TLS-Entschlüsselung

Veröffentlicht: 2024-11-03

Die Verschlüsselung sensibler Daten ist ein wichtiger Bestandteil des Schutzes Ihrer Netzwerkressourcen. Die Verschlüsselung verringert jedoch auch die Sichtbarkeit des Netzwerks im Hinblick auf Cybersicherheit und Forensik. Da verschlüsselter Datenverkehr ein zunehmend verbreiteter Vektor für bösartige Aktivitäten ist, empfehlen wir Ihnen, das ExtraHop-System so zu konfigurieren, dass es Ihren kritischen TLS-Verkehr entschlüsselt, um Erkennungen zu ermöglichen, die verdächtiges Verhalten und potenzielle Angriffe erkennen können.

Die folgenden Anforderungen müssen für die TLS-Entschlüsselung erfüllt sein:

- Ihr TLS-Serververkehr muss mit einem verschlüsselt sein unterstützte Verschlüsselungssuite.
- Sie können nur den Datenverkehr für die Dienste entschlüsseln, die Sie in Ihrem Netzwerk bereitstellen und kontrollieren.

Leistung bei der TLS-Entschlüsselung

Alle ExtraHop-Sensoren unterstützen die TLS-Entschlüsselung. Die Leistung hängt davon ab, wie Sie die TLS-Entschlüsselung in Ihrem Netzwerk implementiert haben, und von den Verkehrseigenschaften Ihres Netzwerks. ExtraHop-Sensoren werden HTTPS-Tests unterzogen, um sicherzustellen, dass sie den Datenverkehr ohne Einschränkungen entschlüsseln können.

Verschlüsselungsarten

Wenn ein Client eine Verbindung zu einem Server über TLS initiiert, identifiziert eine Reihe von Handshake-Austauschen die Verschlüsselungssuite, die den Satz von Algorithmen enthält, die die Daten verschlüsseln und die Datenintegrität authentifizieren.

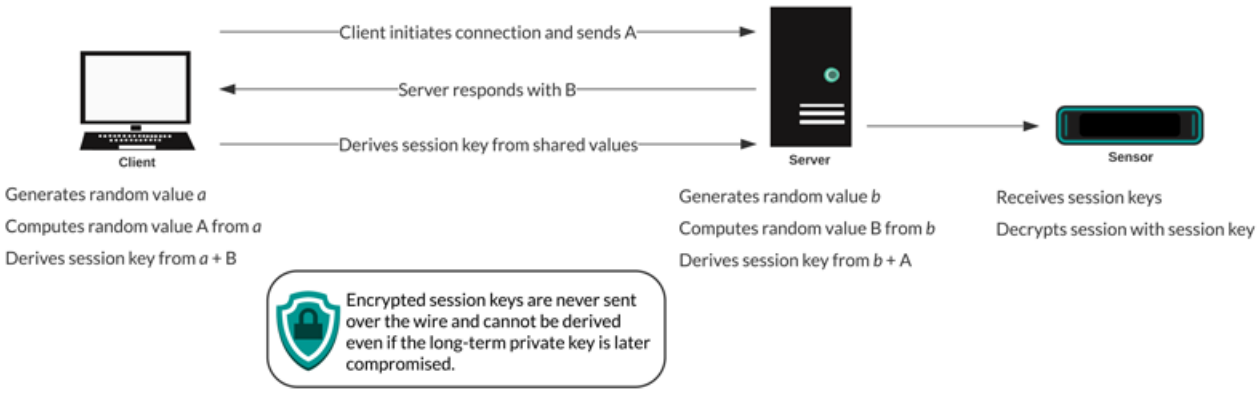
Sie können das ExtraHop-System so konfigurieren, dass TLS-Verkehr basierend auf dem Typ von entschlüsselt wird unterstützte Verschlüsselungssuite mit dem die Netzwerkverbindung gesichert ist.

Video: Erfahren Sie mehr über Verschlüsselung.

Weiterleitung von Sitzungsschlüsseln

Wenn die Weiterleitung von Sitzungsschlüsseln auf dem ExtraHop-System aktiviert ist, kann auf dem Server ein leichter Agent installiert werden, der Sitzungsschlüssel an das System weiterleitet, und das System kann den entsprechenden TLS-Verkehr entschlüsseln. Die Kommunikation zwischen dem Key Forwarder und dem System ist mit TLS 1.2 verschlüsselt.

Perfect Forward Secrecy (PFS) Cipher Suites leiten durch eine Reihe von Austauschen zwischen Client und Server gegenseitig einen Sitzungsschlüssel ab — nur der Client und der Server kennen den Sitzungsschlüssel, der niemals über das Drahtnetz gesendet wird . Selbst wenn der langfristige Serverschlüssel kompromittiert wird, bleibt der kurzlebige Sitzungsschlüssel sicher.



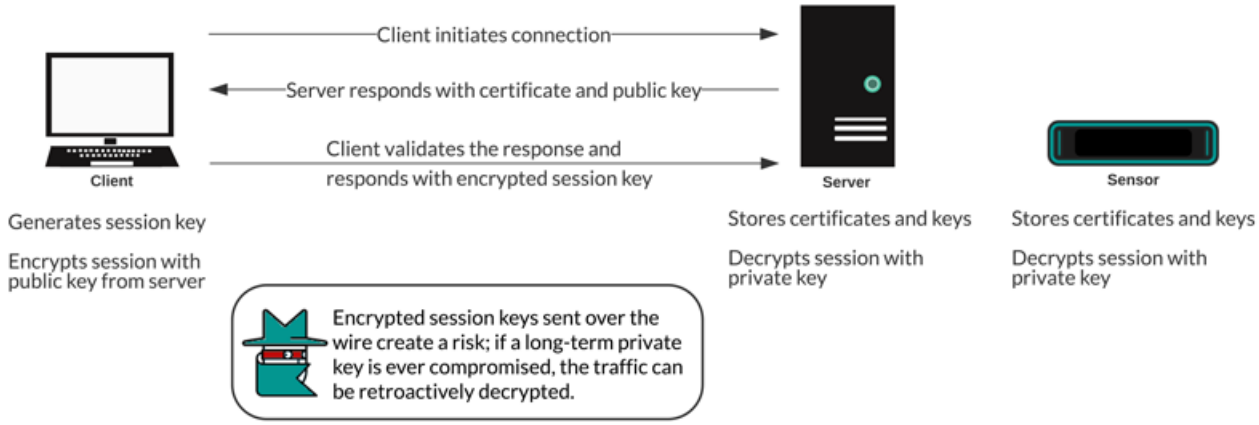
Zertifikate und Schlüssel

Wenn ein Zertifikat und ein privater Schlüssel für unterstützte Cipher Suites werden auf ein ExtraHop-System hochgeladen, das System ist in der Lage, den zugehörigen TLS-Verkehr zu entschlüsseln.

Hinweis: TLS 1.2 und frühere Versionen unterstützen RSA für den Schlüsselaustausch, TLS 1.3 jedoch nicht.

Cipher Suites für RSA können mit einem Serverzertifikat und einem privaten Schlüssel entschlüsselt werden. Wenn ein Client über TLS eine Verbindung zu einem Server herstellt, antwortet der Server mit einem Zertifikat, das seine Identität bestätigt und den öffentlichen Schlüssel teilt. Der Client generiert und verschlüsselt einen Sitzungsschlüssel und sendet den verschlüsselten Sitzungsschlüssel an den Server. Der Client bestätigt, dass das Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle signiert ist und dass der Server mit der angeforderten Domain übereinstimmt.

Da der verschlüsselte Sitzungsschlüssel während des Handschlag über das Drahtnetz gesendet wird und der private Schlüssel langfristig auf dem Server gespeichert wird, kann jeder, der Zugriff auf den Datenverkehr, das Serverzertifikat und den privaten Schlüssel hat, den Sitzungsschlüssel ableiten und die Daten entschlüsseln. Teams, die für die Verschlüsselung ihres Datenverkehrs verantwortlich sind, zögern möglicherweise, private Schlüssel mit anderen Geräten im Netzwerk zu teilen, um das Risiko zu minimieren.



Bewährte Verfahren

Hier sind einige bewährte Methoden, die Sie bei der Implementierung der TLS-Verschlüsselung berücksichtigen sollten.

- Schalten Sie SSLv2 aus, um Sicherheitsprobleme auf Protokollebene zu reduzieren.
- Schalten Sie SSLv3 aus, es sei denn, es ist für die Kompatibilität mit älteren Clients erforderlich.
- Schalten Sie die SSL-Komprimierung aus, um die CRIME-Sicherheitslücke zu vermeiden.

- Deaktivieren Sie Sitzungstickets, sofern Sie nicht mit den Risiken vertraut sind, die PFS schwächen könnten.
- Konfigurieren Sie den Server so, dass er die Verschlüsselungssuite in der Reihenfolge der Servereinstellungen auswählt.
- Beachten Sie, dass die Weiterleitung von Sitzungsschlüsseln die einzige Option für mit TLS 1.3 verschlüsselten Verkehr ist.

Welcher Verkehr muss entschlüsselt werden

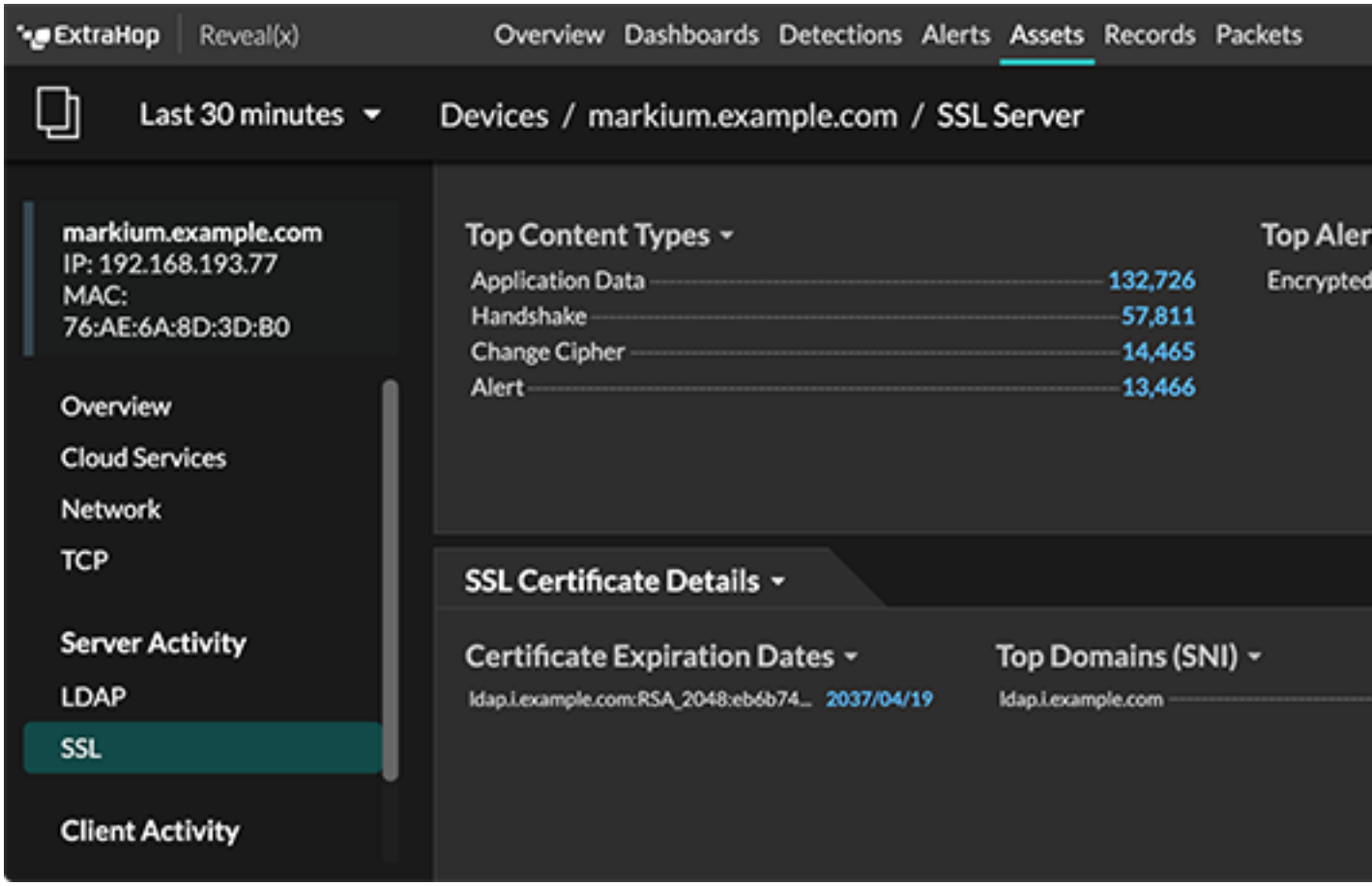
Der Datenverkehr, den Sie überprüfen möchten, enthält wahrscheinlich vertrauliche Daten, sodass das ExtraHop-System keine entschlüsselten Nutzdaten auf die Festplatte schreibt. Das ExtraHop-System analysiert den Datenverkehr in Echtzeit und verwirft dann den Sitzungsschlüssel, sofern keine Trace-Appliance für die kontinuierliche PCAP eingesetzt wird. Optional kann das System so konfiguriert werden, dass der Sitzungsschlüssel zusammen mit den Paketen gespeichert wird. Dies ist sicherer, als den langfristigen privaten Schlüssel mit Analysten zu teilen.

Hier sind einige Beispiele für die Art von Daten, die Sie mit dem ExtraHop-System entschlüsseln sollten:

- Durch die Entschlüsselung von sicherem HTTP-Verkehr (HTTPS), der zwischen einem Server und einem Client über eine TLS-Verbindung ausgetauscht wird, können Angriffe auf Webanwendung wie SQL Injection (SQLi) und Cross-Site Scripting (XSS) auftreten, die zu den häufigsten Sicherheitsrisiken für Webanwendung auf dem OWASP Top 10 Liste. Bei der Entschlüsselung des HTTPS-Datenverkehrs können auch Exploit-Mechanismen zum Vorschein kommen, z. B. ein bösartiger URI oder ein Abfrageparameter, für häufig auftretende Sicherheitslücken und Exposures (CVEs) in Webanwendungen und Servern.
- Das Entschlüsseln von sicherem LDAP-Verkehr (LDAPS), der zwischen einem LDAP-Server und einem Client über eine TLS-Verbindung ausgetauscht wird, kann Aufklärungsaktivitäten aufdecken. Beispielsweise verschlüsselt das BloodHound-Angriffstool LDAP-Abfragen mit TLS (sowie Kerberos oder NTLM), um große Listen von Active Directory Directory-Objekten zur Erkennung zu sammeln. Beim Entschlüsseln des LDAPS-Datenverkehrs kann auch der Exploit-Mechanismus für das kritische CVE zum Vorschein kommen, der als Log4-Shell.
- Beim Entschlüsseln des MySQL-, PostgreSQL-, MS SQL Server- oder Oracle-Datenbankverkehrs, der zwischen einem Datenbankserver und einem Client über eine TLS-Verbindung ausgetauscht wird, können böswillige Anweisungen oder Befehle auftauchen, die darauf abzielen, Daten zu löschen, zu ändern oder zu lesen.
- Die Entschlüsselung des Datenverkehrs, den Sie möglicherweise für forensische Prüfungen benötigen, hilft bei der Einhaltung von Compliance-Vorschriften oder bei der Untersuchung von Vorfällen auf kritischen Systemen — z. B. Ihren Kundendatenbanken, Systemen, die wertvolles geistiges Eigentum enthalten, oder Servern, die wichtige Netzwerkdienste bereitstellen.

Sie können auch die Art des verschlüsselten Datenverkehrs für ein bestimmtes Gerät identifizieren, das vom ExtraHop-System erkannt wurde. Finde das Gerät im System und navigieren Sie zur Gerätedetailseite.

Klicken Sie im linken Bereich auf **TLS** im Abschnitt Serveraktivität. Scrollen Sie im mittleren Bereich zum Diagramm Top Cipher Suites.



So entschlüsseln Sie Ihren TLS-Verkehr

Wie Sie den TLS-Verkehr entschlüsseln, hängt von der Verschlüsselungssuite und Ihrer Serverimplementierung ab.

Hinweis: Siehe unterstützte Cipher Suites um zu erfahren , welche Cipher-Suites entschlüsselt werden können und welche Anforderungen sie haben.

Wenn Ihr TLS-Verkehr mit PFS-Cipher Suites verschlüsselt ist, können Sie die ExtraHop Session Key Forwarder-Software auf jedem Server installieren, auf dem sich der TLS-Verkehr befindet, den Sie entschlüsseln möchten. Der Sitzungsschlüssel wird an das ExtraHop-System weitergeleitet und der Verkehr kann entschlüsselt werden. Beachten Sie, dass Ihre Server die Sitzungsschlüsselweiterleitungssoftware unterstützen müssen.

- Installieren Sie den ExtraHOP Session Key Forwarder auf einem Windows-Server
- Installieren Sie den ExtraHop Session Key Forwarder auf einem Linux-Server

Wenn Sie einen F5-Load Balancer haben, können Sie Sitzungsschlüssel über den Balancer gemeinsam nutzen und vermeiden, die Sitzungsschlüsselweiterleitungssoftware auf jedem Server zu installieren.

- Weiterleitung von Sitzungsschlüsseln von einem F5-LTM

Wenn Ihr TLS-Verkehr mit RSA Cipher Suites verschlüsselt ist, können Sie trotzdem die Session Key Forwarder-Software auf Ihren Servern installieren (empfohlen). Alternativ können Sie das Zertifikat und den privaten Schlüssel in das ExtraHop-System hochladen

- Entschlüsseln Sie den TLS-Verkehr mit Zertifikaten und privaten Schlüsseln

Wir empfehlen, nur den Traffic zu entschlüsseln, den Sie benötigen. Sie können das ExtraHop-System so konfigurieren, dass nur bestimmte Protokolle entschlüsselt werden und der Protokollverkehr nicht standardmäßigen Ports zugeordnet wird.

- Verschlüsselte Protokolle hinzufügen
- Globaler Port zur Protokollzuordnung hinzufügen

Pakete für forensische Audits entschlüsseln

Wenn Sie eine Trace-Appliance oder einen anderen Packetstore konfiguriert haben, können Sie Sitzungsschlüssel auf der Trace-Appliance speichern und Sitzungsschlüssel mit Paketerfassung herunterladen, sodass Sie die Pakete in einem Paketanalysetool wie Wireshark entschlüsseln können. Mit diesen Optionen können Sie den Datenverkehr sicher entschlüsseln, ohne langfristige private Schlüssel mit Analysten zu teilen.

Das System speichert nur Sitzungsschlüssel für Pakete auf der Festplatte — wenn Pakete überschrieben werden, werden die zugehörigen gespeicherten Sitzungsschlüssel gelöscht. Nur Sitzungsschlüssel für entschlüsselten Datenverkehr werden zur Speicherung an die Trace-Appliance gesendet. Das ExtraHop-System sendet den Sitzungsschlüssel mit den zugehörigen Flow-Informationen an die Trace-Appliance. Wenn ein Benutzer über Pakete- und Sitzungsschlüsselberechtigungen verfügt, wird der Sitzungsschlüssel bereitgestellt, wenn im abgefragten Zeitraum ein entsprechender Fluss vorliegt. Überflüssige Sitzungsschlüssel werden nicht gespeichert, und die Anzahl der Sitzungsschlüssel, die das ExtraHop-System empfangen kann, ist unbegrenzt.

Wir empfehlen Ihnen, Vorsicht walten zu lassen, wenn Sie ExtraHop-Systembenutzern Rechte gewähren. Sie können die Rechte angeben die es Benutzern ermöglichen, Pakete anzusehen und herunterzuladen oder Pakete und gespeicherte Sitzungsschlüssel anzusehen und herunterzuladen. Gespeicherte Sitzungsschlüssel sollten nur Benutzern zur Verfügung stehen, die Zugriff auf vertraulichen entschlüsselten Datenverkehr haben sollten. Das ExtraHop-System schreibt zwar keine entschlüsselten Nutzdaten auf die Festplatte, aber der Zugriff auf Sitzungsschlüssel ermöglicht die Entschlüsselung des zugehörigen Datenverkehrs. Um eine durchgängige Sicherheit zu gewährleisten, werden die Sitzungsschlüssel verschlüsselt, wenn sie zwischen Appliances übertragen werden und wenn die Schlüssel auf der Festplatte gespeichert werden.

- Speichern Sie TLS-Sitzungsschlüssel auf verbundenen Trace-Appliances
- Laden Sie Sitzungsschlüssel mit Paket herunter