DNS-oplossingsconflicten tussen Cisco Secure Access en Banyan Security App

Inhoud

uitgeven

Wanneer Cisco Secure Access gelijktijdig wordt geïmplementeerd met de Banyan Security App op Windows-eindpunten, ervaren gebruikers aanzienlijke vertragingen in de DNS-resolutie en time-outs. De specifieke symptomen omvatten:

- De DNS-resolutie begint met time-out wanneer de Banyan Security App is verbonden.
- Webpagina's laden zeer langzaam, ondanks het feit dat ze uiteindelijk zijn opgelost.
- De Banyan App start een lokale DNS proxy op een loopback interface, vergelijkbaar met Umbrella gedrag.
- Deze DNS-proxyconfiguratie verstoort het normale DNS-resolutiegedrag.

Het probleem heeft vooral gevolgen voor gebruikers die toegang moeten krijgen tot externe omgevingen terwijl Cisco Secure Access wordt geïmplementeerd voor hun primaire netwerkbeveiliging.

milieu

- Cisco Secure Access geïmplementeerd met onderdelen voor internettoegang (roamingmodule, VA, DNS, SWG, PAC, IPS, certificaten)
- Banyan Security App draait op Windows-eindpunten
- Gebruikers die toegang nodig hebben tot externe omgevingen via Banyan terwijl ze Secure Access-connectiviteit behouden
- DNS-proxyservices die worden uitgevoerd op loopback-interfaces van beide toepassingen

- Interne domein-bypass al geconfigureerd in Secure Access voor FQDN-resolutie

resolutie

Om de DNS-oplossingsconflicten tussen Cisco Secure Access en Banyan Security App op te lossen, implementeert u deze benaderingen:

Primaire stappen voor probleemoplossing

Dit is een bekende Cisco Bug ID CSCwr21575 die bekende DNS-proxyconflicten tussen Cisco Secure Access en beveiligingstoepassingen van derden die lokale DNS-proxy's implementeren, aanpakt.

Symptoom

DNS-resolutie is niet of aanzienlijk vertraagd.

Voorwaarden

- DNS-query onderschept door Cisco Secure Client Umbrella-module.
- De primaire DNS-server is geconfigureerd voor een IP-adres uit het loopback-bereik 127.0.0.0/8 en de DNS-query richt zich op die server.
- Er is ten minste één andere niet-loopback IPv4 DNS-server op dezelfde of een andere adapter.

Tijdelijke oplossing

Stel de primaire DNS-server in op een IP-adres dat geen loopback is. De permanente oplossing is om Cisco Secure Client te upgraden naar 5.1.13 en hoger.

Verificatie en testen

Voer na het uitvoeren van de afwikkelingsstappen deze validatie uit:

- Test de DNS-resolutiesnelheid met zowel Cisco Secure Access als Banyan Security App actief
- De laadtijden van webpagina's controleren en terugkeren naar aanvaardbare niveaus
- Bevestig dat de toegang tot externe omgevingen via Banyan blijft functioneren
- Valideren dat interne domeinresolutie via Secure Access-bypass operationeel blijft

Oorzaak

De vertraging in de DNS-resolutie wordt veroorzaakt door conflicterende DNS-proxy-implementaties tussen Cisco Secure Access en de Banyan Security App. Beide toepassingen maken lokale DNS-proxy's op loopback-interfaces en maken concurrerende DNS-resolutiepaden die resulteren in time-outs en vertraagde reacties.

Het gedrag van de DNS-proxy van de Banyan Security App interfereert met de DNS-afhandeling van Cisco Secure Access, met name wat betreft de volgorde en prioriteit van de verwerking van DNS-query's op Windows-eindpunten.

Cisco bug ID CSCwr21575 pakt dit specifieke compatibiliteitsprobleem aan.

Verwante 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.