Déchiffrement SSL/TLS

Publié: 2023-10-01

Le chiffrement des données sensibles est essentiel à la protection des actifs de votre réseau ; toutefois, le chiffrement réduit également la visibilité sur le réseau à des fins de cybersécurité et de criminalistique. Le trafic chiffré étant un vecteur de plus en plus courant d' activités malveillantes, nous vous recommandons de configurer le système ExtraHop pour déchiffrer 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 déchiffrement SSL/TLS :

- Le trafic de votre serveur SSL/TLS doit être chiffré à l'aide d'un suite de chiffrement prise en charge.
- Vous ne pouvez déchiffrer le trafic que pour les services que vous fournissez et contrôlez sur votre réseau.

Types de chiffrement

Lorsqu'un client établit une connexion à un serveur via SSL/TLS, une série d'échanges d'établissement dune liaison identifie la suite de chiffrement qui inclut l'ensemble d'algorithmes qui crypte les données et authentifie l'intégrité des données.

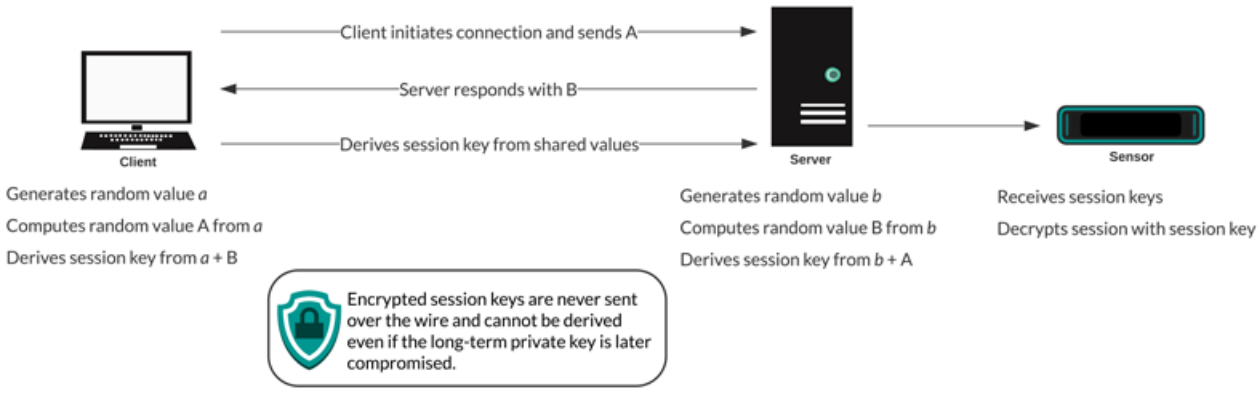
Vous pouvez configurer le système ExtraHop pour déchiffrer le trafic SSL/TLS en fonction du type de suite de chiffrement prise en charge avec lequel la connexion réseau est sécurisée.

Vidéo: En savoir plus sur le chiffrement.

Transfert de clé de session

Lorsque le transfert des clés 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 et le système est capable de déchiffrer le trafic SSL/TLS associé. La communication entre le transmetteur de clés et le système est cryptée avec le protocole TLS 1.2.

Les suites de chiffrement PFS (Perfect Forward Secrecy) dérivent mutuellement une clé de session par le biais d'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 de serveur à long terme est compromise, la clé de session éphémère reste sécurisée.



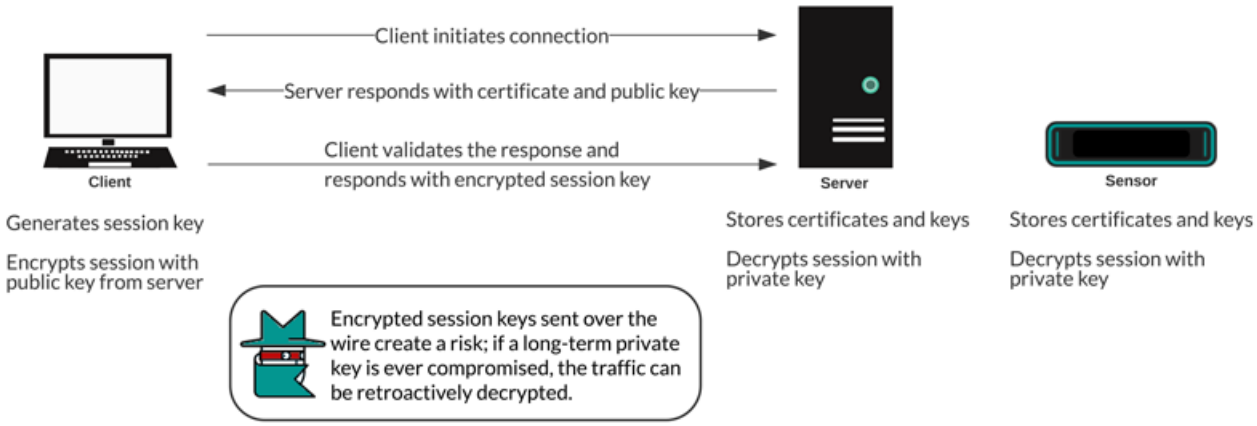
Certificats et clés

Lorsqu'un certificat et une clé privée pour suites de chiffrement prises en charge sont téléchargés sur un système ExtraHop, le système est capable de déchiffrer le trafic SSL/TLS associé.

Note: TLS 1.2 et versions antérieures prennent en charge RSA pour l'échange de clés, mais pas 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 avec un certificat qui valide son identité et partage la clé publique. Le client génère et chiffre une clé de session et envoie la clé de session chiffrée au serveur. Le client confirme que le certificat est signé par une autorité de certification fiable et que le serveur correspond au domaine demandé.

Étant donné que la clé de session cryptée est envoyée sur le réseau filaire pendant l'établissement dac.une liaison 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 obtenir la clé de session et déchiffrer les données. Les équipes chargées de chiffrer leur trafic peuvent hésiter à partager leurs clés privées avec d'autres appareils du réseau afin de minimiser les risques.



Les meilleures pratiques

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

- Désactivez le protocole SSLv2 pour réduire les problèmes de sécurité au niveau du protocole.
- Désactivez SSLv3, sauf si cela est nécessaire pour des raisons de compatibilité avec les anciens clients.
- Désactivez la compression SSL pour éviter la vulnérabilité de sécurité CRIME.
- Désactivez les tickets de session à moins que vous ne connaissiez les risques susceptibles de fragiliser le secret de transmission parfait.
- Configurez le serveur pour sélectionner la suite de chiffrement dans l'ordre de préférence du serveur.
- 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. Le système ExtraHop n'écrit donc pas de données de charge utile déchiffrées sur le disque. Le système ExtraHop analyse le trafic en temps réel, puis supprime la clé de session, sauf si une appliance Trace est déployée pour une capture continue des paquets. 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 des analystes.

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

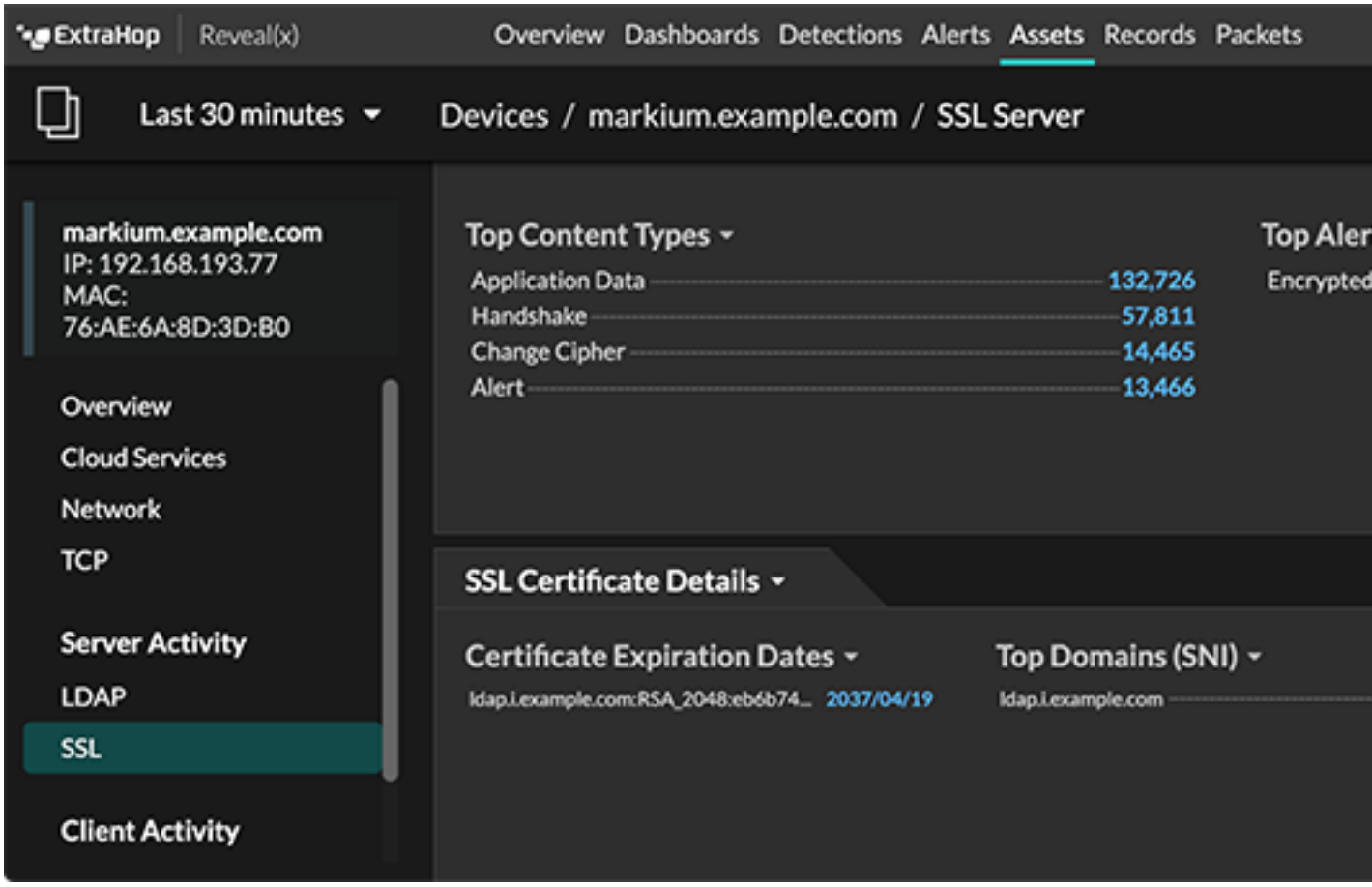
- Le déchiffrement du trafic HTTP sécurisé (HTTPS) échangé entre un serveur Web et un client via une connexion SSL/TLS peut provoquer des attaques d'applications Web telles que l' injection SQL (SQLi) et les scripts intersites (XSS), qui figurent parmi les risques de sécurité des applications Web les plus courants sur le Top 10 de l'OWASP liste. Le déchiffrement du trafic HTTPS peut également faire

apparaître des mécanismes d'exploitation, tels qu'un URI ou un paramètre de requête malveillant, à l'origine de vulnérabilités et d'expositions (CVE) courantes dans les applications Web et les serveurs.

- Le déchiffrement du trafic LDAP sécurisé (LDAPS) échangé entre un serveur LDAP et un client via une connexion SSL/TLS peut faire apparaître une activité 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 déchiffrement du trafic LDAPS peut également faire apparaître le mécanisme d'exploitation du CVE critique appelé Log 4 Shell.
- Le déchiffrement du trafic de base de données MySQL, PostgreSQL, MS SQL Server ou Oracle échangé entre un serveur de base de données et un client via une connexion SSL/TLS peut faire apparaître des instructions ou des commandes malveillantes destinées à supprimer, modifier ou lire des données.
- Le déchiffrement du trafic dont vous pourriez avoir besoin à des fins d'audit judiciaire permet de respecter les réglementations en matière de conformité ou d'enquêter sur des incidents sur des systèmes critiques, tels que les bases de données de vos clients, les systèmes hébergeant de précieuses propriétés intellectuelles ou les serveurs fournissant des services réseau essentiels.

Vous pouvez également identifier le type de trafic crypté pour un équipement spécifique découvert par le système ExtraHop. Trouvez l'équipement dans le système et accédez à la page détaillée de l'équipement.

Dans le volet de gauche, cliquez sur **SLL** dans la section Activité du serveur. Dans le volet central, faites défiler l'écran jusqu'au graphique Top Cipher Suites.



Comment déchiffrer votre trafic SSL

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

Note: Voir 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 à l'aide de suites de chiffrement PFS, vous pouvez installer le logiciel de transfert de clé de session ExtraHop sur chaque serveur hébergeant le trafic SSL que vous souhaitez déchiffrer. 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 clés de session.

- Installez le redirecteur de clé de session ExtraHop sur un serveur Windows
- Installez le redirecteur de clé 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 depuis un F5 LTM

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

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

Nous vous recommandons de ne déchiffrer que le trafic dont vous avez besoin. Vous pouvez configurer le système ExtraHop pour déchiffrer uniquement des protocoles spécifiques et mapper le trafic des protocoles à des ports non standard.

- Ajouter des protocoles chiffrés
- Ajouter un port global au mappage des protocoles

Décryptage de paquets pour des audits médico-légaux

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

Le système ne stocke les clés de session que pour les paquets sur disque. Lorsque les paquets sont remplacés, les clés de session stockées associées sont supprimées. Seules les clés de session pour le trafic déchiffré sont envoyées à l'appliance Trace pour être stockées. Le système ExtraHop envoie la clé de session avec les informations de flux associées à l'appliance Trace. Si un utilisateur dispose de 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 superflues ne sont pas stockées et le nombre de clés de session que le système ExtraHop peut recevoir n'est pas limité.

Nous vous recommandons de faire preuve de prudence lorsque vous accordez des privilèges aux utilisateurs du système ExtraHop. Vous pouvez définir les privilèges qui permettent aux utilisateurs de visualiser et de télécharger des paquets ou de visualiser 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 déchiffré sensible. Bien que le système ExtraHop n'enregistre pas de données de charge utile déchiffrées sur le disque, l'accès aux clés de session permet de déchiffrer le trafic associé. Pour garantir la sécurité de bout en bout, les clés de session sont chiffrées lors du déplacement entre les appliances ainsi que lorsque les clés sont stockées sur disque.

- Stockez les clés de session SSL sur les appareils Trace connectés
- Télécharger les clés de session avec captures de paquets