiement.

STEP 1 | Fixez-vous des objectifs.

- Prévoyez de déchiffrer autant de trafic qui n'est pas privé ou sensible que votre pare-feu ressources permit. Cela réduit la surface d'attaque en exposant et en empêchant les menaces chiffrées. Comprendre les lois et réglementations locales sur le trafic que vous pouvez légalement déchiffrer et les exigences de notification des utilisateurs.
- Migrer d'un port basé sur un serveur vers un modèle basé sur une application Sécurité règles de stratégie avant de créer et de déployer des règles de stratégie de déchiffrement. Si vous créez des règles de déchiffrement basées sur une stratégie de sécurité basée sur les ports, puis que vous migrez vers une stratégie de sécurité basée sur une application, la modification peut entraîner le blocage du trafic que vous avez l'intention d'autoriser, car les règles de stratégie de sécurité sont susceptibles d'utiliser des ports par défaut d'application pour empêcher le trafic d'utiliser des ports non standard. La migration vers des règles basées sur App-ID avant de déployer le déchiffrement garantit que lorsque vous testez votre déploiement de déchiffrement, vous découvrez les erreurs de configuration de la stratégie de sécurité et les corrigez avant de déployer le déchiffrement dans la population générale d'utilisateurs.

STEP 2 | Travailler avec les parties prenantes et les éduquer tels que les services juridiques, financiers, RH, cadres, sécurité et informatique / support pour développer une stratégie de déploiement de décryptage.

- ☐ Obtenez les approbations requises pour déchiffrer le trafic afin de sécuriser l'entreprise.
- ☐ Identifiez et hiérarchisez le trafic à déchiffrer :
  - Décidez quelles applications déchiffrer (sanctionnées, non autorisées). N'autorisez pas les applications chiffrées non autorisées.
  - Décidez quels appareils déchiffrer (entreprise, BYOD, mobile, etc.).

    Les entreprises ne contrôlent pas les appareils BYOD. Si vous autorisez les appareils BYOD sur votre réseau, déchiffrez leur trafic et soumettez-le à la même stratégie de sécurité que celle que vous appliquez à d'autres trafics réseau. Pour ce faire, redirigez les utilisateurs BYOD via un portail d'authentification, indiquez-leur comment télécharger et installer le certificat d'autorité de certification et informez clairement les utilisateurs que leur trafic sera déchiffré. Informez les utilisateurs BYOD sur le processus et incluez-le dans la politique de confidentialité et d'utilisation de l'ordinateur de votre entreprise.

  - Décidez si vous souhaitez utiliser la même stratégie de déchiffrement pour différents groupes, tels que différents groupes d'employés, sous-traitants, partenaires et invités.
- ☐ Identifiez le trafic que vous ne pouvez pas déchiffrer :
  - Trafic qui interrompt le déchiffrement pour raisons techniques tels que l'épinglage de certificat, les chiffrements non pris en charge ou l'authentification mutuelle.
  - Trafic que vous choisir de ne pas déchiffrer tels que les finances, la santé, le gouvernement et d'autres catégories sensibles, y compris les utilisateurs et les groupes tels que les cadres.
  - Comprenez parfaitement le trafic que vous, à l'exception du décryptage. Vous n'avez pas de visibilité sur le trafic chiffré et le pare-feu ne peut pas appliquer de profils de prévention des menaces au trafic chiffré.
- ☐ Préparez des politiques d'utilisation des ordinateurs juridiques et RH mises à jour à distribuer à tous les employés, sous-traitants, partenaires, invités et autres utilisateurs du réseau afin que, lorsque vous déployez le déchiffrement, les utilisateurs comprennent que leurs données peuvent être déchiffrées et analysées à la recherche de menaces.
- ☐ Décider comment gérer la vérification des certificats. Votre modèle d'entreprise peut nécessiter des compromis entre la sécurité et l'expérience utilisateur. Comprendre comment vous souhaitez gérer la vérification des certificats permet de déterminer comment configurer les profils de déchiffrement de proxy de transfert SSL.
- ☐ Identifiez le trafic que vous souhaitez enregistrer. Soyez conscient des différences juridiques et réglementaires locales et de la façon dont elles affectent le trafic que vous pouvez enregistrer et l'endroit où vous pouvez stocker les journaux.

Placez les pare-feu à l'endroit où ils peuvent voir tout le trafic réseau afin qu'aucun trafic chiffré n'accède par inadvertance à votre réseau car il contourne le pare-feu.

STEP 3 | Élaborez un plan de déploiement de votre infrastructure à clé publique (PKI).

- ☐ Si vous disposez d'une infrastructure à clé publique existante, générez le certificat d'autorité de certification SSL Forward Trust à partir de votre autorité de certification racine d'entreprise

en tant que certificat subordonné. Cela facilite le déploiement, car les périphériques réseau font déjà confiance à l'autorité de certification racine d'entreprise, de sorte que vous ne rencontrerez pas de problèmes de certificat. Si vous n'avez pas d'autorité de certification racine d'entreprise, envisagez d'en obtenir une.

Vous pouvez également générer un certificat d'autorité de certification racine auto-signé sur le pare-feu et créer un certificat d'autorité de certification de confiance directe subordonné sur ce pare-feu à installer sur les périphériques réseau. Les certificats auto-signés sont les meilleurs pour les petites entreprises qui n'ont pas d'autorité de certification racine d'entreprise et pour les essais de preuve de concept (POC).

Comme pour les appareils BYOD, les entreprises ne contrôlent pas les appareils invités. Si vous autorisez les appareils invités sur votre réseau, déchiffrez leur trafic et soumettez-le à la même stratégie de sécurité que celle que vous appliquez à d'autres trafics réseau. Pour ce faire, redirigez les utilisateurs invités via un portail d'authentification, indiquez-leur comment télécharger et installer le certificat d'autorité de certification et informez clairement les utilisateurs que leur trafic sera déchiffré. Incluez le processus dans la politique de confidentialité et d'utilisation de l'ordinateur de votre entreprise.

- Générer ***séparer*** Certificats d'autorité de certification pour Forward Trust et Forward Untrust. N'utilisez pas la même autorité de certification subordonnée PKI pour les deux certificats et ne signez pas le certificat Forward Untrust avec l'autorité de certification racine de confiance ! Le certificat Forward Untrust avertit les utilisateurs que le certificat signant le serveur n'est pas légitime et qu'ils ne doivent pas accéder au site. Si l'autorité de certification racine de confiance signe le certificat untrust, les clients approuvent les certificats qui ne doivent pas être approuvés car les clients font confiance à l'autorité de certification racine.
- Générez un certificat d'autorité de certification d'approbation directe subordonné distinct pour chaque pare-feu. L'utilisation d'autorités de certification subordonnées distinctes vous permet de révoquer un certificat lorsque vous mettez hors service un périphérique (ou une paire d'appareils) sans affecter le reste du déploiement et réduit l'impact si vous devez révoquer un certificat. Des certificats d'autorité de certification distincts aident le support technique à résoudre les problèmes des utilisateurs, car le message d'erreur de certificat inclut des informations sur le pare-feu traversé par le trafic. Bien que l'utilisation d'une autorité de certification subordonnée Forward Trust sur tous les pare-feu soit plus facile à déployer, l'utilisation d'un certificat distinct sur chaque pare-feu offre la meilleure sécurité.
- Si vous avez besoin d'une sécurité supplémentaire pour vos clés privées, envisagez les stocker dans un HSM.

STEP 4 | Prenez une mesure de base des performances du pare-feu pour comprendre la consommation de ressources et les ressources de pare-feu disponibles afin de pouvoir comparer les performances après le déploiement du déchiffrement et estimer le taille du déploiement du pare-feu requis pour prendre en charge la quantité de trafic que vous souhaitez déchiffrer.

- Travaillez avec votre Palo Alto Networks SE/CE pour dimensionner le déploiement du pare-feu et éviter les erreurs de dimensionnement.

- ☐ Notez les ressources de pare-feu actuellement disponibles. En général, plus votre sécurité est stricte, plus le décryptage consomme de ressources. Les facteurs qui affectent la quantité de trafic que vous pouvez déchiffrer incluent :
  - La quantité de trafic SSL que vous souhaitez déchiffrer.
  - Version du protocole TLS.
  - Taille de la clé.
  - Algorithme d'échange de clés. Les algorithmes éphémères PFS (Perfect Forward Secrecy) tels que DHE et ECDHE consomment plus de ressources que RSA, mais offrent une plus grande sécurité car le pare-feu génère une nouvelle clé de chiffrement pour chaque session. Si un attaquant compromet une clé de session, PFS l'empêche de l'utiliser pour déchiffrer d'autres sessions entre le même client et le même serveur, contrairement à RSA.
  - Authentification par certificat. L'authentification par certificat RSA (ce n'est pas la même chose que l'algorithme d'échange de clés RSA) consomme moins de cycles CPU que l'authentification par certificat ECDSA, mais ECDSA offre le plus haut niveau de sécurité.
  - Algorithme de chiffrement. L'algorithme d'échange de clés détermine si l'algorithme de chiffrement est PFS ou RSA.
  - Le modèle de pare-feu et ressources. Les nouveaux modèles de pare-feu ont plus de ressources que les modèles plus anciens.
- ☐ La taille des transactions affecte les performances. Mesurez la taille moyenne des transactions de tout le trafic, puis mesurez la taille moyenne des transactions sur le port 443 (port par défaut pour le trafic chiffré HTTPS) pour comprendre la proportion de trafic chiffré sur le pare-feu par rapport à votre trafic total et la taille moyenne des transactions.

La combinaison de ces facteurs détermine la façon dont le déchiffrement consomme les ressources de traitement du pare-feu. Si les ressources du pare-feu sont un problème, utilisez un déchiffrement plus fort pour le trafic à priorité plus élevée et à risque élevé et utilisez un déchiffrement moins gourmand en processeur pour déchiffrer et inspecter le trafic de priorité inférieure jusqu'à ce que vous puissiez augmenter les ressources disponibles.

Dimensionnez le pare-feu pour inclure une marge de manœuvre pour la croissance de la quantité de trafic à déchiffrer, car plus de trafic est chiffré chaque jour.

STEP 5 | Planifier un déploiement échelonné et hiérarchisé.

- ☐ Identifiez les premiers utilisateurs pour défendre le décryptage et obtenez l'adhésion des responsables de service au plan.
- ☐ Configurez des POC pour tester la stratégie de déploiement avant de la déployer auprès de la population d'utilisateurs générale. Mesurez la façon dont le déploiement du POC de déchiffrement affecte l'utilisation du processeur et de la mémoire du pare-feu pour aider à comprendre si le dimensionnement du pare-feu est correct. Les POC peuvent également révéler des applications qui interrompent techniquement le décryptage.
  - Éduquer les participants au POC sur les changements et sur la façon de contacter le support technique.
  - Configurez un POC de support technique pour les POC de décryptage afin que le support ait la possibilité de développer les meilleurs moyens de prendre en charge le déploiement.

- Décryptage progressif. Prévoyez d'abord de déchiffrer le trafic le plus risqué (catégories d'URL les plus susceptibles d'héberger du trafic malveillant, tel que les jeux ou les jeux à haut risque), puis déchiffrez-en davantage à mesure que vous gagnez en expérience. Vous pouvez également déchiffrer les catégories d'URL qui n'affectent pas d'abord votre entreprise (si quelque chose ne va pas, cela n'affectera pas l'entreprise), par exemple, les flux d'actualités. Dans les deux cas, déchiffrez quelques catégories d'URL, écoutez les commentaires des utilisateurs, exécutez des rapports et vérifiez Journaux de décryptage pour s'assurer que le décryptage fonctionne comme prévu, puis déchiffrer progressivement quelques catégories d'URL supplémentaires, etc. Planifier pour faire exclusions de déchiffrement pour exclure des sites du déchiffrement si vous ne pouvez pas les déchiffrer pour des raisons techniques ou parce que vous choisissez de ne pas les déchiffrer.
- Évaluez le succès des POC et affinez les pratiques de déploiement.

- Éduquez la population d'utilisateurs avant le déploiement général. Les POC aident à identifier les points les plus importants à communiquer.
- Distribuez des politiques d'utilisation des ordinateurs juridiques et RH mises à jour à tous les employés, sous-traitants, partenaires, invités et autres utilisateurs du réseau. Assurez-vous que tout le monde comprend que leurs données peuvent être déchiffrées et analysées à la recherche de menaces lorsque vous déployez le déchiffrement dans chaque service ou groupe.
- Créez des calendriers réalistes qui laissent le temps d'évaluer chaque étape du déploiement.

Déployer le décryptage SSL en utilisant les meilleures pratiques

STEP 1 | Générer et diffuser clés et certificats pour les politiques de déchiffrement.

- Si vous disposez d'une infrastructure à clé publique d'entreprise, générez le certificat Forward Trust CA pour le trafic proxy de transfert à partir de votre Enterprise Root CA. Sinon, générez un certificat d'autorité de certification racine auto-signé sur le pare-feu, créez une autorité de certification subordonnée sur ce pare-feu, puis distribuez le certificat auto-signé à tous les systèmes clients. Les certificats auto-signés sont destinés aux tests en laboratoire, aux petits déploiements et aux POC.
- Générez une autorité de certification Forward Trust subordonnée unique pour chaque pare-feu (ou une autorité de certification Forward Trust pour tous les pare-feu, selon votre Planification— un certificat est plus facile à déployer, mais des certificats séparés offrent la meilleure sécurité et d'autres avantages). Différentes plates-formes PKI ont différentes fonctionnalités pour la mise à l'échelle de la gestion des certificats.
- Si vous n'utilisez pas d'autorité de certification d'entreprise, importez le certificat Forward Trust CA dans le stockage de l'autorité de certification de confiance des systèmes clients.
- Ne pas importer le transfert ***Méfiance*** Le certificat de l'autorité de certification dans le stockage de confiance de l'autorité de certification sur les systèmes clients ou le certificat de non-approbation n'agira pas comme un déclencheur pour les sites non approuvés. (Toutefois, si l'autorité de certification racine auto-signée du pare-feu n'est pas installée en tant qu'émetteur approuvé sur les systèmes clients, vous pouvez utiliser un certificat Forward Untrust auto-signé.)
- Utilisez un méthode automatisée pour distribuer les certificats Forward Trust aux appareils connectés, tels que le portail GlobalProtect de Palo Alto Networks, les services de certificats Microsoft AD (à l'aide d'objets de stratégie de groupe), des outils commerciaux ou des outils open source.
- Si vous générez le certificat à partir de votre autorité de certification racine d'entreprise, importez le certificat sur le pare-feu.
- Sauvegardez la clé privée du certificat Forward Trust CA du pare-feu (et non la clé principale du pare-feu) dans un référentiel sécurisé afin qu'en cas de problème, vous puissiez toujours accéder au certificat Forward Trust CA.
- Si vous générez des certificats et des clés privées à partir de votre Enterprise Root CA, bloquer l'exportation des clés privées. (Vous pouvez les installer sur de nouveaux pare-feu et panoramas à partir de votre autorité de certification d'entreprise, vous n'avez donc pas besoin de les exporter à partir de PAN-OS.)
- Si votre plan prévoit l'utilisation d'un HSM, stocker les clés privées sur le HSM.

STEP 2 | Configurer les profils de déchiffrement pour contrôler les protocoles, la vérification des certificats et la gestion des pannes.

- Profils SSL Forward Proxy Decryption contrôler la vérification du certificat du serveur, les modes de session et les vérifications d'échec pour le trafic sortant. Bloquez les sessions avec des certificats expirés, des émetteurs non approuvés, des versions non prises en charge et des suites de chiffrement non prises en charge. Bloquez les sessions avec authentification

du client sauf si une application importante l'exige, auquel cas vous devez créer un profil de déchiffrement distinct qui permet l'authentification du client et l'appliquer uniquement au trafic qui nécessite l'authentification du client.

- Profils SSL Inbound Inspection Decryption contrôler les modes de session et les vérifications d'échec pour le trafic entrant. Bloquez les sessions avec des versions non prises en charge et des suites de chiffrement non prises en charge.
- Paramètres du protocole SSL contrôler les éléments de la suite de chiffrement : versions de protocole, algorithmes d'échange de clés, algorithmes de chiffrement et algorithmes d'authentification pour le trafic SSL Forward Proxy et SSL Inbound Inspection. Utilisez les chiffrements les plus forts que vous pouvez. Pour Forward Proxy, définissez le protocole **Version minimale** à **TLSv1.2** et le **Version maximale** à **Max** pour bloquer les protocoles faibles. Pour l'inspection SSL entrante, créez des profils distincts avec des paramètres de protocole qui correspondent aux capacités du ou des serveurs dont vous inspectez le trafic entrant.

  Utilisez la suite de chiffrement la plus puissante possible. Créez des politiques et des profils de déchiffrement distincts pour optimiser la sécurité. Si les sites hérités dont vous avez besoin à des fins professionnelles ne prennent en charge que des chiffrements plus faibles, créez un profil de déchiffrement distinct pour autoriser ce trafic et appliquez-le dans une stratégie de déchiffrement uniquement aux sites nécessaires. Utilisez la même technique pour affiner la sécurité par rapport aux performances pour différentes catégories d'URL.

  De nombreuses applications mobiles utilisent des certificats épinglés. Étant donné que TLSv1.3 crypte les informations de certificat, le pare-feu ne peut pas automatiquement ajouter ces applications mobiles à la liste d'exclusion de décryptage SSL. Pour ces applications, assurez-vous que le profil de déchiffrement ***Version maximale*** *est défini sur TLSv1.2 ou appliquez une politique de non déchiffrement au trafic.*
- Aucun profil de déchiffrement contrôler la vérification du certificat du serveur pour le trafic que vous choisissez de ne pas déchiffrer. Bloquez les sessions avec des certificats expirés et des émetteurs non approuvés.

  N'appliquez pas de profil No Decryption au trafic TLSv1.3. Les informations de certificat sont cryptées, de sorte que le pare-feu ne peut pas bloquer les sessions en fonction des informations de certificat.
- Pour le proxy de transfert SSL et le trafic sans déchiffrement, configurez à la fois la liste de révocation de certificats (CRL) et la révocation de l'état des certificats en ligne (OCSP) révocation de certificat vérifications pour vérifier que les certificats de site n'ont pas été révoqués.
- Profils proxy SSH contrôler les modes de session et les vérifications d'échec pour le trafic tunnelisé SSH. Bloquer les sessions avec des versions non prises en charge et des algorithmes non pris en charge.

Les paramètres de profil de déchiffrement des meilleures pratiques pour le centre de données et pour le périmètre (passerelle internet) les cas d'utilisation diffèrent légèrement des paramètres généraux des meilleures pratiques.

STEP 3 | Configurer Règles de politique de déchiffrement pour définir le trafic à décrypter et faire exceptions basées sur des règles pour le trafic vous ***choisir*** à ne pas décrypter.

- Créez des règles de stratégie pour exclure des adresses IP de destination spécifiques (par exemple, des serveurs financiers), des utilisateurs et des groupes sources (par exemple, des cadres ou du personnel des RH), des appareils sources et des ports d'application que vous choisissez de ne pas déchiffrer. Placez ces règles en haut de la base de règles de déchiffrement, avant les règles qui déchiffrent le trafic. Pour tout le trafic à l'exception du trafic TLSv1.3, attachez-leur un profil No Decryption pour appliquer SSL contrôles de vérification des certificats de serveur au trafic crypté. Cela empêche de déchiffrer par inadvertance le trafic que vous ne souhaitez pas déchiffrer.
- Utilisez les catégories d'URL, les catégories d'URL personnalisées et les listes dynamiques externes (EDL) pour spécifier les URL à ne pas déchiffrer, telles que les services financiers, la santé et la médecine, le gouvernement et toute autre catégorie que vous ne souhaitez pas déchiffrer pour les entreprises, des raisons légales ou réglementaires. Utilisez une liste EDL dans des environnements avec des adresses IP qui changent dynamiquement (par exemple, Office 365) ou des changements d'adhésion fréquents pour mettre à jour sans avoir à valider.

  Créez une EDL ou une catégorie d'URL personnalisée qui contient toutes les catégories que vous choisissez de ne pas déchiffrer 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.
- Configurer journalisation de déchiffrement et transfert de journaux.
- Si tu utilises Mise en miroir du déchiffrement pour copier et envoyer le trafic décrypté à un outil de collecte de trafic, soyez conscient des réglementations locales en matière de confidentialité qui peuvent interdire la mise en miroir ou contrôler le trafic que vous pouvez mettre en miroir.
- Créez une stratégie pour déchiffrer le reste du trafic en configurant Proxy de transfert SSL, Inspection SSL entrante, et Proxy SSH règles. Décryptez toujours les catégories de stockage et de sauvegarde en ligne, de messagerie Web, d'hébergement Web, de sites personnels et de blogs, de réseaux de diffusion de contenu et d'URL à haut risque. Limitez le proxy SSH aux administrateurs qui gèrent les périphériques réseau, enregistrent tout le trafic SSH et configurent Authentification multifacteur pour empêcher tout accès SSH non autorisé.

STEP 4 | Ajouter des sites à la Liste d'exclusion de décryptage SSL (**Dispositif** > **Gestion des certificats** > **Exclusion de décryptage SSL**) s'ils cassent techniquement le déchiffrement lors des tests POC et ne figurent pas déjà sur la liste d'exclusion. (Le décryptage des sites qui bloquent le décryptage entraîne techniquement le blocage de ce trafic.)

STEP 5 | Dans Politique de sécurité, bloquer le protocole Quick UDP Internet Connections (QUIC).

Chrome et certains autres navigateurs établissent des sessions à l'aide de QUIC au lieu de TLS, mais QUIC utilise un cryptage propriétaire que le pare-feu ne peut pas décrypter, de sorte qu'un trafic potentiellement dangereux peut entrer sur le réseau sous forme de trafic crypté. Créez deux règles, une pour bloquer l'application QUIC sur les ports standard et une pour bloquer les ports UDP 80 et 443. Le blocage de QUIC force le navigateur à utiliser TLS.

STEP 6 | Transférer le trafic décrypté vers WildFire pour l'inspecter à la recherche de logiciels malveillants.

STEP 7 | Déployez le décryptage lentement.

Décryptez quelques catégories d'URL, examinez les commentaires des utilisateurs et exécutez des rapports pour vous assurer que le décryptage fonctionne comme prévu. Décryptez progressivement plus de catégories d'URL jusqu'à ce que vous atteigniez votre objectif. Commencez par le trafic le plus prioritaire (les catégories d'URL les plus susceptibles d'héberger du trafic malveillant, comme les jeux), et déchiffrez-en davantage au fur et à mesure que vous apprenez de l'expérience et affinez le processus. Une alternative plus conservatrice consiste à déchiffrer d'abord les catégories d'URL qui n'affectent pas votre entreprise, par exemple les flux d'actualités.

Suivez les meilleures pratiques de décryptage SSL post-déploiement

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

STEP 1 | Vérifier que le décryptage fonctionne comme prévu.

STEP 2 | Mesurez les performances du pare-feu pour vous assurer qu'elles respectent les normes acceptables et que vous comprenez l'effet du déchiffrement sur les performances.

Si vous souhaitez déchiffrer plus de trafic que les ressources de pare-feu ne prennent en charge, augmentez afin de disposer de suffisamment de ressources pour déchiffrer tout le trafic que vous souhaitez déchiffrer et sécuriser votre réseau.

STEP 3 | Éduquez les nouveaux employés au fur et à mesure que vous les embauchez afin qu'ils comprennent votre politique de décryptage et ne soient pas surpris s'ils ne peuvent pas atteindre un site particulier car il utilise des suites de chiffrement faibles.

STEP 4 | Examinez et mettez à jour périodiquement les stratégies et les profils de déchiffrement.

STEP 5 | Utiliser outils de dépannage du décryptage tels que l'Application Command Center **Activité SSL** widgets et journal de décryptage (**Moniteur** > **Journaux** > **Décryptage**) pour surveiller le trafic de déchiffrement et résoudre les problèmes de déchiffrement.

Exemples de flux de travail de dépannage du déchiffrement vous montrer comment utiliser les outils pour enquêter sur les problèmes.

STEP 6 | Lorsque vous devez modifier le certificat sur un serveur pour lequel le pare-feu fonctionne Inspection entrante SSL, ajouter le nouveau certificat à la règle de stratégie de déchiffrement pour ce serveur avant d'effectuer la modification sur le serveur. Les règles de stratégie de déchiffrement prennent en charge plusieurs certificats de serveur, ce qui vous permet de conserver l'ancien certificat et d'ajouter le nouveau certificat à la règle. Cela évite toute interruption du déchiffrement due à la modification du certificat sur le serveur lorsque le pare-feu ne possède que l'ancien certificat. L'ajout du nouveau certificat de serveur à la règle de stratégie de déchiffrement garantit que lorsque vous modifiez le certificat sur le serveur, le pare-feu dispose du certificat approprié pour continuer à déchiffrer le trafic de manière transparente.

Veillez à supprimer les certificats non valides des règles de stratégie de déchiffrement et du pare-feu après avoir modifié les certificats de serveur.

STEP 7 | Utilisez la documentation et d'autres ressources de Palo Alto Networks pour en savoir plus sur le décryptage et pour rechercher des informations :

- Le Guide de l'administrateur PAN-OS fournit des informations détaillées sur les pare-feu de nouvelle génération de Palo Alto Networks.
- La communauté Palo Alto Networks Live dispose d'un Liste des ressources de déchiffrement d'articles sur la configuration, l'installation et l'administration du déchiffrement.
- Pour trouver les certificats intermédiaires manquants, visitez Laboratoires SSL (Qualys).
- Pour savoir quelles suites de chiffrement un serveur prend en charge, visitez Qualys SSL Labs page de test SSL du serveur.
- Pour consulter les statistiques à jour sur les pourcentages de différents chiffrements et protocoles utilisés sur les 150 000 sites les plus populaires au monde afin de voir les tendances et de comprendre l'étendue de la prise en charge mondiale des chiffrements et des protocoles plus sécurisés, visitez Qualys SSL Labs Page SSL Pulse.