Décryptage TLS

Publié: 2024-11-04

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

- Le trafic de votre serveur 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.

Performances de déchiffrement TLS

Tous les capteurs ExtraHop prennent en charge le déchiffrement TLS. Les performances varient en fonction de la manière dont vous avez implémenté le déchiffrement TLS sur votre réseau et des caractéristiques du trafic de votre réseau. Les capteurs ExtraHop sont soumis à des tests HTTPS pour s'assurer qu'ils sont capables de déchiffrer le trafic sans limitation.

Types de chiffrement

Lorsqu'un client initie une connexion à un serveur via le protocole TLS, une série d'échanges de liaison permet d'identifier la suite de chiffrement qui inclut l'ensemble d'algorithmes qui chiffre les données et authentifie leur intégrité .

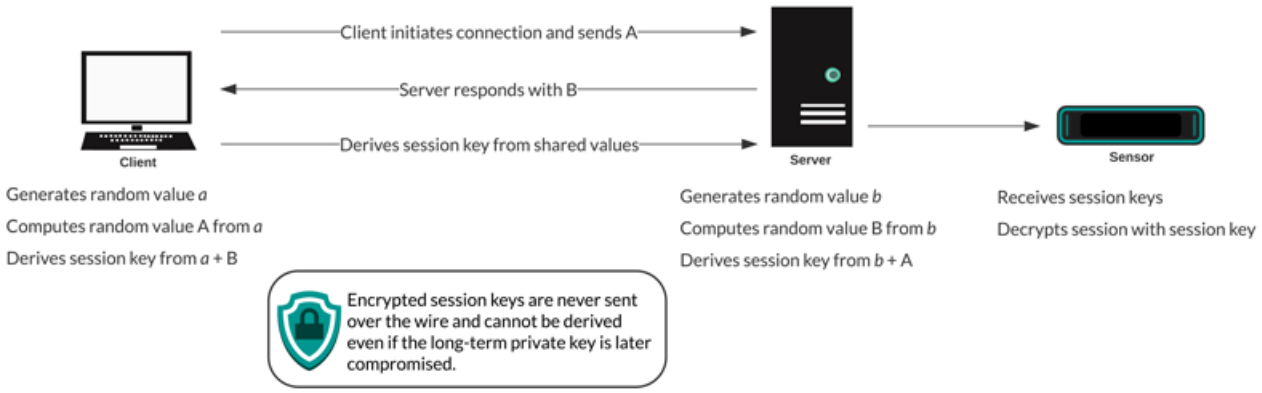
Vous pouvez configurer le système ExtraHop pour déchiffrer le trafic TLS en fonction du type suite de chiffrement prise en charge avec laquelle la connexion réseau est sécurisée.

Vidéo: En savoir plus sur le chiffrement.

Transfert de clés de session

Lorsque le transfert de clés de session est activé sur le système ExtraHop, un agent léger peut être installé sur le serveur pour transmettre les clés de session au système et celui-ci est en mesure de déchiffrer le trafic TLS associé. La communication entre le transitaire de clés et le système est cryptée à l'aide du 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.



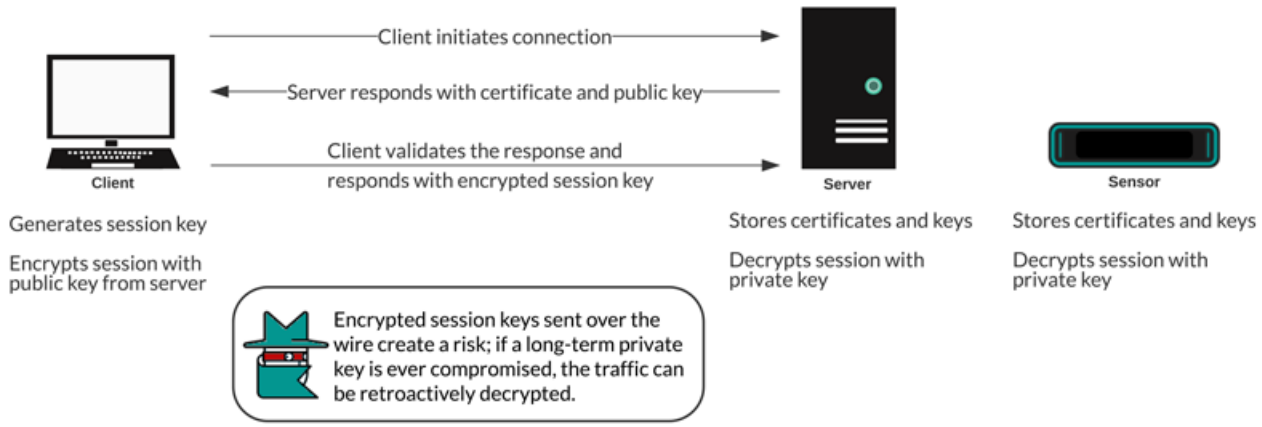
Certificats et clés

Quand un certificat et une clé privée pour suites de chiffrement prises en charge sont chargés sur un système ExtraHop, le système est capable de déchiffrer le trafic 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 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 cryptée 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 chiffrée est envoyée sur le réseau filaire pendant l'établissement dclinaison 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 des 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 TLS .

- Désactivez SSLv2 pour réduire les problèmes de sécurité au niveau du protocole.
- Désactivez le protocole 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 soyez au courant des risques susceptibles d'affaiblir la fonction Perfect Forward Secrecy.
- Configurez le serveur pour sélectionner la suite de chiffrement dans l'ordre des préférences du serveur.
- Notez que le transfert de clé de session est la seule option pour le trafic chiffré avec TLS 1.3.

Quel trafic déchiffrer

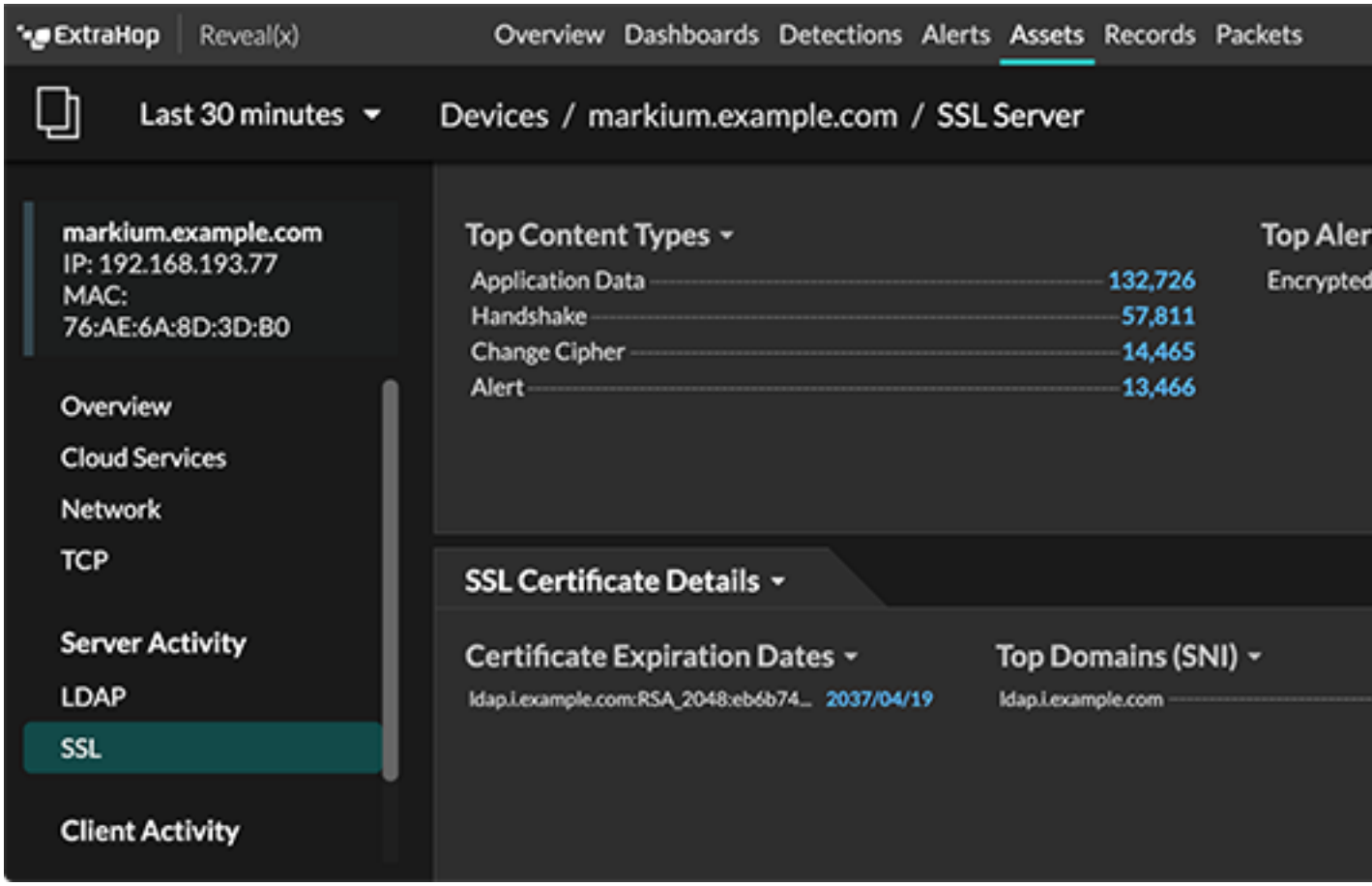
Le trafic que vous souhaitez inspecter est susceptible de contenir des données sensibles. Le système ExtraHop n'écrit donc pas les données de charge utile déchiffrées sur le disque. Le système ExtraHop analyse le trafic en temps réel, puis supprime la clé de session à moins qu'une appliance Trace ne soit déployée pour une capture continue des paquets. Le système peut éventuellement 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 (HTTPS) sécurisé échangé entre un serveur Web et un client via une connexion TLS peut faire apparaître des attaques contre les applications Web telles que l' injection SQL (SQLi) et le cross-site scripting (XSS), qui figurent parmi les risques de sécurité les plus courants pour les applications Web sur Top 10 de l'OWASP liste. Le déchiffrement du trafic HTTPS peut également mettre en évidence des mécanismes d'exploitation, tels qu'un URI ou un paramètre de requête malveillant, pour détecter les vulnérabilités et les expositions (CVE) courantes dans les applications et les serveurs Web.
- Le déchiffrement du trafic LDAP sécurisé (LDAPS) échangé entre un serveur LDAP et un client via une connexion TLS peut révéler une activité de reconnaissance. Par exemple, l'outil d'attaque BloodHound chiffre les requêtes LDAP avec 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 bases de données et un client via une connexion 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 de conformité ou d'enquêter sur des incidents sur des systèmes critiques, tels que les bases de données de vos clients, les systèmes qui hébergent une propriété intellectuelle importante ou les serveurs fournissant des services réseau critiques.

Vous pouvez également identifier le type de trafic chiffré 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 **TLS** dans la section Activité du serveur. Dans le volet central, accédez au graphique des meilleures suites de chiffrement.



Comment déchiffrer votre trafic TLS

La façon dont vous déchiffrez le trafic TLS 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 TLS est chiffré à l'aide des suites de chiffrement PFS, vous pouvez installer le logiciel de redirection de clés de session ExtraHop sur chaque serveur hébergeant le trafic TLS 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.

- Installation du redirecteur de clés de session ExtraHop sur un serveur Windows
- Installation du 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 depuis un F5 LTM

Si votre trafic TLS 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 dans le système ExtraHop

- Déchiffrez le trafic TLS à l'aide de certificats et de 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 protocolaire vers des ports non standard.

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

Décryptage des paquets pour les audits judiciaires

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 vous pouvez 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 de clés privées à long terme avec des analystes.

Le système ne stocke que les clés de session pour les paquets sur le disque. Au fur et à mesure que 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 à des fins de stockage. Le système ExtraHop envoie la clé de session avec les informations de flux associées à l'appliance Trace. Si un utilisateur possède des privilèges de paquets et de clé 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 est illimité.

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 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 devraient être accessibles qu'aux utilisateurs qui devraient avoir accès au trafic déchiffré sensible. Bien que le système ExtraHop n'enregistre pas les données de charge utile déchiffrées sur le disque, l'accès aux clés de session permet de déchiffrer le trafic associé. Pour garantir une sécurité de bout en bout, les clés de session sont cryptées lors du transfert entre les appliances ainsi que lorsque les clés sont stockées sur disque.

- Stockez les clés de session TLS sur les appliances Trace connectées
- Télécharger les clés de session avec captures de paquets