Oplossen van DNS-strafbaarstelling in MacOS en toegangsprobleem met interne domeinen

Inhoud

Inleiding

Achtergrondinformatie

- reikwijdte
- Symptomen

Probleem

Oplossing

- Optie 1
- Optie 2

Inleiding

In dit document wordt beschreven hoe u een probleem kunt oplossen met nieuwere versies van MacOS Big Sur die van invloed zijn op de DNS-resolutie.

Achtergrondinformatie

reikwijdte

- AnyConnect-beveiligingsmodule voor roaming of paraplu op het netwerk (zoals VA of doorsturen)
  - Paraplu standalone roaming client niet beïnvloed. Single-DNS omgeving is aanwezig waar alle DNS wordt overschreven met 127.0.0.1).
- Komt voor in omgevingen met meerdere netwerkinterfaces, maar slechts één kan interne adressen oplossen. Voorbeeld:
  - VPN en off-VPN
  - Meerdere NIC's - één bedrijfs- en één niet-bedrijfs

Symptomen

- Onvermogen (of intermitterend vermogen) om toegang te krijgen tot lokale domeinen met behoud van de mogelijkheid om toegang te krijgen tot openbare domeinen
  - NSLOOKUP wordt niet specifiek beïnvloed en blijft functioneren
    - Ping, traceroute, enz. lost het interne domein niet of onjuist op

Probleem

Dit probleem wordt veroorzaakt door code in MacOS die de manier behandelt waarop DNS-

resoluties worden beheerd in de aanwezigheid van meerdere DNS-servers. Dit kunnen meerdere resolvers op één netwerkadapter zijn of meerdere resolvers op verschillende netwerkadapters. Een DNS-server die reageert met GEWEIGERD wordt gedurende 60 seconden "bestraft". Wanneer dit gebeurt, worden alle verdere DNS-query's die tijdens deze periode plaatsvinden, geprobeerd op alternatieve DNS-servers die niet worden bestraft.

Als DHCP bijvoorbeeld twee DNS-servers adverteert voor een netwerk, A en B, en A reageert met GEWEIGERD, dan krijgt B gedurende 60 seconden de voorkeur boven A, zolang B niet wordt bestraft.

Als alle DNS-servers worden bestraft, dan geeft MacOS de voorkeur aan de minst recent gestrafte server. Als B bijvoorbeeld wordt bestraft terwijl A al was bestraft, dan geeft MacOS de voorkeur aan A boven B.

Dit wordt nog verergerd door de manier waarop MacOS 11 en hoger DoH (DNS over HTTPS) proberen te bevestigen. MacOS is geprogrammeerd om de voorkeur te geven aan een door de gebruiker ingestelde DoH-provider, indien mogelijk. Dit zou Umbrella DNS-beveiliging omzeilen, wat betekent dat we een GEWEIGERD antwoord (volgens RFC) retourneren wanneer MacOS een DoH-verzoek initieert. Vanwege DNS Penalization kan dit ertoe leiden dat interne domeinen niet correct worden opgelost. Voor meer informatie over dit probleem, zie dit artikel: DNS Resolver Selection in iOS 14 en macOS 11.

Oplossing

We weten nog niet of Apple van plan is dit gedrag te veranderen of dat Umbrella in staat is om hun gedrag te veranderen om dit probleem te omzeilen. Voorlopig zijn er twee opties die dienen als work around:

Optie 1

Schakel split-DNS in het groepsbeleid in en voeg specifiek de interne domeinen toe aan de split-DNS-configuratie, zodat ze alleen via tunnel kunnen worden opgelost. Dit zorgt ervoor dat die domeinen alleen via tunnel kunnen worden opgelost door de native OS-resolver, terwijl andere domeinen alleen buiten de tunnel kunnen worden opgelost.

Optie 2

Schakel tunnel-all-DNS in het groepsbeleid in om te voorkomen dat DNS-verkeer buiten de tunnel gaat.

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.