Probleem met WSA Upstream Proxy Health Check na netwerkstoring

Inhoud

uitgifte

Na een langdurige netwerkonderbreking kan een Cisco Web Security Appliance (WSA) die is geconfigureerd om een upstream proxy te gebruiken die door FQDN is opgegeven, het doorsturen van verkeer naar een upstream proxy niet hervatten en in plaats daarvan rechtstreeks verkeer verzenden. Dit probleem manifesteert zich wanneer de WSA de upstream-proxy tijdens de netwerkstoring als "dood" markeert, maar niet herkent wanneer de upstream-proxy weer beschikbaar wordt, zelfs nadat de netwerkconnectiviteit is hersteld.

De specifieke symptomen die zijn waargenomen zijn:

- WSA geconfigureerd met upstream proxy via FQDN en "Failure Handling = go Direct"
- Langdurige netwerkonderbreking die van invloed is op de connectiviteit met zowel upstream proxy als DNS-server
- Na netwerkherstel tonen toegangslogs geen DEFAULT_PARENT-tags, wat aangeeft dat het verkeer de upstream-proxy blijft omzeilen
- Probleem treedt op bij één WSA-apparaat terwijl een ander apparaat in dezelfde omgeving normaal werkt

milieu

- Cisco Web Security Appliance (WSA) S-reeks
- AsyncOS 14.5.2-011 (getroffen versie)
- Hardware: S695
- Upstream proxy geconfigureerd met FQDN-specificatie

- Mislukte afhandeling geconfigureerd als "go Direct"
- Netwerkomgeving met L2-Switch-infrastructuur

resolutie

Dit probleem wordt opgelost door AsyncOS te upgraden naar een versie die de oplossing voor CSCwi13124 bevat. Deze bug is opgelost in deze AsyncOS-versies:

- AsyncOS 15.5.0-566
- AsyncOS 15.5.0-710

Tijdelijke workaround voor huidige versies

Voor omgevingen die niet onmiddellijk kunnen upgraden, is een tijdelijke mitigatie beschikbaar door de maximale inactieve time-out aan te passen voor het controleren van niet-reagerende upstream proxy's:

Stap 1: Toegang tot de CLI en navigeren naar geavanceerde proxyconfiguratie:

```
cli -> advancedproxyconfig -> MISCELLANEOUS
```

Stap 2: Wijzig de instelling voor de maximale inactieve time-out:

```
"Enter maximum idle timeout for checking unresponsive upstream proxy (in seconds)"
```

Stap 3: Verminder de standaardmaximumwaarde (86400 seconden/24 uur) tot een kleinere waarde om de tijd tussen de gezondheidscontroles te verkorten.

methode voor onmiddellijk herstel

Als het probleem momenteel de verkeersstroom beïnvloedt, kan de volgende opdracht onmiddellijk de upstream-proxyfunctionaliteit herstellen:

Stap 1: Toegang tot het diagnostische menu:

```
CLI > diagnostic > PROXY > kick
```

Hiermee wordt het proxyproces opnieuw gestart en worden normale upstream proxybewerkingen hersteld.

Validatie- en testprocedure

Als u wilt testen of het probleem aanwezig is of is opgelost na een upgrade, voert u de volgende stappen uit:

Stap 1: Basislijnbewaking instellen

Controleer toegangslogs en proxylogs om te bevestigen dat WSA verkeer naar de upstream proxy verzendt. Controleer of het verkeer de upstream-proxyzijde bereikt.

Stap 2: Netwerkonderbreking simuleren

Nadat u de normale verkeersstroom naar de upstream proxy hebt bevestigd, koppelt u deze verbindingen los:

- WSA naar upstream proxyverbinding
- WSA-naar-DNS-serververbinding

Stap 3: Foutdetectie bewaken

Controleer proxylogs en systeemlogs voor deze indicatoren:

- Proxylog kan upstream proxy weergeven als "... dood verklaard"
- Systeemlogboek kan "Kritiek: Maximaal aantal storingen bereikt bij het opvragen van DNS-

server ..." weergeven

Stap 4: Verstoorde toestand handhaven

Zonder het proxyproces opnieuw op te starten, moet u de status van de verbroken verbinding van stap 2 behouden en ongeveer 10 uur doorgaan met het genereren van verzoeken.

Stap 5: Connectiviteit herstellen

Herstel na ongeveer 10 uur de verbindingen die in stap 2 waren verbroken.

Stap 6: Bewaak het herstelgedrag

Nadat u stap 5 hebt voltooid, controleert u toegangslogs en proxylogs zonder het proxyproces opnieuw op te starten:

- In een vast systeem: het verkeer stroomt weer door de upstream-proxy en proxylogs tonen normale statusovergangen
- In een getroffen systeem: toegangslogboeken tonen het verkeer dat de upstream proxy blijft omzeilen, en proxylogs zullen geen "... was sick, now healthy" of "... was healthy, now sick" berichten tonen

Oorzaak

De grondoorzaak van dit probleem is een logische fout in het upstream proxy-gezondheidscontrolemechanisme. Wanneer WSA bepaalt dat een geconfigureerde upstream proxy "dood" (niet-reagerend) is, implementeert het een exponentieel back-off-algoritme dat het health-check-interval na elke storing verdubbelt. Dit interval kan maximaal 24 uur (86400 seconden) bereiken.

Dit probleem treedt op wanneer de upstream-proxy opnieuw beschikbaar komt tijdens een van deze verlengde intervallen. Hoewel de proxy zich heeft hersteld en normaal reageert, voert WSA geen gezondheidscontrole uit totdat het volledig geconfigureerde tijdsinterval is verstreken. Dit kan resulteren in maximaal 24 uur doorlopende directe verkeersroutering in plaats van het upstream proxygebruik te hervatten.

Dit gedrag is van invloed op WSA-configuraties waarbij:

- Upstream-proxy wordt opgegeven door DNS-hostnaam/FQDN (geen IP-adres)
- Failure Handling is ingesteld op "go Direct"
- Uitgebreide netwerkstoringen hebben invloed op zowel upstream proxy- als DNS-serverconnectiviteit

ID Cisco-bug: CSCwi13124

Gerelateerde inhoud

- Cisco Technical Support en downloads

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.