Fehler 502 / 504 GATEWAY_TIMEOUT beim Surfen auf bestimmten Websites

Inhalt

Frage:

Warum sehen wir 502/504 GATEWAY_TIMEOUT-Fehler beim Surfen auf bestimmten Websites?

Symptome: Benutzer erhalten beim Surfen auf bestimmten Websites 502 oder 504 Gateway-Timeout-Fehler von der Cisco WSA.

Benutzer erhalten beim Surfen auf Websites 502 oder 504 Gateway-Timeout-Fehler. Zugriffsprotokolle zeigen entweder "NONE/504" (KEINE/504) oder "NONE/502" (KEINE/502) an.

Beispiel für eine Zugriffsprotokollleitung:

1233658928.496 153185 10.10.70.50 **KEINE/504** 1729 GET http://www.example.com/ - DIRECT/www.example - .....

Es gibt viele Gründe, warum die WSA einen 502- oder 504-Gateway-Timeout-Fehler zurückgibt. Obwohl diese Fehlerantworten ähnlich sind, ist es wichtig, die kleinen Unterschiede zwischen ihnen zu verstehen.

Hier einige Beispiele für mögliche Szenarien:

- **502**: Die WSA hat versucht, eine TCP-Verbindung mit dem Webserver herzustellen, aber kein SYN/ACK erhalten.
- **504**: Die WSA erhält einen TCP-Reset (RST), der die Verbindung mit dem Webserver beendet.
- **504**: Die WSA erhält keine Antwort von einem erforderlichen Service, bevor sie mit dem Webserver kommuniziert, z. B. wenn DNS fehlschlägt.
- **504**: Die WSA hat eine TCP-Verbindung mit dem Webserver hergestellt und eine GET-Anforderung gesendet, die WSA erhält jedoch nie die HTTP-Antwort.

Nachfolgend finden Sie Beispiele für jedes Szenario und weitere Details zu potenziellen Problemen:

502: Die WSA hat versucht, eine TCP-Verbindung mit dem Webserver herzustellen, aber kein SYN/ACK erhalten.
Wenn der Webserver nicht auf die SYN-Pakete der WSA reagiert, wird dem Client nach einer

bestimmten Anzahl von Versuchen ein 502 Gateway-Timeout-Fehler gesendet.

Typische Ursachen hierfür sind:
1. Beim Webserver oder Webserver-Netzwerk treten Probleme auf.
2. Ein Netzwerkproblem im WSA-Netzwerk verhindert, dass die SYN-Pakete ins Internet gelangen.
3. Eine Firewall oder ein ähnliches Gerät verwirft entweder die WSA SYN-Pakete oder die SYN/ACK des Webservers.
4. IP-Spoofing ist auf der WSA aktiviert, aber nicht richtig konfiguriert (keine Rückgabepfad-Umleitung)

Schritte zur Fehlerbehebung:

Im ersten Schritt wird überprüft, ob die WSA einen ICMP-Ping an den Webserver senden kann. Dies kann mithilfe des folgenden CLI-Befehls erfolgen:
WSA> *ping*www.example.com
Wenn der Ping fehlschlägt, bedeutet dies nicht, dass der Server ausgefallen ist. Dies kann bedeuten, dass ICMP-Pakete irgendwo im Pfad blockiert werden. Wenn der Ping erfolgreich ist, können wir sicher sein, dass die WSA über eine einfache Layer-3-Verbindungsebene mit dem Webserver verfügt.
Ein Telnet-Test überprüft, ob die WSA eine TCP-Verbindung an Port 80 zum Webserver herstellen kann. Lesen Sie die Anweisungen in diesem Artikel zum Durchführen eines Telnet-Tests.

Netzwerkprobleme oder Firewall-Block
Wenn der Ping erfolgreich ist, das Telnet jedoch ausfällt, besteht die gute Möglichkeit, dass ein Filtergerät wie eine Firewall diesen Datenverkehr vom Netzwerk fernhält. Es wird empfohlen, die Firewall-Protokolle und/oder die Paketerfassungen von der Firewall auf weitere Details zu analysieren.
IP-Spoofing ist aktiviert, aber nicht richtig konfiguriert
Wenn die explizite Proxy-Funktion über die WSA oder den Telnet-Test erfolgreich ist, zeigt dies, dass die WSA direkt mit dem Webserver kommunizieren kann. Wenn jedoch ein Client die WSA mit IP-Spoofing durchführt, besteht ein Problem.

Ohne Client-IP-Spoofing:
- Die WSA sendet ein SYN mithilfe einer eigenen IP-Adresse als Quelle an den Webserver. Wenn das Paket zurückgesendet wird, wird es direkt an die WSA weitergeleitet.

Mit Client-IP-Spoofing:
- Die WSA sendet das SYN, verwendet jedoch stattdessen die IP des Clients als Quelle. Ohne eine spezielle Netzwerkeinrichtung wird das Rückgabepaket an den Client anstatt an die WSA gesendet.
- Um Client-IP-Spoofing verwenden zu können, muss das Netzwerk auf sehr spezifische Weise konfiguriert werden, um eine ordnungsgemäße Umleitung der Pakete zu ermöglichen. Wenn die Rückgabepfad-Pakete des Webservers an den Client anstatt an die WSA gesendet werden, wird die WSA die Server SYN/ACK nie sehen und einen 502 Gateway-Timeout-Fehler zurück an den Client senden.

504: Die WSA erhält einen TCP-Reset (RST), der die Verbindung mit dem Webserver beendet.
Wenn die WSA ein TCP-Reset-Paket für die Upstream-Verbindung zum Webserver empfängt,

sendet die WSA dem Client einen 504 Gateway-Timeout-Fehler.

Typische Ursachen hierfür sind:
1. Die Cisco Layer 4 Traffic Monitor (L4TM) blockiert den WSA-Proxy, um den Webserver anzuschließen.
2. Eine Firewall, IDS, IPS oder ein anderes Gerät zur Paketprüfung blockiert die WSA.

Schritte zur Fehlerbehebung:
Stellen Sie zuerst fest, ob der TCP-RST vom L4TM oder von einem anderen Gerät kommt. Wenn das L4TM diesen Datenverkehr blockiert, wird der Datenverkehr in den GUI-Berichten unter "***Monitor -> L4 Traffic Monitor***" angezeigt. Andernfalls kommt der RST von einem anderen Gerät.
L4TM-Blockierung:
Es wird empfohlen, Ports, auf denen der WSA-Proxy ebenfalls ausgeführt wird, nicht zu blockieren, wenn das L4TM blockiert wird. Dafür gibt es mehrere Gründe:
1. Der WSA-Proxy stellt im Problemfall eine benutzerfreundliche Fehlermeldung bereit, anstatt einfach nur die Verbindung zurückzusetzen. So wird die Verwirrung der Endbenutzer bei der Blockierung begrenzt.
2. Der WSA-Proxy kann bestimmte Inhalte scannen und blockieren, während der L4TM-Proxy den gesamten Datenverkehr blockiert, der einer Blacklist-IP-Adresse entspricht.
Um L4TM so zu konfigurieren, dass es keine Proxy-Ports blockiert, gehen Sie zu "***GUI -> Security Services -> L4 Traffic Monitor***".
Wenn es sich bei der Website um eine bekannte, schädliche Website handelt, der Datenverkehr jedoch aus bestimmten Gründen zugelassen werden sollte, kann die Website in der folgenden Liste als "weiß" angezeigt werden:
"***GUI -> Web Security Manager -> L4 Traffic Monitor -> Allow List***" (Liste zulassen)

Firewall-/IDS-/IPS-Blockierung:
Wenn ein anderes Gerät im Netzwerk die Verbindung der WSA mit dem Webserver blockiert, wird empfohlen, Folgendes zu analysieren:
1. Firewall-Blockprotokolle
2. Erfassung von Ein-/Ausgangs-Paketen während des Problems

Die Blockprotokolle können schnell bestätigen, ob das Gerät die WSA blockiert. Manchmal blockieren eine Firewall, IPS oder IDS den Datenverkehr und protokollieren ihn NICHT entsprechend. In diesem Fall kann der einzige Weg, aus dem der TCP-RST kommt, darin bestehen, ein- und ausgehende Erfassung vom Gerät zu erhalten. Wenn ein RST über die Eingangs-Schnittstelle gesendet wird und keine Pakete über die Ausgangsseite übertragen werden, ist das Sicherheitsgerät definitiv die Ursache.

504: Die WSA hat eine TCP-Verbindung mit dem Webserver hergestellt und eine GET-Anforderung gesendet, die WSA erhält jedoch nie die HTTP-Antwort.

Wenn die WSA eine HTTP GET-Nachricht sendet, jedoch keine Antwort empfängt, sendet sie dem Client einen 504 Gateway-Timeout-Fehler.

Typische Ursachen hierfür sind:

- Eine Firewall, IDS, IPS oder ein anderes Paket-Inspection-Gerät ermöglicht die TCP-Verbindung, verhindert jedoch, dass der HTTP-Inhalt den Webserver erreicht. In diesem Fall kann der Telnet-Test dazu beitragen, zu isolieren, welche HTTP-Daten blockiert werden.

Die Firewall-Blockprotokolle können schnell bestätigen, ob/warum das Gerät die WSA blockiert.

Manchmal blockieren eine Firewall, IPS oder IDS den Datenverkehr und protokollieren ihn NICHT entsprechend. In diesem Fall kann der einzige Weg, aus dem der TCP-RST kommt, darin bestehen, ein- und ausgehende Erfassung vom Gerät zu erhalten. Wenn ein RST über die Eingangs-Schnittstelle gesendet wird und keine Pakete über die Ausgangsseite übertragen werden, ist das Sicherheitsgerät definitiv die Ursache.

Testen der Verbindung mit einem Webserver mithilfe von Telnet

Führen Sie über die WSA-CLI den Befehl **telnet** aus:

WSA> **Telnet**
Wählen Sie die Schnittstelle aus, von der Sie Telnet senden möchten.
1. Automatisch
2. Management (192.168.15.200/24: wsa.hostname.com)
3. P1 (192.168.113.199/24: data.com)
[1]> **3**

Geben Sie den Remote-Hostnamen oder die IP-Adresse ein.
[]> www.example.com

Geben Sie den Remote-Port ein.
[25]> **80**

10.3.2.99 wird versucht..
Verbindung mit www.example.com hergestellt..
Escape-Zeichen ist '^]'.

Hinweis: Die rote Meldung "Connected" (Verbunden) weist darauf hin, dass TCP erfolgreich zwischen der WSA und dem Webserver eingerichtet wurde.

Eine HTTP-Anfrage kann auch manuell über diese Telnet-Sitzung gesendet werden. Nachfolgend finden Sie eine Beispielanforderung, die nach der Meldung "Verbunden" eingegeben werden kann:
—
http://www.example.com **HTTP/1.1**
HOST: www.example.com
{Enter}
—

Hinweis: Stellen Sie sicher, dass Sie am Ende den zusätzlichen Wagenrücklauf hinzufügen, da der Server ansonsten nicht auf die Anforderung antwortet.