

Begrijp Paraplu DNS met QNAME-minimalisatie

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Overzicht](#)

[Begrijp queryminimalisatie](#)

[Mogelijke bijwerkingen](#)

Inleiding

In dit document wordt beschreven hoe het Cisco Umbrella Domain Name System (DNS) met QNAME-minimalisatie kan worden gebruikt.

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op Cisco Umbrella

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Overzicht

In juni 2019 heeft Cisco Umbrella ondersteuning toegevoegd voor het minimaliseren van querynamen ([RFC7816](#)). QNAME-minimalisatie is een privacygeoriënteerde functie in DNS die tot doel heeft het verzenden van de volledige domeinbestemming naar de root nameservers te beperken. Als gevolg hiervan wordt de stroom DNS-query's gewijzigd om de DNS-queryrespons te bepalen.

QNAME-minimalisatie is een wereldwijd onderwerp. Het Internet Systems Consortium heeft een [introductieartikel over QNAME-minimalisatie](#). Mozilla Firefox vereist dat resolvers QNAME-minimalisatie gebruiken voor DNS via HTTPS-implementaties en heeft een [artikel over dit](#)

[onderwerp.](#)

Begrijp queryminimalisatie

Query minimalisatie is een nieuwe data privacy-gerichte aanpak van DNS gezaghebbende query's. Om te onderzoeken wat queryminimalisatie is, begint u met een uitleg over hoe een DNS-verzoek momenteel werkt.

Omdat de meeste menselijke interactie met internet begint met een DNS-query, zijn big data over waar gebruikers naartoe gaan waardevolle informatie, die kan worden beschouwd als privégegevens.

In dit voorbeeld gaat u naar `umbrella.cisco.com`. U hebt een DNS-query nodig om te bepalen waar deze server zich bevindt, dus Umbrella stuurt die query naar een recursieve DNS-server om het antwoord van de autoriteit te vinden met behulp van deze stappen:

1. Gebruikersquery naar de recursieve DNS-resolver: `umbrella.cisco.com`
2. Recursieve DNS-server zoekt het antwoord van de root nameservers: waar kan ik vinden `umbrella.cisco.com` naar root > antwoord voor `.com`
3. Query op de `.com`-naamservers: `umbrella.cisco.com` naar `.com` > krijgt locatie van `cisco.com`-naamservers
4. Query naar `cisco.com` name servers: `umbrella.cisco.com` naar `cisco.com` > Antwoord verstrekt

In veel gevallen kan dit doorgaan met meerdere iteraties naar verschillende nameservers totdat een A-record is gevonden. In stap 1-2 zoekt Umbrella alleen actief naar de locatie van de `.com` nameservers. Het volledige `umbrella.cisco.com` domein wordt echter naar de root en `.com` nameserver gestuurd. Hetzelfde geldt voor de naamserver `cisco.com` die de volledige query ontvangt.

Met queryminimalisatie verschuift het algoritme naar alleen vragen om het vereiste detailniveau in de upstream-query's:

1. Gebruikersquery naar de recursieve DNS-resolver: `umbrella.cisco.com`
2. Recursieve DNS-server zoekt naar de root nameservers: waar kan ik `.com` > antwoord voor `.com` vinden
3. Query op de `.com`-naamservers: `cisco.com` naar `.com` > locatie van `cisco.com`
4. Query op de `cisco.com` nameservers voor `umbrella.cisco.com` > Antwoord

Dit werkt in de meeste gevallen geweldig en maakt het mogelijk om het antwoord te vinden zonder de unieke query te onthullen die wordt gemaakt voor de root- of TLD-naamservers.

Deze privacy is nog belangrijker voor domeinen die gebruik maken van EDNS Client Subnet, waarbij de DNS-autoriteit bij het opvragen wordt geïnformeerd over de bron van de gebruiker C-

Block (/24). Zonder QNAME-minimalisatie weten de root- en .com-naamservers (in dit voorbeeld) uw algemene locatie en waar u precies naartoe gaat. Met QNAME Minimization weten de roots alleen dat iemand op zoek is naar .com en wordt de privacy van de aanvrager behouden. Ze vereisen niet het detailniveau dat ze vandaag hebben zonder QMIN-privacybescherming.

Mogelijke bijwerkingen

QNAME minimalisatie werkt in de meeste gevallen zonder problemen. Het is echter onderhevig aan extra bronnen van mislukking in vergelijking met een directe zoekopdracht. Aangezien de volledige bestemming pas in de laatste stap van het proces aan de gezaghebbende nameserver wordt onthuld, kunnen onderbrekingen in de DNS-keten de resolutie van het domein verbreken. Hier is bijvoorbeeld een lange fictieve naam - `umbrellas.in.the.rain.umbrella.cisco.com`. Dit kan leiden tot deze vragen:

1. Wat is de nameservers voor .com naar de rootservers.
2. Wat is de nameservers voor `cisco.com` naar de .com-servers
3. Wat is de naamserver voor `umbrella.cisco.com` naar de `cisco.com` naamserver
4. Wat is de nameservers voor `rain.umbrella.cisco.com` naar de `umbrella.cisco.com` nameservers.
5. Wat is de nameservers voor `the.rain.umbrella.cisco.com` naar de `rain.umbrella.cisco.com` nameservers
6. Wat is de nameservers voor `in.the.rain.umbrella.cisco.com` naar de `rain.umbrella.cisco.com` nameservers: SERVFAIL
7. Wat is de nameservers voor `umbrellas.in.the.rain.umbrella.cisco.com` naar de `rain.umbrella.cisco.com` nameservers (niet eerder opgevraagd vanwege SERVFAIL)
8. Wat is het antwoord voor `umbrellas.in.the.rain.umbrella.cisco.com` op de `umbrellas.in.the.rain.umbrella.cisco.com` nameservers die eerder zijn gevonden (niet opgevraagd vanwege SERVFAIL eerder)

Aangezien de roots niet de volledige query krijgen, kan het zijn dat als een van de levels van het domein een NXDOMAIN, SERVFAIL, het IP van een RFC-1918 interne nameserver of een andere slechte respons retourneert, de query geen succesvol upstream autoritatief antwoord ontvangt. Als de zesde stap eerder (vet, onderstreept) bijvoorbeeld mislukt, kan de query voor `umbrellas.in.the.rain.umbrella.cisco.com` niet worden opgelost. Om deze problemen op te lossen, moet de domeineigenaar ervoor zorgen dat elk niveau een geldig publiek antwoord heeft.

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.