Fehlerbehebung bei Problemen mit dem Zugriff auf die SWG-Website über Secure Web Gateway

Inhalt

Einleitung

In diesem Dokument wird die strukturierte Methodik zur Diagnose von Website-Zugriffsproblemen beschrieben, wenn diese über einen Cloud-basierten Proxy (Secure Web Gateway/SWG) weitergeleitet werden, jedoch nicht bei Verwendung von Direct Internet Access (DIA).

- Geltungsbereich: Gilt für Cisco Umbrella SIG und Cisco Secure Access.

Voraussetzungen und wichtige Warnungen

- Überprüfen Sie, ob bei reproduzierbaren Problemen alle Fehlerbehebungsmaßnahmen durchgeführt werden.
- Sammeln Sie eine HAR-Datei (HTTP Archive) und eine gleichzeitige Paketerfassung (PCAP), um präzise Daten für die Analyse bereitzustellen.
- Änderungen an Proxy-Richtlinien (z. B. Umgehung der Entschlüsselung oder Überprüfung) können sich auf den Sicherheitsstatus auswirken. nur für die Fehlerbehebung oder wie empfohlen.

Identifizieren von Fehlern auf Proxyebene

Gängige Störungsindikatoren für Proxys:

- 502 Ungültiges Gateway
- 515 Upstream-Zertifikat nicht vertrauenswürdig
- 517 Upstream-Zertifikat widerrufen
- 403 Verboten
- Entzogene Zertifikate

- Nichtübereinstimmungen der Verschlüsselungssuite
- Timeouts für Websiteverbindungen

Methodik der Fehlerbehebung

Schritt 1: Datenverkehr bestätigen, der den Proxy durchquert

- Datensammlung: Generieren Sie eine HAR-Datei und PCAP, wenn das Problem auftritt.
- Header-Analyse: Überprüfen Sie den Via-Header in HTTP-Antworten. Das Vorhandensein von `s_proxy` (Nginx-Proxy) oder `m_proxy` (Modular Proxy Service/MPS) bestätigt, dass der Datenverkehr als Proxy weitergeleitet wird.
- TCP-Stream: Befolgen Sie in Wireshark den TCP-Stream, um sicherzustellen, dass die Verbindung mit der IP des Proxys und nicht mit der Ziel-IP-Adresse besteht.

Phase 2: TLS-Entschlüsselungsstatus überprüfen

- Browser-Überprüfung: Klicken Sie in der Adressleiste des Browsers auf das Sperrsymbol. Wenn das Cisco Secure Access Root-Zertifikat in der Zertifikatskette angezeigt wird, ist die HTTPS-Prüfung aktiv.
- Validierung: Querverweise auf die Via-Header in HAR-/PCAP-Dateien
- OpenSSL-Befehl: So prüfen Sie Zertifikatsketten:
  `openssl s_client -connect www.example.com:443 -showcerts`
  Mit diesem Befehl wird die Zertifikatskette überprüft, die vom Server dargestellt wird. Führen Sie es von einem Computer aus, der den Proxy durchläuft, um eine direkte Validierung zu ermöglichen.

Schritt 3: Isolierung und Eliminationsprozess

1. Phase A - HTTPS-Prüfung testen (Nginx-Layer):
   - Fügen Sie die problematische Domäne der SWG-Liste "Nicht entschlüsseln" hinzu.
   - Dateiprüfung aktiviert lassen.
   - Wenn das Problem behoben ist: Die Ursache ist wahrscheinlich Nginx SSL/TLS Inspection. Analysieren Sie PCAP auf Cipher-Diskrepanzen oder SNI-Probleme. Verwenden Sie `curl` mit und ohne Proxy, um das Verhalten zu vergleichen.
   - Wenn das Problem weiterhin besteht: Fahren Sie mit Phase B fort.
2. Phase B - Prüfung der Testdatei (Scan-Layer):
   - Deaktivieren Sie die Dateiüberprüfung für den jeweiligen Datenverkehr.

- Wenn das Problem behoben ist: Die Ursache liegt in der Datei-Scan-Engine. Überprüfen Sie PCAP und HAR, führen Sie die Wiedergabe im Labor durch, und stellen Sie fest, ob das Problem durch eine bestimmte Datei oder eine Scan-Signatur verursacht wird.
- Falls nicht behoben: Wenden Sie sich mit umfassenden Protokollen und Ergebnissen an den Support.

Häufige Probleme und Fehlercodes

515 Upstream-Zertifikat nicht vertrauenswürdig

Dieser Fehler tritt auf, wenn der SWG-Proxy das Zertifikat des Zielservers nicht validieren kann. Ursachen sind abgelaufene, selbstsignierte oder unvollständige Zertifikatsketten.

- HTTPS-Inspektion EIN + Dateiinspektion EIN: Website funktioniert; keine Zertifikatfehler.
- HTTPS-Inspektion EIN + Dateiinspektion AUS: 515 Fehler festgestellt, Benutzerbericht entspricht.
- HTTPS-Inspektion AUS + Dateiinspektion AUS (Domäne auf Liste "Nicht entschlüsseln"): Keine Probleme beobachtet.

Technische Details: Der Nginx-Proxy kann fehlschlagen, wenn der Upstream-Server darauf angewiesen ist, dass der Authority Information Access (AIA) nach fehlenden Zwischenzertifikaten fragt, da Nginx AIA nicht so anmutig behandelt wie der File Scanning-Proxydienst. SNI- und SAN-Diskrepanzen während des TLS-Handshakes können ebenfalls zu Ausfällen führen.

517 Upstream-Zertifikat widerrufen

Der Fehler 517 bedeutet, dass die CRL- oder OCSP-Prüfung des SWG-Proxys festgestellt hat, dass das Zertifikat des Upstream-Servers widerrufen wurde.

- Fehlerbehebung: Verwenden Sie externe Tools wie SSL Labs oder OpenSSL, um den Sperrstatus zu bestätigen.
- Dokumentation:
  - Cisco Troubleshooting Error 517 - Upstream-Zertifikat widerrufen
  - Häufige Zertifikat- und Protokollfehler

Optionen für die Behandlung von Zertifikatfehlern

Cisco Secure Access führt eine neue Funktion mit der Bezeichnung "Certificate Error Handling Options" ein, die eine präzise Fehlerumgehung ermöglicht, ohne die Entschlüsselung vollständig zu deaktivieren. Domänen, die aufgrund einer Überprüfung Zertifikatfehler auslösen, können mit dieser Funktion anstelle von umfangreichen "Nicht entschlüsseln"-Listen verwaltet werden. Diese Funktion ist in Umbrella SIG ab sofort verfügbar. Details zu Funktionsanforderungen für CSA

502 Ungültiges Gateway

Der Fehler 502 zeigt an, dass der SWG-Proxy vom Upstream-Server als Vermittler eine ungültige Antwort erhalten hat.

- Downstream: Client an SWG-Proxy
- Upstream: SWG-Proxy zum Zielserver

Der Fehler tritt immer in der Upstream-Verbindung auf - aufgrund von Protokollfehlern, TCP-Resets oder falsch formatierten Headern.

Häufige 502 Ursachen

- Nicht unterstützte SWG Cipher Suites
- Authentifizierungsanforderung für Clientzertifikat
- Vom SWG-Proxy hinzugefügte Header

Nicht unterstützte Cipher Suites

Ursache: Für den Server ist eine Verschlüsselung erforderlich, die von SWG nicht unterstützt wird (z. B. TLS_CHACHA20_POLY1305_SHA256).
Auflösung: Fügen Sie die Domäne zur Liste der selektiven Entschlüsselung hinzu.

Testbefehle:
Mit 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
```

Ohne Proxy:

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

Mac/Linux:

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

Windows:

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

Authentifizierungsanforderung für Clientzertifikat

Ursache: Der Upstream-Server erfordert clientseitige Zertifikate, die von der SWG nicht unterstützt werden.
Auflösung: Umgehen der Domäne vom Proxy mithilfe der Verwaltungsliste für externe Domänen (Umbrella SIG) oder über Sicheren Proxy umgehen (Cisco Secure Access) Die Umgehung der HTTPS-Überprüfung allein ist nicht ausreichend.

Von Proxy hinzugefügte Header

Ursache: Einige Server lehnen Anforderungen mit dem von SWG hinzugefügten X-Forwarded-For (XFF)-Header ab, wenn die HTTPS-Überprüfung aktiviert ist.
Auflösung: Verhalten mit/ohne HTTPS und Dateiprüfung vergleichen. Wenn der Fehler nur auftritt, wenn XFF vorhanden ist, ist der Webserver wahrscheinlich falsch konfiguriert.

Beispiel:

```
curl https://www.xyz.com -k –header 'X-Forwarded-For: 1.1.1.1' -o /dev/null -w "Statuscode: %{http_code}" - s
```

Statuscode: 502

```
curl https://www.xyz.com -k -o /dev/null -w "Statuscode: %{http_code}" - s
```

Statuscode: 200

Der XFF-Header wird für die Geolokalisierung hinzugefügt. Wenn der Server es nicht verarbeiten kann, wird ein 502-Fehler ausgegeben.

Potenziell unerwünschte PUA oder beschädigte Dateien

Wenn die SWG eine Datei nicht mithilfe einer Dateiprüfung (z. B. geschützte, vom Bereich angeforderte oder beschädigte Dateien) scannen kann, wird der Download blockiert, und es werden Berichte erstellt - Blockiert - Potenziell unerwünschte Anwendung (geschützte Datei).

- Fehlerbehebung: Erfassen Sie ein HAR während des Blockereignisses. Verwenden Sie "Sicherheit außer Kraft setzen" als temporäre Problemumgehung. Wenn die Datei beschädigt oder schädlich ist, muss sie an der Quelle behoben werden.

Potenziell schädliche Kategorien und Reputationsbausteine

- Verwenden Sie Talos, um die Web-Reputation (WBRS) zu überprüfen. Wenn eine Domain falsch kategorisiert ist, senden Sie eine COG Jira Anfrage zur Prüfung an Talos. Talos kategorisiert als sicher oder günstig, aber immer noch SWG Block dann brauchen wir Scheck von Beaker Service der SWG.

Zugriff von Akamai für SWG-Ausgangs-IPs verweigert

- Die SWG verwendet gemeinsam genutzte Ausgangs-IPs. Wenn diese von IP-Reputationsdiensten (z. B. Brightcloud) auf die Blacklist gesetzt werden, kann der Zugriff auf bestimmte Websites verweigert werden.

Bekannte Probleme: YouTube-Sign-In-Bot und Video nicht verfügbar

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.