# F5 Load Balancer DNS Forwarding Configuration voor veilige toegang

## Inhoud

## uitgeven

De DNS-resolutie werkte niet bij het gebruik van een F5-taakverdeling als de client-DNS-server tijdens migratie van Umbrella naar Secure Access. Wanneer DNS-verzoeken het virtuele IP (VIP) raken, heeft de F5-taakverdeler met succes pakketten doorgestuurd naar back-end DNS-forwarders, maar hostnamen werden niet opgelost op eindpuntmachines. De DNS-resolutie werkte prima wanneer een virtueel toestel rechtstreeks als de client-DNS-server werd gebruikt, wat aangeeft dat het probleem specifiek was voor de F5-taakverdelingsconfiguratie.

Packet captures onthulden dat DNS-antwoorden het IP-adres van het virtuele apparaat gebruikten in plaats van het verwachte F5 VIP-adres. De clientcomputer verwachtte dat DNS-antwoorden afkomstig zouden zijn van het F5 VIP-adres, maar ontving in plaats daarvan antwoorden van het IP-adres van het back-end virtuele toestel.

## milieu

- Cisco Umbrella naar veilige toegangsomgeving voor migratie
- F5 load balancer met DNS load balancing VIP geconfigureerd
- Meerdere DNS-forwarders als back-endservers
- Virtuele apparaten die als DNS-servers dienen
- Client-eindpunten die een DNS-resolutie vereisen via de taakverdelingsfunctie

## resolutie

Het probleem is opgelost door de taakverdeling van F5 zodanig te configureren dat deze correct fungeert als proxy tussen de clientcomputers en de virtuele toestellen. De belangrijkste configuratiewijziging betrof het inschakelen van SNAT (Source Network Address Translation) met automatische toewijzingsfunctionaliteit.

## Diagnostische stappen uitgevoerd

Stap 1: DNS-resolutiegedrag controleren

De DNS-resolutie werd getest met behulp van zowel de F5 load balancer VIP als directe virtuele apparaatverbindingen om het probleem te isoleren.

Stap 2: DNS-verkeer vastleggen en analyseren

Packet captures werden uitgevoerd om de DNS-aanvraag- en responsstroom door de F5-taakverdelingsfunctie te analyseren.

Stap 3: Onjuiste bronadres identificeren

Uit analyse bleek dat DNS-antwoorden het IP-adres van het virtuele toestel bevatten in plaats van het F5 VIP-adres, waardoor verwarring bij de klant ontstond.

## Configuratiewijziging

Stap 1: Toegang tot de configuratie van de F5-taakverdeler

Navigeer naar de F5 load balancer management interface om de DNS VIP configuratie aan te passen.

Stap 2: SNAT-automatische toewijzing inschakelen

Configureer SNAT (Source Network Address Translation) om automatisch toe te wijzen op de F5-taakverdeling. Dit zorgt ervoor dat het F5-apparaat DNS-verzoeken en -antwoorden tussen clients en back-end DNS-servers op de juiste manier proxyleert.

Stap 3: Controleer de configuratie

Na het implementeren van de SNAT auto-map configuratie, DNS resolutie begon correct te werken door middel van de F5 load balancer.

## Oorzaak

De hoofdoorzaak was een onjuiste SNAT-configuratie (Source Network Address Translation) op de werklastverdeler van F5. Zonder SNAT auto-map ingeschakeld, was het F5-apparaat niet goed fungeert als een proxy voor DNS-verkeer. Hierdoor werden DNS-antwoorden rechtstreeks van de back-end virtuele toestellen naar de clientcomputers verzonden, waarbij het IP-adres van het virtuele toestel als bron werd gebruikt in plaats van het verwachte F5 VIP-adres. Clientcomputers verwachtten dat DNS-reacties afkomstig waren van hetzelfde IP-adres waarnaar ze hun verzoeken stuurden (de F5 VIP), maar kregen antwoorden van verschillende IP-adressen (de back-endservers), waardoor DNS-oplossingsfouten ontstonden.

## Verwante inhoud

- F5 GTM-taakverdeling configureren
- 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.