HTTPS-Zugriffsformat in sicherer Web-Appliance

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Hintergrundinformationen

Schlüsselwörter im Zugriffsprotokoll

HTTPS-Protokolle im Zugriffsprotokoll

Zugehörige Informationen

Einleitung

In diesem Dokument werden die Secure Web Appliance (SWA)-Zugriffsprotokolle für HTTPS-Datenverkehr beschrieben.

Voraussetzungen

Anforderungen

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

- Installierte physische oder virtuelle SWA.
- 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.

Hintergrundinformationen

Die Protokollierung des Cisco SWA-HTTPS-Datenverkehrs in den Zugriffsprotokollen unterscheidet sich vom normalen HTTP-Datenverkehr.

Anmerkung: Die Protokolle hängen vom Proxy-Bereitstellungsmodus ab, im expliziten Weiterleitungsmodus oder im transparenten Modus werden die Protokolle zurückgestellt.

Schlüsselwörter im Zugriffsprotokoll

Hier sind einige wichtige Schlüsselwörter, die Sie in den Accesslogs sehen können:

TCP_VERBINDUNG: Zeigt an, dass Datenverkehr transparent empfangen wurde (über WCCP, L4-Umleitung oder andere transparente Umleitungsmethoden).
VERBINDEN: Zeigt an, dass der Datenverkehr explizit empfangen wurde.
DECRYPT_WBRS: Dies zeigt, dass SWA den Datenverkehr aufgrund der Web Reputation Score (WBRS)-Bewertung entschlüsselt hat.
PASSTHRU_WBRS: Dies zeigt, dass SWA den Datenverkehr aufgrund der WBRS-Bewertung weitergeleitet hat.
DROP_WBRS: Zeigt an, dass SWA den Datenverkehr aufgrund der WBRS-Bewertung verloren hat.

HTTPS-Protokolle im Zugriffsprotokoll

Wenn HTTPS-Datenverkehr entschlüsselt wird, protokolliert die WSA zwei Einträge.

- TCP_CONNECT tunnel:// oder CONNECT tunnel:// hängt vom Typ der empfangenen Anfrage ab, d. h. der Datenverkehr ist verschlüsselt (wurde noch nicht entschlüsselt).
- GET https:// hat die entschlüsselte URL angezeigt.

Anmerkung: Die vollständige URL wird im transparenten Modus nur angezeigt, wenn der Datenverkehr von der SWA entschlüsselt wird.

```
1706174571.215 582 10.61.70.23 TCP_MISS_SSL/200 39 CONNECT tunnel://www.example.com:443/ - DIRECT/www.e
1706174571.486 270 10.61.70.23 TCP_MISS_SSL/200 1106 GET https://www.example.com:443/ - DIRECT/www.exam
```

Anmerkung: Im transparenten Modus hat SWA die Ziel-IP-Adresse zu Beginn, wenn der Datenverkehr dorthin umgeleitet wird.

Hier sind einige Beispiele für das, was Sie in den Accesslogs sehen:`

Transparente Bereitstellung - Entschlüsselter Datenverkehr

1252543170,769 386 192,168,30,103 TCP_MISS_SSL/200 0 TCP_CONNECT 192,168,34,32:443/ - DIRECT/192.168.34.32 - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,5.0,-,-,-,-,-,-,-,-,-,-,-,-,-> - 1252543171.166 395 192.168.30.103 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif - DIRECT/192.168.34.32 image/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-,-> -
Transparente Bereitstellung - Passthrough-Datenverkehr
1252543337,373 690 192,168,30,103 TCP_MISS/200 2044 TCP_CONNECT 192,168,34,32:443/ - DIRECT/192.168.34.32 - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9.0,-,-,-,-,-,-,-,-,-,-,-,-,-> -
Transparente Bereitstellung - Löschen
1252543418,175 430 192,168,30,103 TCP_DENIED/403 0 TCP_CONNECT 192,168,34,32:443/ - DIRECT/192,168,34,32 - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,-9.1.0,-,-,-,-,-,-,-,-,-,-,-,-,-> -
Explizite Bereitstellung - Entschlüsselter Datenverkehr
252543558,405 385 10,66,71,105 TCP_CLIENT_REFRESH_MISS_SSL/200 40 CONNECT tunnel://www.example.com:443/ - DIRECT/www.example.com - DECRYPT_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,5.0,-,-,-,-,-,-,-,-,-,-,-,-,-> - 1252543559,535 1127 10,66,71,105 TCP_MISS_SSL/200 2061 GET https://www.example.com:443/sample.gif - DIRECT/www.example.com image/gif DEFAULT_CASE-test.policy-test.id-NONE-NONE-NONE <Sear,5.0,0,-,-,-,-,0,-,-,-,-,-,-,-,-> -
Explizite Bereitstellung - Passthrough-Datenverkehr
1252543491,302 568 10,66,71,105 TCP_CLIENT_REFRESH_MISS/200 2256 CONNECT tunnel://www.example.com:443/ - DIRECT/www.example.com - PASSTHRU_WBRS-DefaultGroup-test.id-NONE-NONE-DefaultRouting <Sear,9.0,-,-,-,-,-,-,-,-,-,-,-,-,-> -
Explizite Bereitstellung - Löschen
1252543668.375 1 10.66.71.105 TCP_DENIED/403 1578 CONNECT tunnel://www.example.com:443/ - NONE/- - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-NONE-NONE <Sear,-9.1,-,-,-,-,-,-,-,-,-,-,-,-,-> -

Zugehörige Informationen

- Benutzerhandbuch für AsyncOS 15.0 für Cisco Secure Web Appliance - LD (begrenzte Bereitstellung) - Fehlerbehebung...

- Konfigurieren von Leistungsparametern in Zugriffsprotokollen - 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.