

DNS-resolutie koppelen aan CNAME-domeinbeleid en -rapportage

Inhoud

[Inleiding](#)

[Probleem](#)

[Oplossing](#)

[Oorzaak](#)

[Aanvullende informatie](#)

Inleiding

In dit document wordt beschreven hoe u uw DNS-oplossing kunt afstemmen op het beleid en de rapportage van uw CNAME-recorddomein.

Probleem

Wanneer u een DNS-cachingserver (Domain Name System) gebruikt, zoals BIND (met caching ingeschakeld) of Infoblox, komt uw DNS-resolutie niet overeen met het verwachte beleid en de rapportage voor uw CNAME-recorddomeinen. Een toegestaan A-record verzoek wordt beantwoord door een CNAME verwijzing naar een andere A-record op een ander, geblokkeerd domein.

domain.com is bijvoorbeeld toegestaan en blocked.com is geblokkeerd, terwijl domain.com een CNAME-record is dat verwijst naar blocked.com, dat een A-record heeft. Dit probleem presenteert zich als een toegestaan domein dat wordt geblokkeerd zonder dat een dergelijke gebeurtenis op het dashboard is geregistreerd.

Oplossing

Er zijn verschillende manieren om dit probleem op te lossen:

- DNS-caching uitschakelen voor DNS doorgestuurd naar Umbrella. Dit voorkomt dat dit probleem zich voordoet.
- Sta de doel-CNAME toe in het Umbrella Dashboard wanneer deze zich voordoen.
- Vermijd caching van het CNAME-recordtype of selectief niet-reactief cachebeïnvloede domeinen.

Oorzaak

De hoofdoorzaak van dit probleem is DNS-caching voor CNAME-records die verwijzen naar een ander domein, waar het doeldomein wordt geblokkeerd. Aangezien het domein is toegestaan,

markeert de Umbrella resolvers de gehele query als toegestaan, waarbij de CNAME-keten wordt weergegeven. Dit resulteert in een toegestane query.

Omdat verschillende domeinen variëren in TTL, en Umbrella block records voor kwaadaardige categorieën hebben een TTL van nul, caching interfereert.

Hier is een scenario waarin domain.com is toegestaan en blocked.com is geblokkeerd en domain.com is een CNAME-record dat verwijst naar blocked.com met een A-record.

Eerste zoekopdracht:

A-record voor domain.com: Allow list, CNAME voor blocked.com -> A-record query voor blocked.com, afkomstig van een CNAME, allow bit passed inside Umbrella - A-record voor blocked.com geretourneerd.

Analyse: Vragen gesteld aan Umbrella: domain.com -> blocked.com. Resultaat: toegestaan. Paraplu-logs domain.com zoals toegestaan, blocked.com zoals toegestaan.

Volgende zoekopdracht:

A-record voor domain.com: CACHED - het is een CNAME voor blocked.com -> A-record query voor blocked.com: CACHED - A-record voor blocked.com geretourneerd.

Analyse: Vragen gesteld aan Umbrella: None. Geen paraplu-logs.

Toekomstige query (veroorzaakt het probleem):

A-record voor domain.com: CACHED - het is een CNAME voor blocked.com -> A-record query voor blocked.com (standalone query - CNAME werd in de cache geplaatst) - geblokkeerd.

Analyse: Vragen gesteld aan Umbrella: blocked.com. Resultaat: geblokkeerd. Paraplu logt blocked.com als geblokkeerd.

Aanvullende informatie

- [Overkoepelende documentatie: DNS-resolutie](#)

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.