Inzicht in HTTPS-toegangslogindeling in Secure Web Appliance

Inhoud

Inleiding

Voorwaarden

- Vereisten
- Gebruikte componenten

Achtergrondinformatie

Trefwoorden in de accesslogs

HTTPS-logboeken in de accesslogs

Gerelateerde informatie

Inleiding

In dit document worden toegangslogs voor Secure Web Appliance (SWA) voor HTTPS-verkeer beschreven.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Fysieke of virtuele SWA geïnstalleerd.
- Licentie geactiveerd of geïnstalleerd.
- Secure Shell (SSH)-client.
- De installatiewizard is voltooid.
- Administratieve toegang tot de SWA.

Gebruikte componenten

Dit document is niet beperkt tot specifieke software- en hardware-versies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Achtergrondinformatie

De manier waarop Cisco SWA HTTPS-verkeerslogboeken in de toegangslogboeken registreren, is anders dan normaal HTTP-verkeer.

Opmerking: De logs zijn afhankelijk van de Proxy-implementatiemodus, in de expliciete voorwaartse of transparante modus zijn de logs deferent.

Trefwoorden in de accesslogs

Hier zijn enkele belangrijke trefwoorden die u kunt zien in de Accesslogs:

TCP_CONNECT: Dit toont aan dat het verkeer transparant is ontvangen (via WCCP, L4-omleiding of andere transparante omleidingsmethoden)
CONNECT: Hieruit blijkt dat het verkeer expliciet is ontvangen.
DECRYPT_WBRS: Dit toont aan dat SWA het verkeer heeft ontsleuteld vanwege de Web Reputation Score (WBRS)-score.
PASSTHRU_WBRS: Dit toont SWA heeft Pass Through het verkeer als gevolg van WBRS score.
DROP_WBRS: Dit toont SWA heeft Drop het verkeer als gevolg van WBRS score

HTTPS-logboeken in de accesslogs

Wanneer HTTPS-verkeer wordt gedecodeerd, registreert WSA twee vermeldingen.

- TCP_CONNECT tunnel:// of CONNECT tunnel:// hangt af van het type ontvangen aanvraag, wat betekent dat het verkeer is gecodeerd (nog niet is gedecodeerd).
- GET https:// toont de gedecodeerde URL.

Opmerking: Volledige URL in de transparante modus is alleen zichtbaar als SWA het verkeer decodeert.

```
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
```

Opmerking: In de transparante modus heeft SWA het IP-adres van de bestemming in eerste instantie wanneer het verkeer ernaar wordt omgeleid.

Hier zijn enkele voorbeelden van wat je ziet in accesslogs:`

Transparante implementatie - Ontsleuteld verkeer

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-NONE <Sear,5.0,0,-,-,-,-,0,-,-,-,-,-,-> -
Transparante implementatie — doorvoerverkeer
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,-,-,-,-,-,-,-,-,-,-,-,-> -
Transparante implementatie - Drop
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,-,-,-,-,-,-,-,-,-,--,-> -
Expliciete implementatie - gedecodeerd verkeer
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 <Sear, 5.0,-,-,-,-,-,-,-, 0,-,-,-,-,-,-,-,-,-,-,-,-,-> ->
Expliciete implementatie - Passthrough-verkeer
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-NONE-DefaultRouting <Sear, 9.0,-> ->
Expliciete implementatie - Drop
1252543668.375 1 10.66.71.105 TCP_DENIED/403 1578 CONNECT tunnel://www.example.com:443/ - GEEN/- - DROP_WBRS-DefaultGroup-test.id-NONE-NONE-NONE <Sear,-9.1,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-,-> ->

Gerelateerde informatie

- Gebruikershandleiding voor AsyncOS 15.0 voor Cisco Secure Web Appliance - LD (Limited

Deployment) - Probleemoplossing...
- Prestatieparameter configureren in toegangslogboeken - Cisco

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.