# Ermitteln der Entschlüsselungsrate in SWA

## Inhalt


Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Auswirkungen auf die Entschlüsselungsleistung

Schritte zum Berechnen des Entschlüsselungsprozentsatzes

- Gesamtverkehrsstatistik von CLI


## Einleitung

In diesem Dokument werden die Schritte zur Berechnung des Prozentsatzes des entschlüsselten Datenverkehrs in der Secure Web Appliance (SWA), die früher als WSA bekannt war, beschrieben.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Physische oder Virtual Secure Web Appliance (SWA) installiert.
- Lizenz aktiviert oder installiert.
- Secure Shell (SSH)-Client.
- Der Setup-Assistent ist abgeschlossen.

- Administratorzugriff auf die SWA.

### Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

## Auswirkungen auf die Entschlüsselungsleistung

Von allen von der SWA ausgeführten Services ist die Bewertung des Hypertext Transfer Protocol Secure (HTTPS)-Verkehrs aus Performance-Sicht am wichtigsten.

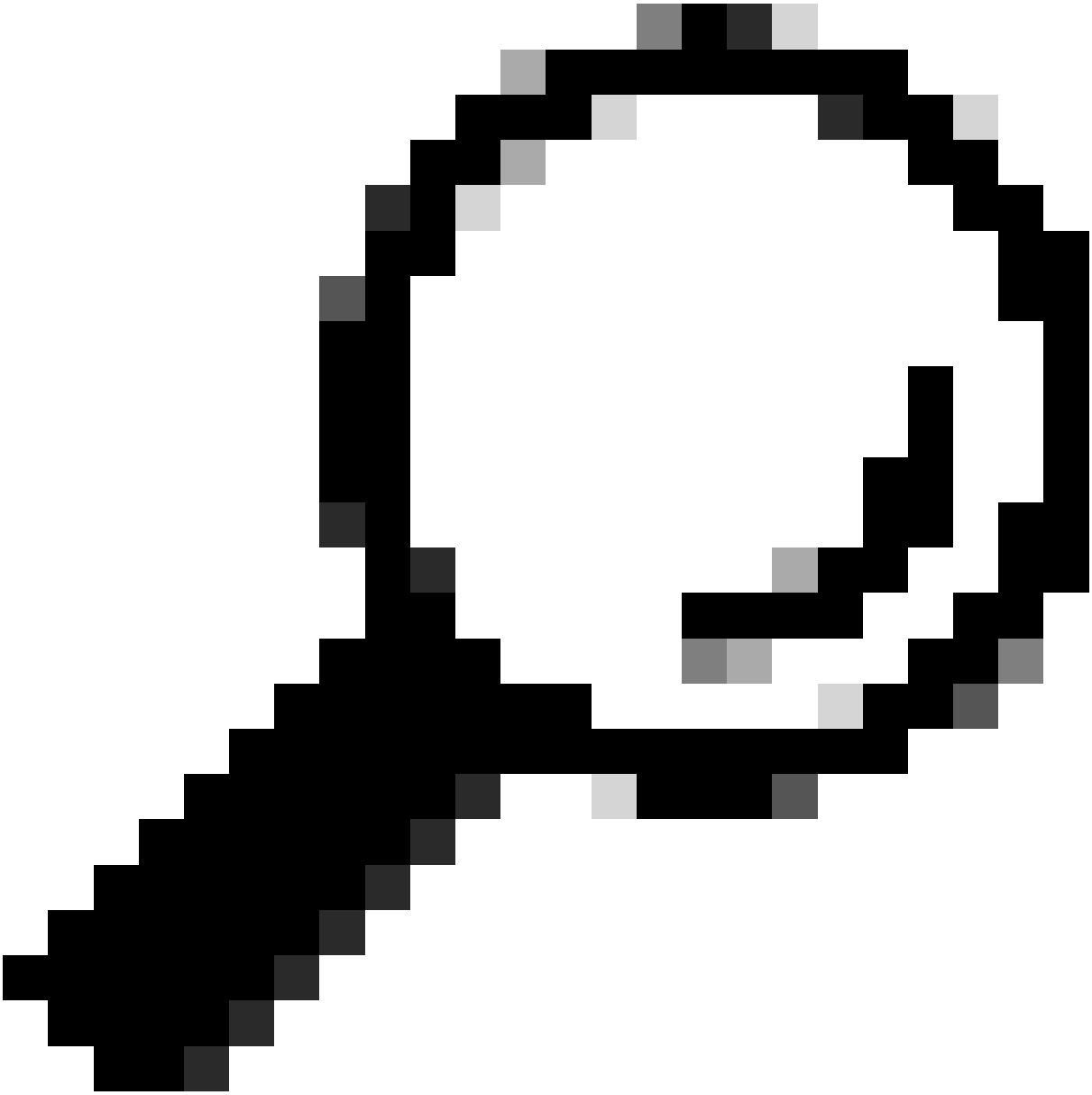
Der Anteil des entschlüsselten Datenverkehrs hat direkte Auswirkungen auf die Größe der Appliance. Ein Administrator kann sich darauf verlassen, dass mindestens 75 % des Webdatenverkehrs über HTTPS erfolgen wird.

Nach der Erstinstallation muss der Prozentsatz des entschlüsselten Datenverkehrs bestimmt werden, um sicherzustellen, dass die Erwartungen für ein zukünftiges Wachstum richtig festgelegt werden. Nach der Bereitstellung muss diese Anzahl einmal pro Quartal überprüft werden.

Wenn die Entschlüsselungsrate mehr als 30 % beträgt und SWA ein Leistungsproblem hat, wird empfohlen:

- Entfernen Sie die Entschlüsselung für verschiedene Kategorien oder vertrauenswürdige URLs (z. B. Microsoft Update oder Antivirus Updates) aus den Entschlüsselungsrichtlinien.
- Lastausgleich über mehrere SWAs zur Lastverteilung

---



---

Tipp: Weitere Informationen zum Umgehen der Entschlüsselung in SWA finden Sie unter: https://www.cisco.com/c/en/us/support/docs/security/web-security-appliance/214746-how-to-exempt-office-365-traffic-from-au.html

## Schritte zum Berechnen des Entschlüsselungsprozentsatzes

Um den prozentualen Anteil des HTTPS-Datenverkehrs zu ermitteln, der im Vergleich zum gesamten HTTPS-Datenverkehr entschlüsselt wird, kopieren Sie access_logs vom SWA File Transfer Protocol (FTP).

Diese Nummer kann mit einfachen Bash- oder PowerShell-Befehlen abgerufen werden. Im Folgenden werden die einzelnen Schritte für die jeweilige Umgebung beschrieben:

1. Ermitteln Sie die Anzahl der HTTPS-Verbindungen insgesamt (explizit und transparent):

```
Bash:
grep -cE 'tunnel://|TCP_CONNECT' aclog.current

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT').length
```

2. Die Anzahl der entschlüsselten HTTPS-Verbindungen ermitteln:

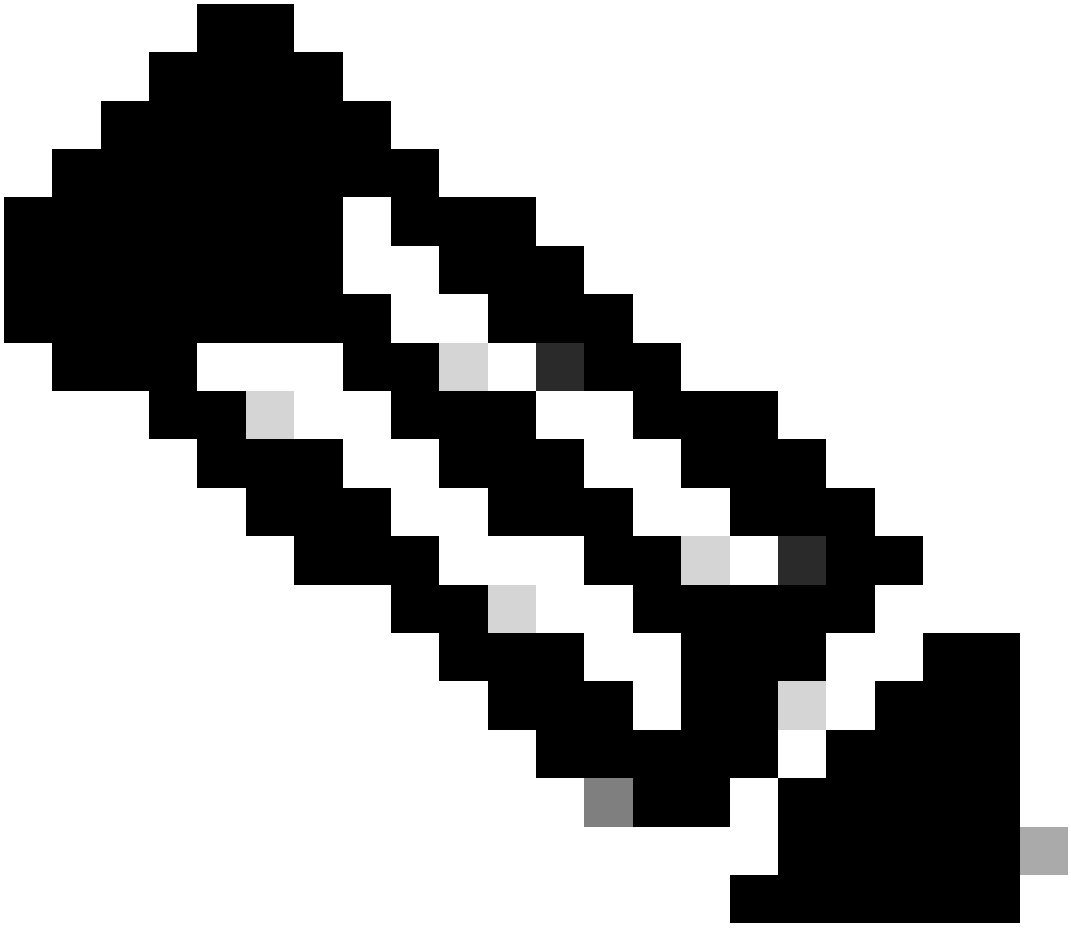
```
Bash:
grep -E 'tunnel://|TCP_CONNECT' aclog.current | grep -c DECRYPT

PowerShell:
(Get-Content aclog.current | Select-String -Pattern 'tunnel://|TCP_CONNECT'| Select-String -Pattern 'DE
```

3. Den zweiten Wert durch den ersten Wert teilen und mit 100 multiplizieren.

### Gesamtverkehrsstatistik von CLI

Sie können die Verkehrsstatistiken in der CLI anzeigen, mit dem Befehl accessloganalyzer, den Sie für Ihren Bericht als Zeitbereich oder letzte N Stunden auswählen können.



Hinweis: Die Ausführungszeit des Befehls hängt vom gewählten Zeitraum ab.

```
SWA_CLI> accessloganalyzer

Choose the option to define the time range:
- HOURS - Last N hours.
- RANGE - Time range with start and end specified in  MM/DD/YYYY HH:MM:SS format.
[]> HOURS

Analyze logs upto N hours old (oldest on this WSA is N = 312 hours). Enter N:
[]> 10

The log processing might take more than 15 secs. Do you want to continue: (Yes/No)
[No]> yes


-------------------------------------------------------------------------------------------------
                                       HTTP                HTTPS               Cumulative
---------------------------------------- ------------------- ------------------- -------------------
Num transactions                       1512509             4170261             5682770
```

| | | | |
|---|---|---|---|
| Transaction/sec | 42 | 115 | 157 |
| Bandwidth (Mbps) | 0.0001 | 0.0004 | 0.0003 |
| Max Resp time (ms) | 643269 | 285036670 | 285036670 |
| Average Resp time(ms) | 95663 | 141715 | 129458 |
| Max Object size (KB) | 92246 | 1215832 | 1215832 |
| Avg Object size (Total Trans)(KB) | 5 | 54 | 41 |
| Avg Object size (Allowed Trans) (KB) | 20 | 67 | 62 |
| Methods | | | |
| GET | 1295658 | 0 | 1295658 |
| POST | 34968 | 0 | 34968 |
| CONNECT | 0 | 4170261 | 4170261 |
| Others | 181883 | 0 | 181883 |
| Status Codes | | | |
| 1xx | 0 | 0 | 0 |
| 2xx | 319799 | 3351382 | 3671181 |
| 3xx | 75011 | 0 | 75011 |
| 4xx | 11697 | 115467 | 127164 |
| 5xx | 1105999 | 703412 | 1809411 |

---

## Zugehörige Informationen

Benutzerhandbuch für AsyncOSAsyncOS oder Cisco SCisco Web Appliance - LD (LimLDed-Bereitstellung) - Cisco

UCiscocure Web Appliance - Best Practices - Cisco

HCisco Befreien von Office 365-Datenverkehr von Authentifizierung und Entschlüsselung auf Cisco WCiscurity Appliance (WSA) - WSAco

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.