Klarstellung der Leistungsauswirkungen und Best Practices für die SSL/TLS-Verschlüsselung auf FTD

Inhalt

Problem

Ein Benutzer plant, die SSL/TLS-Entschlüsselung auf einem FTD-Gerät (Firewall Threat Defense) zu aktivieren, und muss sich vor der Implementierung der potenziellen Auswirkungen auf die Geräteleistung bewusst sein. Zu den wichtigsten Bedenken gehören:

- Auswirkungen auf Firewall-Durchsatz, Latenz und die Gesamtleistung der Datenverkehrsverarbeitung
- Erwartete Steigerung der CPU- und Speichernutzung nach Aktivierung der Entschlüsselung.
- Dimensionierungsrichtlinien und Benchmarks für bestimmte FTD-Modelle.
- Empfohlene Grenzwerte für gleichzeitig entschlüsselte Sitzungen.
- Best Practices und Voraussetzungen für die Produktionsbereitstellung

Umwelt

- Firepower 4115 Auch andere Hardwareplattformen können betroffen sein.
- FTD Version 7.4.2 (Build 172). Auch andere Softwareversionen können betroffen sein.
- SSL/TLS-Entschlüsselungsfunktion.
- Bereitstellungsplanung für die Produktionsumgebung

Auflösung

Die SSL/TLS-Entschlüsselung erhöht zwar den Verarbeitungsaufwand für die Firepower 4115, die tatsächlichen Auswirkungen hängen jedoch stark davon ab, wie viel Datenverkehr entschlüsselt wird und welche Überprüfung nach der Entschlüsselung durchgeführt wird.

Analyse der Performance-Auswirkungen

Die SSL/TLS-Entschlüsselung hat folgende Auswirkungen:

- Geringerer effektiver Durchsatz.
- Höhere Latenz
- Erhöhte CPU-Auslastung bei Snort/Inspection.
- Eine Zunahme von CPU und Arbeitsspeicher, die ohne eine Analyse des tatsächlichen Datenverkehrsprofils nicht als fester Prozentsatz genau vorhergesagt werden kann.

FPR 4115 Performance-Benchmarks

Veröffentlichte Benchmark-Spezifikationen für die Firepower 4115 von Cisco:

- TLS-Hardware-Entschlüsselungsdurchsatz: 6.5 Gbit/s.
- FW- + AVC-Durchsatz: 33 Gbit/s.
- Maximale Anzahl gleichzeitiger Sitzungen mit AVC: 15 Millionen.
- Maximale Anzahl neuer Verbindungen pro Sekunde mit AVC: 210 K.

Wichtiger Hinweis zur Bedarfsbestimmung: Der TLS-Hardware-Entschlüsselungs-Benchmark von 6,5 Gbit/s basiert auf bestimmten Testbedingungen. Der Produktionsdurchsatz kann niedriger sein, wenn Sie einen großen Prozentsatz des Datenverkehrs entschlüsseln, den entschlüsselten Datenverkehr mithilfe von Intrusion-/Datei-/Malware-Richtlinien überprüfen oder viele kurzlebige

TLS-Sitzungen verarbeiten.

Cisco veröffentlicht keine separate Nummer für "maximale Anzahl gleichzeitiger entschlüsselter Sitzungen" für Firepower 4115 in FTD 7.4.2. In der Praxis wird die Kapazität anhand des Datenverkehrs-Mixes, gleichzeitiger Sitzungen, der Verbindungsrate, der Verschlüsselungssuiten und der Prüfrichtlinienlast validiert.

Empfohlener Produktionsbereitstellungsansatz

Schritt 1: Mit einem begrenzten Pilotprojekt starten

- Aktivieren Sie nicht zu Beginn allgemeine Regeln zum Entschlüsseln aller.
- Beginnen Sie mit ausgewählten Benutzern, Subnetzen oder Zielkategorien.
- Halten Sie die Standardbehandlung bei Datenverkehr, der keiner Überprüfung bedarf, mit der Option "Nicht entschlüsseln" vorsichtig.

Phase 2: Datenverkehr ausschließen, der normalerweise durch Entschlüsselung unterbrochen wird

- Bank-/Finanzstandorte
- Gesundheitsportale.
- Anwendungen, die mit einem Zertifikat verbunden sind.
- Einige Software-as-a-Service (SaaS)- und Endpunkt-Sicherheits-/Cloud-Anwendungen.
- Sensible geschäftskritische Anwendungen, sofern sie nicht explizit getestet wurden.

Schritt 3: Halten Sie SSL-Regeln einfach und sorgfältig geordnet

- Stellen Sie bestimmte Ausschlüsse für die Nicht-Entschlüsselung über breiter angelegte Entschlüsselungsregeln.
- Vermeiden Sie nach Möglichkeit eine zu breite oder komplexe Zuordnung.
- Verwenden Sie nicht die TLS-Version oder die Bedingungen für die Verschlüsselungssuite

für die Regeln "Decrypt-Resign/Known-Key", da Cisco dokumentiert, dass dies zu unvorhersehbarem Verhalten führen kann.

Schritt 4: Überprüfung der Zertifikatbereitschaft

- Bei ausgehendem Decrypt-Resign muss das signierende Zertifizierungsstellenzertifikat von den Clientendpunkten als vertrauenswürdig angesehen werden.
- Für die eingehende Entschlüsselung mit bekanntem Schlüssel muss die Firewall über das richtige Material für das Serverzertifikat/den privaten Schlüssel verfügen.

Schritt 5: Überwachung während der Einführung

- Verfolgen Sie die CPU-Auslastung und, was noch wichtiger ist, die Snort/Inspection-CPU.
- Verfolgen Sie gleichzeitig Verbindungen und neue Verbindungen pro Sekunde.
- Überprüfen von SSL-Flussstatus-/Handshake-Fehlern in Verbindungsereignissen
- Achten Sie auf TLS-Überbelegungsindikatoren und anwendungsspezifische Fehler.

Weitere Informationen zum Überwachen der CPU-Prüfung finden Sie unter:

- https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2026/pdf/BRKSEC-2362.pdf
- Denken Sie wie ein TAC-Techniker: Ein Leitfaden für die häufigsten Probleme mit der Cisco Secure Firewall

Für Tracking-Verbindungen und neue Verbindungen pro Sekunde prüfen:

- Protokollierende optimale Verfahren

Zur Nachverfolgung von SSL-Flussstatus-/Handshake-Fehlern bei der Überprüfung von Verbindungsereignissen und der Überprüfung von TLS-Überbelegungsindikatoren:

- Fehlerbehebung: TLS/SSL-Überbelegung

Schritt 6: Zurücksetzen oder Einschränken des Bereichs, wenn Folgendes angezeigt wird:

- Dauerhafte CPU-Sättigung.

- Erhöhung der für den Benutzer sichtbaren Latenz
- TLS-Handshake-Fehler.
- Geschäftsanwendungen schlagen nach der Entschlüsselung fehl.
- Überbelegung oder übermäßige SSL-Fehler.

Schritt 7: Berücksichtigen der Auswirkungen von TLS 1.3

Die Einführung von TLS 1.3 kann die Transparenz und das Verhalten beeinflussen, da sich bestimmte Handshake- und Inspektionsmerkmale von TLS 1.2 unterscheiden.

Ursache

Für die SSL-/TLS-Entschlüsselung sind zusätzliche Rechenressourcen zum Entschlüsseln, Überprüfen und Wiederverschlüsseln von Datenverkehrsflüssen erforderlich. Die Auswirkungen auf die Leistung variieren erheblich je nach Datenverkehrsmustern, auf entschlüsselten Datenverkehr angewendeten Prüfrichtlinien und der jeweiligen Bereitstellungskonfiguration. Ohne angemessene Planung und schrittweise Implementierung kann es in Produktionsumgebungen zu unerwarteten Leistungseinbußen kommen.

Verwandte Inhalte

- Gerätekonfigurationsanleitung für Cisco Secure Firewall Management Center - Entschlüsselungsregeln
- Cisco Richtlinien für sichere Firewall-Entschlüsselungsrichtlinien
- Best Practice für die Reihenfolge der Entschlüsselungsrichtlinienregeln
- Vereinfachung der Entschlüsselung mit der sicheren Firewall 7.7 von Cisco
- Best Practices für Entschlüsselungsregeln
- Datenblatt zur Cisco Firepower Serie 4100
- Technischer Support und Downloads von Cisco

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.