Décryptage SSL/TLS

Publié: 2023-09-19

Le cryptage des données sensibles est un élément essentiel de la protection des actifs de votre réseau. Cependant, le cryptage réduit également la visibilité du réseau pour la cybersécurité et la criminalistique. Le trafic crypté étant un vecteur de plus en plus courant d'activités malveillantes, nous vous recommandons de configurer le système ExtraHop pour qu'il décrypte votre trafic SSL/TLS critique afin de permettre des détections permettant d'identifier les comportements suspects et les attaques potentielles.

Les conditions suivantes doivent être remplies pour le décryptage SSL/TLS :

- Le trafic de votre serveur SSL/TLS doit être chiffré avec une suite de chiffrement prise en charge.
- Vous ne pouvez décrypter que le trafic des services que vous fournissez et contrôlez sur votre réseau.

Types de chiffrement

Lorsqu'un client établit une connexion avec un serveur via SSL/TLS, une série d'échanges identifie la suite de chiffrement qui comprend l'ensemble des algorithmes permettant de chiffrer les données et d'en authentifier l'intégrité.

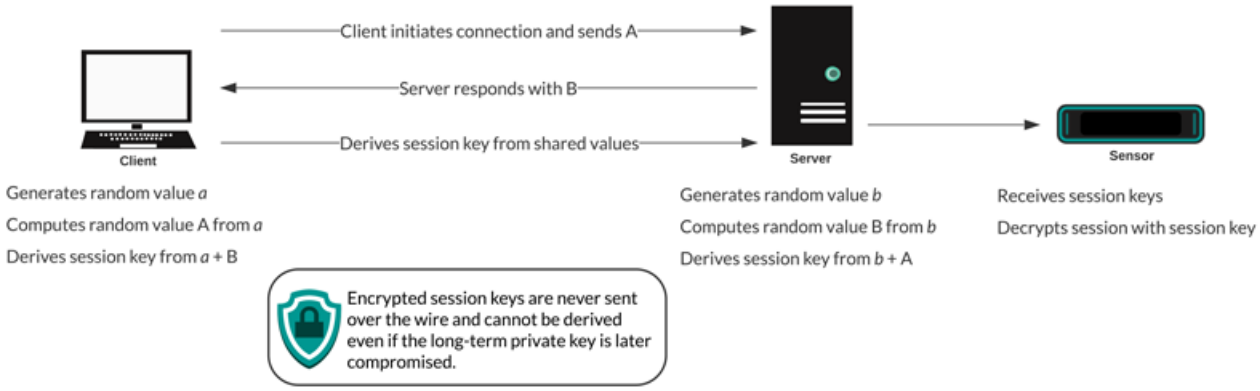
Vous pouvez configurer le système ExtraHop pour qu'il déchiffre le trafic SSL/TLS en fonction du type de suite de chiffrement pris en charge avec lequel la connexion réseau est sécurisée.

Vidéo: En savoir plus sur le cryptage.

Transfert de clé de session

Lorsque le transfert de clé de session est activé sur le système ExtraHop, un agent léger peut être installé sur le serveur pour transférer les clés de session au système, qui est alors en mesure de déchiffrer le trafic SSL/TLS correspondant. La communication entre le transmetteur de clés et le système est cryptée avec TLS 1.2.

Les suites de chiffrement Perfect Forward Secrecy (PFS) dérivent mutuellement une clé de session par une série d'échanges entre le client et le serveur - seuls le client et le serveur connaissent la clé de session, qui n'est jamais envoyée sur le réseau filaire. Même si la clé à long terme du serveur est compromise, la clé de session éphémère reste sécurisée.



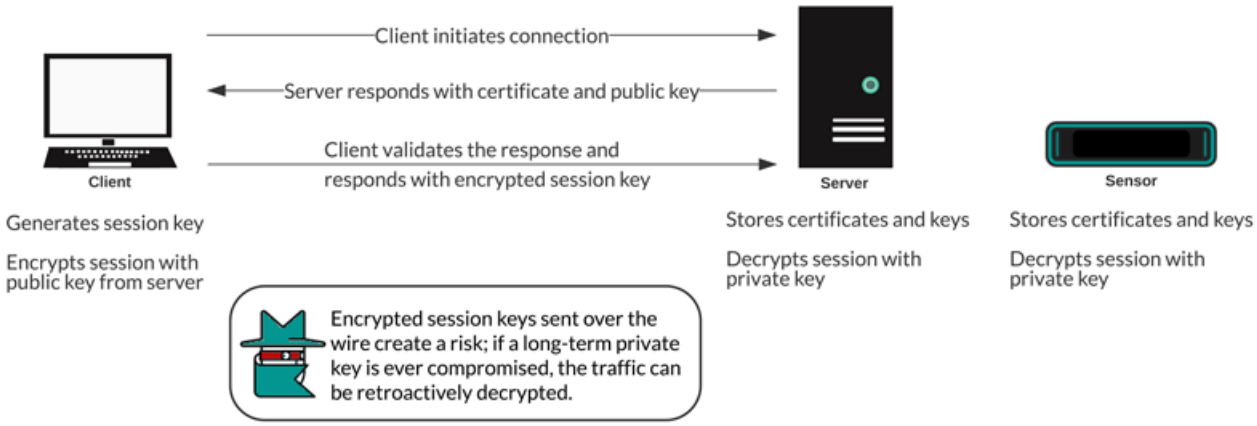
Certificats et clés

Lorsqu'un certificat et une clé privée pour les suites de chiffrement prises en charge sont téléchargés vers un système ExtraHop, ce dernier est en mesure de déchiffrer le trafic SSL/TLS correspondant.

Note: TLS 1.2 et les versions antérieures prennent en charge RSA pour l'échange de clés, ce qui n'est pas le cas de TLS 1.3.

Les suites de chiffrement pour RSA peuvent être déchiffrées à l'aide d'un certificat de serveur et d'une clé privée. Lorsqu'un client se connecte à un serveur via SSL/TLS, le serveur répond par un certificat qui valide son identité et partage la clé publique. Le client génère et crypte une clé de session qu'il envoie au serveur. Le client vérifie que le certificat est signé par une autorité de certification de confiance et que le serveur correspond au domaine demandé.

Étant donné que la clé de session cryptée est envoyée sur le réseau filaire pendant la poignée de main et que la clé privée est conservée à long terme sur le serveur, toute personne ayant accès au trafic, au certificat du serveur et à la clé privée peut déduire la clé de session et décrypter les données. Les équipes responsables du cryptage de leur trafic peuvent hésiter à partager les clés privées avec d'autres appareils du réseau afin de minimiser les risques.



Meilleures pratiques

Voici quelques bonnes pratiques à prendre en compte lors de la mise en œuvre du cryptage SSL/TLS.

- Désactiver SSLv2 pour réduire les problèmes de sécurité au niveau du protocole.
- Désactiver le protocole SSLv3, sauf s'il est nécessaire pour assurer la compatibilité avec les anciens clients.
- Désactiver la compression SSL pour éviter la faille de sécurité CRIME.
- Désactiver les tickets de session, à moins que vous ne connaissiez les risques susceptibles d'affaiblir le Perfect Forward Secrecy.
- Configurer le serveur pour qu'il sélectionne la suite de chiffrement dans l'ordre de ses préférences.
- Notez que le transfert de clé de session est la seule option pour le trafic chiffré avec TLS 1.3.

Quel trafic décrypter ?

Le trafic que vous souhaitez inspecter est susceptible de contenir des données sensibles, c'est pourquoi le système ExtraHop n'écrit pas les données utiles déchiffrées sur le disque. Le système ExtraHop analyse le trafic en temps réel et rejette ensuite la clé de session, à moins qu'une appliance Trace ne soit déployée pour capturer les paquets en continu. En option, le système peut être configuré pour stocker la clé de session avec les paquets, ce qui constitue une approche plus sûre que le partage de la clé privée à long terme avec les analystes.

Voici quelques exemples du type de données que vous devriez envisager de déchiffrer avec le système ExtraHop :

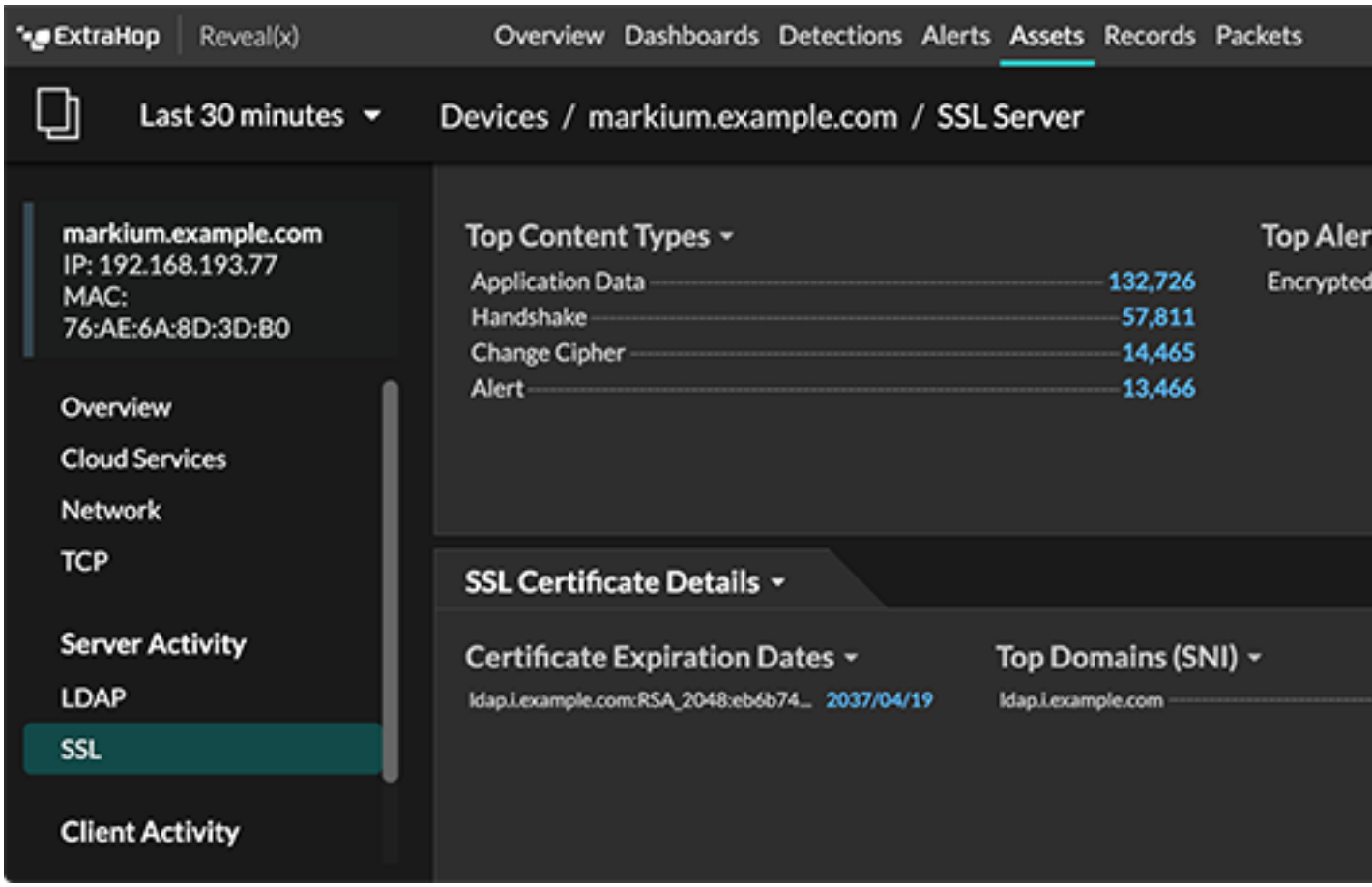
- Le décryptage du trafic HTTP sécurisé (HTTPS) échangé entre un serveur web et un client par le biais d'une connexion SSL/TLS peut révéler des attaques d'applications web telles que l'injection SQL (SQLi) et le cross-site scripting (XSS), qui figurent parmi les risques de sécurité des applications web les plus

courants de la liste Top 10 de l'OWASP. Le décryptage du trafic HTTPS peut également mettre en évidence des mécanismes d'exploitation, par exemple un URI ou un paramètre de requête malveillant, pour des vulnérabilités et des expositions courantes (CVE) dans les applications et les serveurs web.

- Le décryptage du trafic LDAP sécurisé (LDAPS) échangé entre un serveur LDAP et un client par le biais d'une connexion SSL/TLS peut révéler des activités de reconnaissance. Par exemple, l'outil d'attaque BloodHound chiffre les requêtes LDAP avec SSL/TLS (ainsi que Kerberos ou NTLM) pour collecter de grandes listes d'objets Active Directory à des fins de reconnaissance. Le décryptage du trafic LDAPS peut également mettre en évidence le mécanisme d'exploitation du CVE critique appelé Log4Shell.
- Le décryptage du trafic des bases de données MySQL, PostgreSQL, MS SQL Server ou Oracle échangé entre un serveur de base de données et un client par le biais d'une connexion SSL/TLS peut faire apparaître des instructions ou des commandes malveillantes destinées à supprimer, modifier ou lire des données.
- Le décryptage du trafic dont vous pourriez avoir besoin pour un audit médico-légal vous aide à respecter les réglementations en matière de conformité ou à enquêter sur les incidents survenant sur des systèmes critiques, tels que les bases de données de vos clients, les systèmes abritant des propriétés intellectuelles de valeur ou les serveurs fournissant des services réseau essentiels.

Vous pouvez également identifier le type de trafic crypté pour un périphérique spécifique découvert par le système ExtraHop. Recherchez le périphérique dans le système et accédez à la page de détails du périphérique.

Dans le volet de gauche, cliquez sur **SSL** dans la section Activité du serveur. Dans le volet central, faites défiler jusqu'au tableau Suites de chiffrement les plus utilisées.



Comment décrypter votre trafic SSL

La manière dont vous décryptez le trafic SSL dépend de la suite de chiffrement et de l'implémentation de votre serveur.

Note: Consultez les suites de chiffrement prises en charge pour savoir quelles suites de chiffrement peuvent être déchiffrées et quelles sont leurs exigences.

Si votre trafic SSL est crypté avec des suites de chiffrement PFS, vous pouvez installer le logiciel ExtraHop Session Key Forwarder sur chaque serveur ayant le trafic SSL que vous souhaitez décrypter. La clé de session est transmise au système ExtraHop et le trafic peut être déchiffré. Notez que vos serveurs doivent prendre en charge le logiciel de transfert de clé de session.

- Installer le redirecteur de clés de session ExtraHop sur un serveur Windows
- Installer le redirecteur de clés de session ExtraHop sur un serveur Linux

Si vous disposez d'un équilibreur de charge F5, vous pouvez partager les clés de session via l'équilibreur et éviter d'installer le logiciel de transfert de clés de session sur chaque serveur.

- Transfert de clé de session à partir d'un F5 LTM

Si votre trafic SSL est crypté avec des suites de chiffrement RSA, vous pouvez toujours installer le logiciel de transfert de clé de session sur vos serveurs (recommandé). Vous pouvez également télécharger le certificat et la clé privée vers le système ExtraHop.

- Déchiffrer le trafic SSL avec des certificats et des clés privées

Nous vous recommandons de ne décrypter que le trafic dont vous avez besoin. Vous pouvez configurer le système ExtraHop pour qu'il ne déchiffre que des protocoles spécifiques et qu'il mappe le trafic des protocoles sur des ports non standard.

- Ajouter des protocoles cryptés
- Ajouter un port global au mappage de protocole

Décryptage des paquets pour les audits judiciaires

Si vous avez configuré une appliance Trace ou un autre packetstore, vous pouvez stocker des clés de session sur l'appliance Trace et télécharger des clés de session avec des captures de paquets afin de décrypter les paquets dans un outil d'analyse de paquets tel que Wireshark. Ces options vous permettent de décrypter le trafic en toute sécurité sans partager les clés privées à long terme avec les analystes.

Le système ne stocke que les clés de session des paquets sur le disque ; au fur et à mesure que les paquets sont écrasés, les clés de session stockées correspondantes sont supprimées. Seules les clés de session du trafic décrypté sont envoyées à l'appliance Trace pour y être stockées. Le système ExtraHop envoie la clé de session avec les informations de flux associées à l'appliance Trace. Si un utilisateur dispose des privilèges relatifs aux paquets et aux clés de session, la clé de session est fournie lorsqu'il existe un flux correspondant dans la plage de temps demandée. Les clés de session étrangères ne sont pas stockées et il n'y a pas de limite au nombre de clés de session que le système ExtraHop peut recevoir.

Nous vous recommandons de faire preuve de prudence lorsque vous accordez des privilèges aux utilisateurs du système ExtraHop. Vous pouvez spécifier les privilèges qui permettent aux utilisateurs d'afficher et de télécharger des paquets ou d'afficher et de télécharger des paquets et des clés de session stockées. Les clés de session stockées ne doivent être accessibles qu'aux utilisateurs qui doivent avoir accès au trafic décrypté sensible. Bien que le système ExtraHop n'écrive pas les données utiles décryptées sur le disque, l'accès aux clés de session permet de décrypter le trafic correspondant. Pour garantir la sécurité de bout en bout, les clés de session sont cryptées lorsqu'elles sont déplacées d'un appareil à l'autre et lorsqu'elles sont stockées sur le disque.

- Stocker les clés de session SSL sur les appliances Trace connectées
- Télécharger les clés de session avec les captures de paquets