502/504 GATEWAY_TIMEOUT-fouten bij het bladeren naar bepaalde sites

Inhoud

Vraag:

Waarom zien we 502 / 504 GATEWAY_TIME OUT fouten bij het bladeren naar bepaalde sites?

Symptomen: Gebruikers ontvangen 502 of 504 gateway-tijdelijke fouten van Cisco WSA bij het bladeren naar bepaalde websites

Gebruikers ontvangen 502 of 504 fouten in de gateway-time-out bij het bladeren naar websites. Toegangslogboeken tonen ofwel 'NONE/504' of 'NONE/502'

Logregel voorbeeldtoegang:

1233658928.496 153185 10.10.70.50 NO/504 1729 GET http://www.example.com/ - DIRECT/www.example.com - .....

Er zijn vele redenen waarom WSA een 502 of 504 gateway timeout fout kan terugkeren. Hoewel deze foutreacties vergelijkbaar zijn, is het belangrijk om de subtiele verschillen tussen ze te begrijpen.

Hier zijn een paar voorbeelden van de soorten scenario's die kunnen voorkomen:

- 502: De WSA heeft geprobeerd een TCP verbinding met de webserver te maken, maar heeft nog geen SYN/ACK ontvangen.
- 504: De WSA ontvangt een TCP reset (RST) die de verbinding met de webserver beëindigt.
- 504: De WSA krijgt geen antwoord van een vereiste dienst voorafgaand aan het communiceren met de webserver, zoals DNS faalt.
- 504: De WSA heeft een TCP-verbinding met de webserver tot stand gebracht en een GET-verzoek verstuurd, maar de WSA ontvangt nooit de HTTP-reactie.

Hieronder staan voorbeelden van elk scenario en meer details over mogelijke problemen:

502: De WSA heeft geprobeerd een TCP verbinding met de webserver te maken, maar heeft nog geen SYN/ACK ontvangen.

Als de webserver niet reageert op de SYN-pakketten van de WSA, wordt de client na een bepaalde hoeveelheid pogingen een Time-outfout met 502 Gateway gestuurd.

De typische oorzaken hiervan zijn:
1. Het webserver- of webservernetwerk heeft problemen.
2. Een netwerkkwestie op het netwerk WSA verhindert de pakketten SYN aan Internet te krijgen.
3. Een firewall of gelijkaardig apparaat laat vallen of de pakketten van WSA SYN of SYN/ACK van de webserver
4. IP-spoofing is ingeschakeld op de WSA, maar is niet goed geconfigureerd (geen omleiding van retourpad)

Stappen voor probleemoplossing:

De eerste stap is te verifiëren als WSA ICMP de webserver kan pingen. Dit kan worden gedaan met de volgende CLI-opdracht:

WSA> ping www.example.com

Als ping mislukt, betekent dit niet dat de server down is. Het kan betekenen dat ICMP-pakketten ergens op het pad worden geblokkeerd. Als pingelen slaagt, dan kunnen wij zeker weten dat WSA een basis layer3 niveau van connectiviteit aan de webserver heeft.

Een telnet-test zal controleren of de WSA de mogelijkheid heeft om een TCP-verbinding op poort 80 naar de webserver te maken. Zie de instructies verder in dit artikel voor het uitvoeren van een Telnet test.

Netwerkproblemen of firewallblokkering

Als pingelen succesvol is, maar het telnet mislukt, is er een goede mogelijkheid dat een filterapparaat, zoals een firewall, dit verkeer door het netwerk verhindert. Aanbevolen wordt dat de logbestanden van de firewall en/of de pakketopname van de firewall voor meer informatie worden geanalyseerd.

IP-spoofing inschakelen maar niet goed geconfigureerd

Als het uitdrukkelijk proxying door WSA of de Telnet test succesvol is, toont dit aan dat WSA rechtstreeks aan de Webserver kan communiceren, maar wanneer een cliëntvolmachten door WSA met IP voor de gek houden, is er een probleem.

Zonder client-IP-spoofing:

- De WSA stuurt een SYN naar de webserver met behulp van zijn eigen IP-adres als bron. Wanneer het pakket terugkomt, gaat het direct naar WSA.

Met client-IP-spoofing:

- De WSA verstuurt de SYN, maar gebruikt in plaats daarvan de IP van de client als bron. Zonder een speciale netwerkinstallatie wordt het retourpakket naar de client verzonden in plaats van naar de WSA.
- Om client IP spoofing te gebruiken, moet het netwerk op een zeer specifieke manier worden geconfigureerd om te vergemakkelijken dat de pakketten goed worden omgeleid. Als de webserver-retourpakpakketten naar de client worden verzonden in plaats van naar de WSA, zal de WSA nooit de servers SYN/ACK zien en zal een 502 Gateway Time-out fout terugsturen naar de client.

504: De WSA ontvangt een TCP reset (RST) die de verbinding met de webserver beëindigt.

Als de WSA een TCP reset-pakket ontvangt op zijn upstream verbinding met de webserver, zal de WSA een 504 Gateway Time-out-fout naar de client sturen.

De typische oorzaken hiervan zijn:
1. De Cisco Layer 4 Traffic Monitor (L4TM) blokkeert de WSA-proxy om verbinding te maken met de webserver.
2. Een firewall, IDS, IPS of ander pakketinspectieapparaat blokkeert de WSA.

Stappen voor probleemoplossing:

Bepaal eerst of de TCP RST afkomstig is van de L4TM of van een ander apparaat.

Als de L4TM dit verkeer blokkeert, verschijnt het verkeer in de GUI-rapporten onder "Monitor -> L4 Traffic Monitor". Anders komt de RST van een ander apparaat.

L4TM-blokkering:

Aanbevolen wordt om, als de L4TM blokkeert, niet te blokkeren op poorten waarop de WSA proxy ook actief is. Hiervoor zijn verschillende redenen:

1. De WSA proxy biedt een vriendelijke foutmelding in het geval van probleem, in plaats van alleen TCP resetten van de verbinding. Hierdoor wordt de verwarring bij de eindgebruikers beperkt wanneer zij worden geblokkeerd.
2. De WSA-proxy heeft de mogelijkheid om specifieke inhoud te scannen en te blokkeren, terwijl de L4TM alle verkeer blokkeert dat overeenkomt met een IP-adres dat op de zwarte lijst staat.

Als u wilt dat de L4TM niet wordt geblokkeerd op proxy-poorten, gaat u naar "GUI -> Security Services -> L4 Traffic Monitor".

Als de site een bekende slechte website is, maar er zijn redenen waarom het verkeer zou

moeten worden toegestaan, kan de site wit worden vermeld in:
"GUI -> Web Security Manager -> L4 Traffic Monitor -> Lijst toestaan"

Firewall/IDS/IPS-blokkering:

Als een ander apparaat op het netwerk de WSA blokkeert om verbinding te maken met de webserver, wordt aanbevolen om het volgende te analyseren:

1. Logboeken voor firewallblokkering
2. Ingres/uitgaand pakket neemt tijdens het probleem op

De bloklogboeken kunnen snel bevestigen of het apparaat de WSA blokkeert. Soms blokkeert een firewall, IPS of IDS het verkeer en wordt dit NIET correct vastgelegd. Als dit het geval is, is de enige manier om te bewijzen waar TCP RST uit komt, toegang en uitgang te verkrijgen van het apparaat. Als een RST wordt verzonden de ingangsinterface en geen pakketten door de uitgangskant worden gereisd, is het veiligheidsapparaat absoluut de oorzaak.

504: De WSA heeft een TCP-verbinding met de webserver tot stand gebracht en een GET-verzoek verstuurd, maar de WSA ontvangt nooit de HTTP-reactie.
Als de WSA een HTTP GET verstuurt, maar nooit een reactie ontvangt, zal het een 504 Gateway Time-out fout naar de client versturen. De typische oorzaken hiervan zijn: • Een firewall, IDS, IPS of ander pakketinspectieapparaat staat de TCP-verbinding toe, maar blokkeert de HTTP-inhoud om de webserver te bereiken. In dit geval, kan de Telnet test helpen isoleren welk soort HTTP- gegevens worden geblokkeerd. De logboeken van het firewallblok kunnen snel bevestigen als/waarom het apparaat WSA blokkeert. Soms blokkeert een firewall, IPS of IDS het verkeer en wordt dit NIET correct vastgelegd. Als dit het geval is, is de enige manier om te bewijzen waar TCP RST uit komt, toegang en uitgang te verkrijgen van het apparaat. Als een RST wordt verzonden de ingangsinterface en geen pakketten door de uitgangskant worden gereisd, is het veiligheidsapparaat absoluut de oorzaak.

Connectiviteit testen met een webserver met behulp van telnet

Vanaf de WSA CLI voert u de opdracht Telnet uit:

WSA> telnet

Selecteer de interface waaruit u wilt telnet.
1. Automatisch
2. Beheer (192.168.15.200/24: wsa.hostname.com)
3. P1 (1992.168.113.199/24: data.com)
[1]> 3

Voer de externe hostnaam of het IP-adres in.
[]> www.example.com

Voer de externe poort in.
[25]> 80

Proef 10.3.2.9...
Verbonden met www.example.com.
Escape is '^]'.

Opmerking: Het "Verbonden" bericht in rood geeft aan dat TCP succesvol is ingesteld tussen de WSA en de webserver.

Een HTTP-aanvraag kan ook handmatig via deze telnet-sessie worden verzonden. Het volgende is een voorbeeldverzoek dat kan worden getypt na het bericht "Connected":

ONTVANG http://www.example.com HTTP/1.1.
HOST: www.example.com
{Voer in}

Opmerking: Zorg ervoor dat de extra wagenterugloop aan het einde wordt toegevoegd, anders zal de server niet op de aanvraag reageren.

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.