Informazioni sul formato HTTPS Accesslog in Secure Web Appliance

Sommario

Introduzione

In questo documento vengono descritti i log degli accessi di Secure Web Appliance (SWA) per il traffico HTTPS.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- SWA fisico o virtuale installato.
- Licenza attivata o installata.
- Client Secure Shell (SSH).
- Installazione guidata completata.
- Accesso amministrativo all'SWA.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

I log del traffico HTTPS SWA di Cisco nei log degli accessi sono diversi dal normale traffico HTTP.

Nota: I registri dipendono dalla modalità di distribuzione proxy, in modalità di inoltro esplicito o in modalità trasparente i registri sono differiti.

Parole chiave nei log degli accessi

Di seguito sono riportate alcune parole chiave importanti che è possibile visualizzare nei log degli accessi:

TCP_CONNECT: Questo messaggio indica che il traffico è stato ricevuto in modo trasparente (tramite WCCP, reindirizzamento L4 o altri metodi di reindirizzamento trasparenti)
CONNETTI: Ciò indica che il traffico è stato ricevuto esplicitamente.
DECRYPT_WBRS : Questo comando mostra che il protocollo SWA ha decrittografato il traffico a causa del punteggio Web Reputation Score (WBRS).
PASSTHRU_WBRS : Questo mostra che SWA ha superato il traffico a causa del punteggio WBRS.
DROP_WBRS: Questo mostra che SWA ha perso il traffico a causa del punteggio WBRS

Log HTTPS nei log degli accessi

Quando il traffico HTTPS viene decrittografato, WSA registra due voci.

- TCP_CONNECT tunnel:// o CONNECT tunnel:// dipende dal tipo di richiesta ricevuta, ovvero il traffico è crittografato (non è stato ancora decrittografato).
- GET https:// ha visualizzato l'URL decrittografato.

Nota: L'URL completo in modalità trasparente è visibile solo se il protocollo SWA decrittografa il traffico.

```
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
```

Nota: In modalità trasparente, SWA ha l'indirizzo IP di destinazione inizialmente quando il traffico viene reindirizzato a esso.

Di seguito sono riportati alcuni esempi di quanto riportato nei log degli accessi:

Distribuzione trasparente - Traffico decrittografato
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-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,-,-,-,-,-,-> -
Distribuzione trasparente - Traffico pass-through
125254337.373 690 192.168.30.103 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,-,-,-,-,-,-,-,-,-,-,-> -
Distribuzione trasparente - Elimina
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-DefaultRouting <Sear,-9.1.0,-,-,-,-,-,-,-,-,-,-,-> -
Distribuzione esplicita - Traffico decrittografato
25254358.405 385 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,-,-,-,-,-,-,-,-,-,-,-> - 125254359.535 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 <Sear,5.0,0,-,-,-,0,-,-,-,-,-,-,-> -
Distribuzione esplicita - Traffico pass-through
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-DefaultRouting <Sear,9.0,-,-,-,-,-,-,->
Distribuzione esplicita - Elimina
125254368.375 10.66.71.105 TCP_DENIED/403 1578 CONNECT tunnel://www.example.com:443/ - NONE/- - DROP_WBRS-DefaultGroup-test.id-NONE-NONE <Sear,-9.1,-,-,-,-,-,-,-,-,-,-,-,-,-> -

Informazioni correlate

- Guida per l'utente di AsyncOS 15.0 for Cisco Secure Web Appliance - LD (installazione

limitata) - Risoluzione dei problemi...

- Configura parametro prestazioni nei log degli accessi - Cisco

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).