Problemen met toegang tot de Secure Web Gateway SWG-website oplossen

Inhoud

Inleiding

Dit document beschrijft de gestructureerde methodologie voor het diagnosticeren van problemen met de toegang tot websites wanneer deze worden gerouteerd via een cloudgebaseerde proxy (Secure Web Gateway/SWG), maar niet wanneer gebruik wordt gemaakt van Direct Internet Access (DIA).

- Toepassingsgebied: geldt voor zowel Cisco Umbrella SIG als Cisco Secure Access.

Voorwaarden en belangrijke waarschuwingen

- Controleer of alle probleemoplossing wordt uitgevoerd voor reproduceerbare problemen.
- Verzamel een HAR (HTTP Archive) bestand en een gelijktijdige Packet Capture (PCAP) om nauwkeurige gegevens voor analyse te bieden.
- Wijzigingen in het proxybeleid (bijvoorbeeld het omzeilen van decodering of inspectie) kunnen van invloed zijn op de beveiligingshouding; gelden alleen voor probleemoplossing of zoals aanbevolen.

Fouten op proxyniveau identificeren

Gemeenschappelijke proxy-interferentie-indicatoren omvatten:

- 502 Bad Gateway
- 515 Upstream-certificaat niet vertrouwd
- 517 Upstream-certificaat ingetrokken
- 403 Verboden
- Ingetrokken certificaten
- Mismatches in coderingssuite
- Time-outs voor websiteverbindingen

Methodologie voor probleemoplossing

Stap 1: Bevestig dat de proxy door het verkeer gaat

- Gegevensverzameling: Genereer een HAR-bestand en PCAP wanneer het probleem zich voordoet.
- Header-analyse: Inspecteer de Via-header in HTTP-reacties. De aanwezigheid van `s_proxy` (Nginx-proxy) of `m_proxy` (Modular Proxy Service/MPS) bevestigt dat het verkeer wordt benaderd.
- TCP-stream: volg in Wireshark de TCP-stream om ervoor te zorgen dat de verbinding is verbonden met het IP-adres van de proxy, niet met het IP-adres van de bestemming.

Stap 2: TLS-decoderingsstatus controleren

- Browserinspectie: Klik op het vergrendelingspictogram in de adresbalk van de browser. Als het Cisco Secure Access Root Certificate in de certificaatketen wordt weergegeven, is HTTPS-inspectie actief.
- Validatie: kruisverwijzing naar de Via-headers in HAR/PCAP-bestanden.
- OpenSSL-opdracht: certificaatketens inspecteren:
  `OpenSSL S_Client -connect www.example.com:443 -showcerts`
  Met deze opdracht wordt de certificaatketen gecontroleerd die door de server wordt gepresenteerd. Voer het uit vanaf een systeem dat de proxy doorkruist voor directe validatie.

Stap 3: Isolatie en eliminatie

1. Fase A – Test HTTPS-inspectie (NGINX-laag):
   - Voeg het problematische domein toe aan de SWG-lijst "Niet decoderen".
   - Bestandsinspectie ingeschakeld houden.
   - Als het probleem is opgelost: De hoofdoorzaak is waarschijnlijk Nginx SSL / TLS inspectie. Analyseer de PCAP op mismatches in coderingen of SNI-problemen. Gebruik `curl` met en zonder proxy om gedrag te vergelijken.
   - Als het probleem zich blijft voordoen: ga verder met Fase B.
2. Fase B – Controle van testbestanden (scanlaag):
   - Bestandsinspectie uitschakelen voor het specifieke verkeer.
   - Als het probleem is opgelost: De hoofdoorzaak ligt in de bestandsscanengine. Controleer PCAP en HAR, reproduceer in het laboratorium en bepaal of een specifiek

bestand of een scanhandtekening het probleem veroorzaakt.
- Indien niet opgelost: neem contact op met de support met uitgebreide logboeken en bevindingen.

Veelvoorkomende problemen en foutcodes

515 Upstream-certificaat niet vertrouwd

Deze fout treedt op wanneer de SWG-proxy het certificaat van de bestemmingsserver niet kan valideren. Oorzaken zijn verlopen, zelf ondertekende of onvolledige certificaatketens.

- HTTPS-inspectie ON + bestandsinspectie ON: website werkt; geen certificaatfouten.
- HTTPS-inspectie AAN + bestandsinspectie UIT: 515-fout wordt waargenomen, overeenkomend gebruikersrapport.
- HTTPS-inspectie UIT + bestandsinspectie UIT (domein op lijst Niet decoderen): geen problemen waargenomen.

Technische details: Nginx-proxy kan mislukken als de upstream-server vertrouwt op Authority Information Access (AIA) voor het ophalen van ontbrekende tussenliggende certificaten, omdat Nginx AIA niet zo sierlijk behandelt als de proxyservice voor bestandsscanning. SNI- en SAN-mismatches tijdens TLS-handshake kunnen ook fouten veroorzaken.

517 Upstream-certificaat ingetrokken

De 517-fout betekent dat de CRL- of OCSP-controle van de SWG-proxy het certificaat van de upstream-server heeft ingetrokken.

- Problemen oplossen: gebruik externe tools zoals SSL Labs of OpenSSL om de intrekkingsstatus te bevestigen.
- Documentatie:
  - Cisco-fout voor probleemoplossing 517 – Upstream-certificaat ingetrokken
  - Algemene fouten in certificaten en protocollen begrijpen

Opties voor het afhandelen van fouten in certificaten

Cisco Secure Access introduceert een nieuwe functie genaamd "Certificate Error Handling Options" voor het omzeilen van granulaire fouten zonder de decodering volledig uit te schakelen.

Domeinen die certificaatfouten veroorzaken als gevolg van inspectie, kunnen worden beheerd met deze functie in plaats van brede "Do Not Decrypt" -lijsten.
Deze functie bestaat in Umbrella SIG vanaf vandaag. Specificatieverzoeken details voor CSA.

502 Bad Gateway

De 502-fout geeft aan dat de SWG-proxy een ongeldig antwoord heeft ontvangen van de upstream-server terwijl deze als tussenpersoon fungeert.

- Downstream: client naar SWG-proxy
- Upstream: SWG-proxy naar bestemmingsserver

De fout zit altijd in de upstream-verbinding als gevolg van protocolfouten, TCP-resets of misvormde headers.

502 oorzaken

- Niet-ondersteunde SWG-coderingssuites
- Aanvraag voor verificatie clientcertificaat
- Headers toegevoegd door de SWG Proxy

Niet-ondersteunde coderingssuites

Oorzaak: Server vereist een cijfer dat niet wordt ondersteund door SWG (bijvoorbeeld TLS_CHACHA20_POLY1305_SHA256).
Resolutie: Voeg het domein toe aan de lijst Selectieve decryptie.

Testen, opdrachten:
Met proxy:

```
curl -x proxy.sig.umbrella.com:80 -v xyz.com:80
curl -x swg-url-proxy-https.sigproxy.qq.opendns.com:443 -vvv -k "https://www.cnn.com" >> null
```

Zonder proxy:

```
curl -v www.xyz.com:80
```

Mac/Linux:

```
curl -vvv -o /dev/null -k -L www.cnn.com
```

Windows:

```
curl -vvv -o null -k -L www.cnn.com
```

Aanvraag voor verificatie clientcertificaat

Oorzaak: De upstream-server vereist certificaten aan de clientzijde, die SWG niet ondersteunt. Oplossing: omzeilen van het domein van de proxy met behulp van de External Domains management list (Umbrella SIG) of Bypass Secure Proxy (Cisco Secure Access). Het omzeilen van HTTPS-inspectie alleen is onvoldoende.

Headers toegevoegd door Proxy

Oorzaak: Sommige servers weigeren aanvragen met de X-Forwarding-For (XFF) header toegevoegd door SWG wanneer HTTPS-inspectie is ingeschakeld.
Resolutie: Vergelijk gedrag met/zonder HTTPS en bestandsinspectie. Als de fout alleen optreedt wanneer XFF aanwezig is, is de webserver waarschijnlijk verkeerd geconfigureerd.

Voorbeeld:
`curl https://www.xyz.com -k --header 'X-Forwarding-For: 1.1.1.1' -o /dev/null -w "Status Code: %{http_code}" -s`
Statuscode: 502
`curl https://www.xyz.com -k -o /dev/null -w "Status Code: %{http_code}" -s`
Statuscode: 200

De XFF-header wordt toegevoegd voor geolocatie. Als de server deze niet kan verwerken, wordt een 502-fout weergegeven.

Mogelijk ongewenste PUA of beschadigde bestanden

Als SWG een bestand niet kan scannen met bestandsinspectie (bijvoorbeeld beveiligde, aangevraagde of beschadigde bestanden), blokkeert het de download en rapporteert het - Geblokkeerd - Potentieel ongewenste toepassing (beveiligd bestand)

- Problemen oplossen: leg een HAR vast tijdens het blokevenement. Gebruik Override Security als tijdelijke oplossing. Als het bestand beschadigd of kwaadaardig is, moet het aan de bron worden gecorrigeerd.

Potentieel schadelijke categorieën en reputatieblokken

- Gebruik Talos om de webreputatie (WBRS) te controleren. Als een domein ten onrechte is gecategoriseerd, dient u een COG Jira-verzoek in bij Talos voor beoordeling. Talos

gecategoriseerd als veilig of gunstig, maar nog steeds SWG blok dan moeten we controleren van Beaker service van SWG.

Toegang geweigerd door Akamai voor SWG Egress IP's

- SWG maakt gebruik van gedeelde IP-adressen. Als deze op de zwarte lijst staan van IP-reputatieservices (bijvoorbeeld Brightcloud), kan de toegang tot bepaalde sites worden geweigerd.

Bekende problemen: aanmeldbot voor YouTube en video niet beschikbaar

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.