Probleme beim Zugriff auf die SWG-Website beheben

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wie Sie Probleme mit dem Website-Zugriff beheben, die beim Umbrella Secure Web Gateway (SWG) Proxy aufgetreten sind.

Hintergrundinformationen

Nehmen wir an, dass die Website www.xyz.com nicht über den SWG-Proxy erreichbar ist und wenn Nutzer versuchen, direkt auf das Internet zuzugreifen (ohne dass Umbrella SWG im Bild ist), funktioniert sie einwandfrei. Lassen Sie uns verschiedene Symptome und verschiedene Arten von Fehlermeldungen, die gemeldet, wenn Website nicht über SWG zugänglich ist. Die häufigsten sind 502 fehlerhafte Gateway, 502 konnte keine Nachricht Upstream-Fehler weiterleiten, Upstream-Zertifikat widerrufen, Zugriff verweigert 403 verboten, Upstream-Chiffren stimmen nicht überein, Website ist gerade nach dem Drehen für einige Zeit oder Ähnliches abgelaufen.

Fehler "Access Denied 403" (Zugriff verweigert) aufgrund von Upstream-Block

Webserver oder Upstream blockiert oder drosselt unsere SWG-Proxy-Egress-IP-Bereiche. Die WAF von Akamai hat beispielsweise einige SWG-Ausgangs-IP-Bereiche blockiert. Um dieses Problem zu beheben, ist nur die Option verfügbar, dass Sie sich an Website-Administratoren

wenden und sie unsere IP-Bereiche entsperren lassen. Bis dahin sollten Sie die SWG-Domäne mithilfe einer externen Domänenverwaltungsliste für Anyconnect SWG- und PAC-Dateibereitstellungen umgehen. Kurz gesagt, diese Art von Problem liegt nicht am Proxy selbst, sondern an der Inkompatibilität zwischen Proxy und Webservern. Hier ist der Link, um die KB speziell für "Access Denied 403" Fehler aufgrund der Egress-IP-Block.

Darüber hinaus finden Sie hier den Link mit einigen möglichen Gründen, warum Akamai aufgelistete IP-Adressen blockiert.

Fehler "Access Denied 403" aufgrund von Java-Problem

Der Zugriff auf die Website ist nicht möglich, und es wird "Zugriff verweigert oder 403 Verboten - Umbrella Cloud Security Gateway-Fehler" ausgelöst, wenn die Anforderung über den SWG-MPS-Proxy gesendet wird und die Dateiprüfungseinstellung aktiviert ist. Wenn die Dateiinspektion jedoch deaktiviert ist, werden die Websites erfolgreich geladen. Oder wenn wir die Website in Bypass-Entschlüsselung, Websites erfolgreich geladen.

Hauptursache des Problems

Welches Java-bezogene Problem besteht bei MPS?

Die betreffende Website oder der Webserver gibt eine TLS-Warnung bezüglich einer SNI- oder SSL-Warnung an den Proxy zurück, nachdem der Proxy versucht, eine Verbindung zum Server herzustellen. Im Grunde geschieht dies, nachdem der Client-Hello gesendet wurde. MPS-Proxy (basiert auf Java und als solche) behandelt alle TLS-Warnungen mit "Unknown Name" im Beschreibungsfeld während des SNI-Parsens als Fehler und beendet die Transaktion. Weitere Informationen finden Sie hier

Bitte beachten Sie, dass es sich nicht um ein SWG- oder MPS-Proxy-Problem handelt. Dies ist eine der Inkompatibilitäten mit der SWG oder anderen Proxys aufgrund von serverseitigen Fehlkonfigurationen. Browser ignorieren diese Warnung normalerweise, aber SWG oder andere Content-Sicherheitsfilter behandeln die SSL-Warnung als schwerwiegenden Fehler und beenden die Sitzung, was zu 403 verbotenen Fehlerseiten für die Benutzer führt. Es kann auch melden 502 Bad Gateway-Fehler, aber mit den meisten Beispielen, was wir gesehen haben, ist 403 verbotene Fehler, wie in diesem Bild gezeigt.

Da MPS auf Anwendungsebene arbeitet, hat es wenig bis gar keine Kontrolle darüber, wie die TLS-Schicht die Transaktion auf Grundlage der im TLS-Protokoll erzeugten Warnungen handhabt. Es obliegt dem Server, sicherzustellen, dass seine TLS-Endpunkte bzw. -Zertifikate korrekt

konfiguriert sind. Weitere Informationen finden Sie unter diesem Link.

Um das Problem einzugrenzen oder Probleme zu beheben, kann im SSL-Labor darauf hingewiesen werden.

15152060146964

Wenn der Zugriff auf die Website ohne SWG-Proxy in der Mitte erfolgt oder die HTTPS-Prüfung von SWG umgangen wird, funktioniert die Website, da der Browser die SNI-Warnung Unbekannter Name ignoriert und die Kommunikation mit dem Webserver fortsetzt.

Zum Zeitpunkt der Erstellung dieses Artikels ist die empfohlene Problemumgehung die beste Abmilderung, die wir Ihnen vorschlagen können. Mit der neuen Proxy-Architektur können wir diese Probleme in naher Zukunft besser bewältigen.

Auflösung

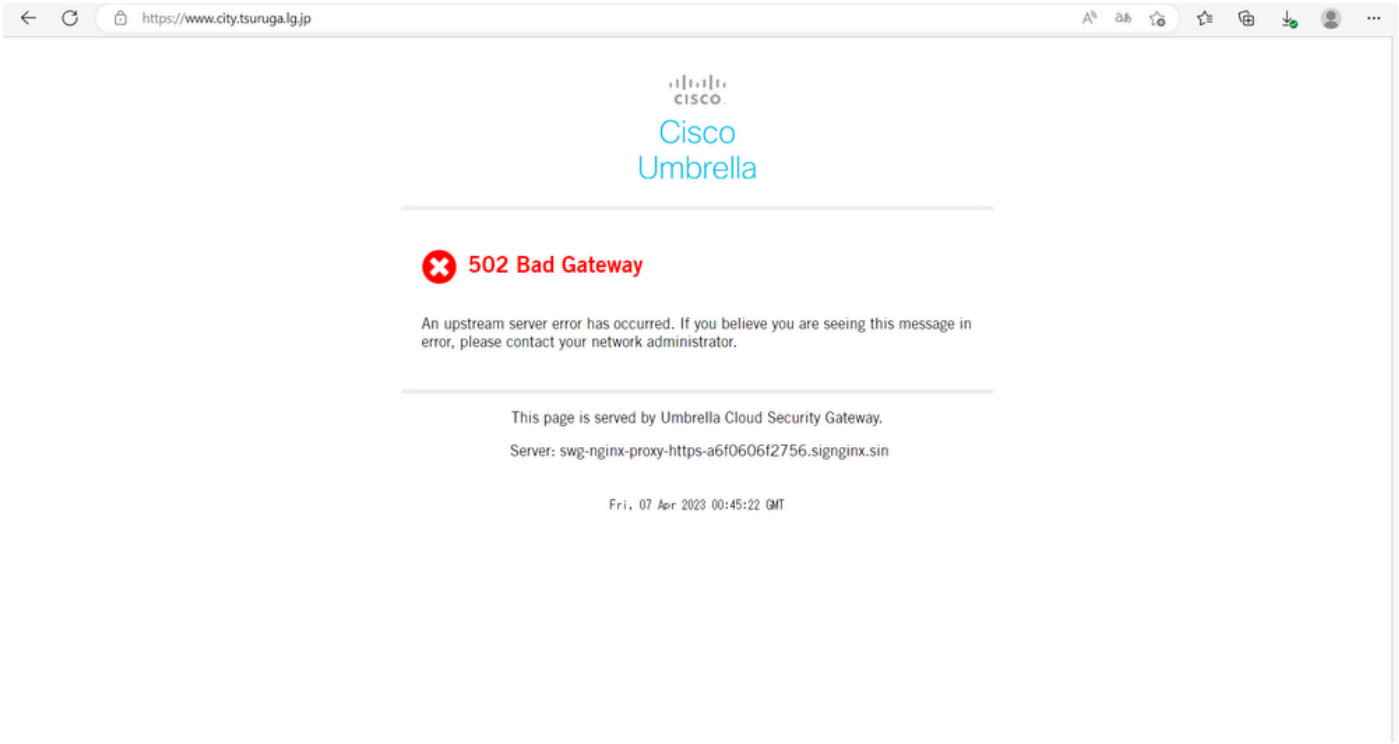
1. Entschlüsselung für die betroffenen Domänen deaktivieren - ODER
2. Fügen Sie die Domäne zu einer Zielliste hinzu, und ordnen Sie eine Zulassungsregel zu (wenn Sie der Site vertrauen)

Was ist 502 Bad Gateway?

Ein 502 Bad Gateway Error (Fehler 502 Ungültiges Gateway) bedeutet, dass der Server als Gateway oder Proxy agiert und eine ungültige Antwort vom Upstream-Server erhalten hat. Wenn der Benutzer versucht, über den SWG Proxy auf die Website zuzugreifen, passieren zwei Kommunikationsflüsse.

a) Client —> Proxy-Verbindung (Downstream)
b) Proxy—> Webserververbindung beenden (Upstream)

502 Fehler beim fehlerhaften Gateway zwischen SWG-Proxy (MPS, Nginx) und End-Server-Verbindung.



15026978020884

Allgemeine Faktoren für fehlerhafte 502-Gateways

1. Nicht unterstützte SWG Cipher Suites

2. Authentifizierungsanforderung für Clientzertifikat

3. Vom SWG-Proxy hinzugefügte oder entfernte Header

Nicht unterstützte SWG Cipher Suites

Nehmen wir an, ein Webserver meldet während der TLS-Aushandlung nicht unterstützte SWG-Verschlüsselungssuiten. Bitte beachten Sie, dass der SWG MPS (Modular Proxy Service) Proxy die TLS_CHACHA20_POLY1305_SHA256-Verschlüsselungs-Suite nicht unterstützt. Bitte beachten Sie, dass es einen separaten Artikel gibt, der die von SWG unterstützten Verschlüsselungssuiten und TLS behandelt. Wir können dieses Problem leicht lokalisieren, indem wir die Pakete prüfen, die während des Cipher-Suites-Austauschs in Client-Hello und Server-Hello erfasst wurden. Verwenden Sie zur Fehlerbehebung den CURL-Befehl, um die Verwendung bestimmter Chiffren zu erzwingen, um das Problem einzugrenzen und zu bestätigen, dass es sich um Verschlüsselungssuiten handelt, wie in Beispiel 1 und 2 gezeigt.

Beispiel für Curl-Befehle:

<#root>

```
curl -vvv "" --ciphers TLS_DHE_DSS_WITH_AES_256_GCM_SHA384 >> /dev/null
curl -vvv "" --ciphers ECDHE-RSA-AES256-GCM-SHA384 >> /dev/null
```

Testing website With 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
```

Testing website without Proxy

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

Mac/Linux:

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

Windows:

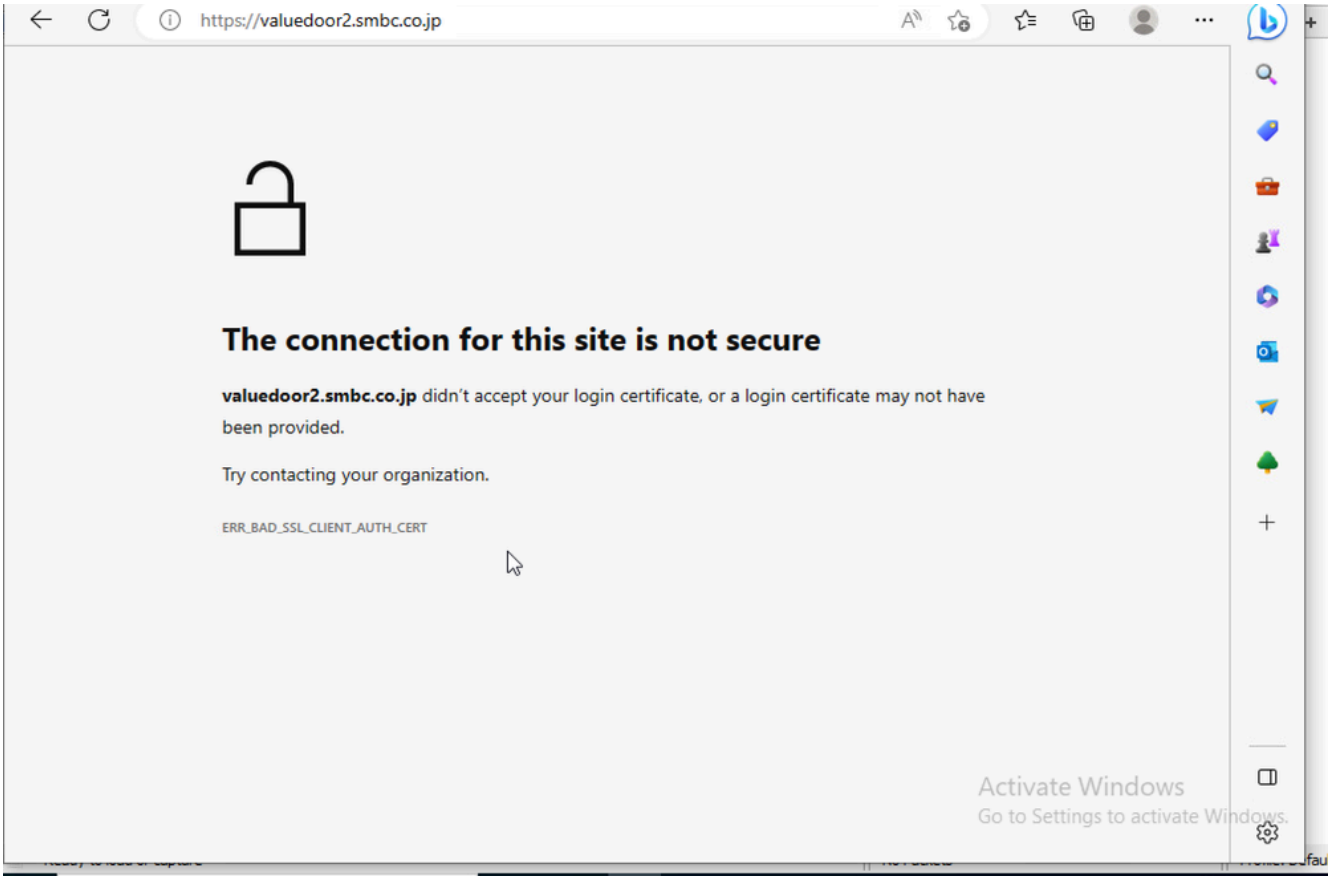
```
 - curl -vvv -o null -k -L www.cnn.com
```

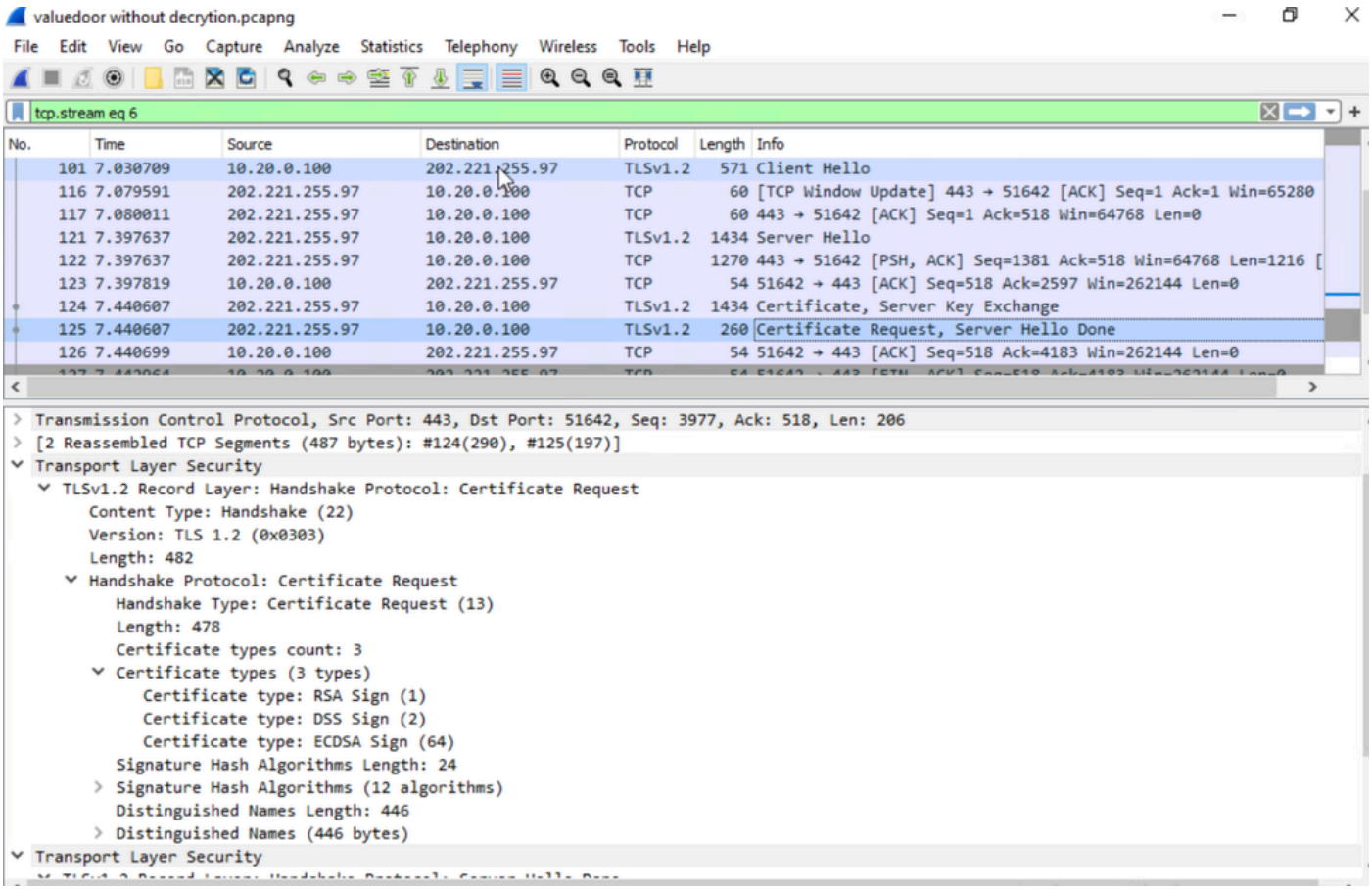
Auflösung

Um das Problem zu beheben, überspringen Sie die Suche nach der problematischen Website mithilfe der selektiven Entschlüsselungsliste.

Authentifizierungsanforderung für Clientzertifikat

Während des TLS-Handshakes zwischen dem SWG-Proxy und dem Upstream erwartet der Upstream-Webserver eine Client-Zertifikatsauthentifizierung. Da die Authentifizierung von Client-Zertifikaten nicht unterstützt wird, müssen diese Domänen vom Proxy mithilfe der externen Domänenverwaltungsliste umgangen werden, und die Umgehung der reinen HTTPS-Überprüfung reicht nicht aus. Beispiele: https://valuedoor2.smbc.co.jp

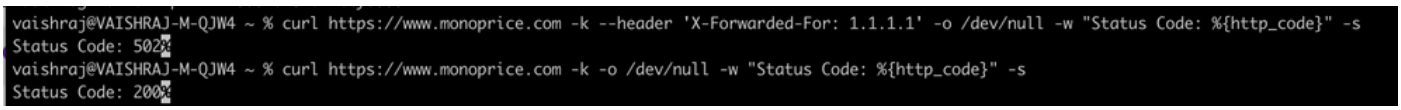




15027192992276

Von Proxy hinzugefügte Header

Der Webserver meldet 502 fehlerhafte Gateway-Fehler aufgrund des vom SWG-Proxy hinzugefügten X-Forward-For-Headers (XFF), wenn die HTTPS-Überprüfung aktiviert ist. Wir können die meisten Probleme mit schädlichen 502 Gateways eingrenzen, indem wir das Problem zuerst mit oder ohne HTTPS-Inspektion und mit oder ohne Dateiinspektion beheben, um das Problem mit dem MPS-Proxy-Scanner auszuschließen.



15123666760340

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

Wenn die HTTPS-Prüfung aktiviert ist, verwenden wir den XFF-Header, damit der Upstream-Server auf Basis der Client-IP (die den physischen Standort des Benutzers angibt) den optimalen Geolokalisierungsinhalt bereitstellen kann.

Wenn die HTTPS-Überprüfung nicht aktiviert ist, wird dieser Header vom Proxy nicht hinzugefügt. Es liegt also kein Fehler bei "502 Bad Gateway" vor. Dies ist kein Problem mit einem SWG-Proxy. Dieser Fehler ist auf den Upstream-Webserver zurückzuführen, der falsch konfiguriert ist, um den Standard-XFF-Header nicht zu unterstützen.

Auflösung

Um das Problem zu beheben, umgehen Sie die HTTPS-Prüfung für bestimmte Domänen mithilfe von selektiven Entschlüsselungslisten.

- 517 Upstream-Zertifikat widerrufen
- Fehler beim Zertifikat und TLS-Protokoll
- SWG DC manuell für interne Tests auswählen

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.