Begrijp waarom zoekopdrachten voor interne domeinen niet zijn aangemeld in Umbrella Insights

Inhoud

Inleiding

Overzicht

verklaring

Inleiding

In dit document wordt beschreven waarom query's voor interne domeinen niet worden vastgelegd.

Overzicht

Bij het gebruik van Umbrella Insights, waaronder de Virtual Appliance (VA) valt, mogen op alle werkstations alleen de DNS-serverinstellingen naar de VA's verwijzen. De VA's moeten worden geconfigureerd om uw bestaande interne DNS-servers te gebruiken. Op het dashboard kunt u een lijst met 'Interne domeinen' invoeren, zodat wanneer de client een DNS-query voor een interne bron maakt, de VA het verzoek doorstuurt naar een van de interne DNS-servers. Af en toe wordt ons gevraagd waarom geen van deze interne verzoeken in de logboekregistratie wordt weergegeven.

verklaring

Zoals hierboven beschreven, worden interne DNS-verzoeken die door de VA worden ontvangen, tijdens de installatie doorgestuurd naar een van de interne DNS-servers die op de VA zijn geconfigureerd. Deze zijn te zien op de console. Alles goed en wel, de interne DNS-server geeft een reactie en de VA stuurt dit terug naar de client.

Wanneer de client een DNS-verzoek doet voor een resource die NIET op de lijst van Interne domeinen staat, stuurt deze deze door naar de IP-adressen van Umbrella Anycast. Dit verzoek bevat extra gegevens in de DNS-query voor onze resolvers, waardoor het verzoek kan worden gekoppeld aan een oorsprong. De oorsprong kan bijvoorbeeld een UserID-hash, een bron-IP of een aantal andere identificerende factoren zijn die in dit uitgebreide DNS-pakket zijn opgenomen. Deze extra gegevens kunnen worden weergegeven door een specifieke DNS-query uit te voeren vanaf een opdrachtregel:

```
nslookup -server=208.67.222.222 -type=txt debug.opendns.com.
```

De daadwerkelijke registratie van DNS-verzoeken vindt plaats op onze resolvers. De registratie is afhankelijk van deze unieke informatie die aan het DNS-pakket wordt toegevoegd. De VA registreert de DNS-verzoeken niet waarop deze worden doorgestuurd. Het is vooral een recursieve DNS-server. Zodra onze public resolvers een DNS-query ontvangen, gebruikt het de uitgebreide gegevens die met de eigenlijke query zijn verzonden om de bron te identificeren, het juiste beleid toe te passen en de informatie van het verzoek te registreren en als deze is toegestaan of geblokkeerd, die vervolgens in het dashboard wordt weergegeven. Aangezien interne DNS-query's onze resolvers nooit zien, is het niet mogelijk om ze te registreren.

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.