DNS staat regel toe die niet overeenkomt wanneer deze wordt gevolgd door een regel om het even welke te weigeren

Inhoud

- uitgifte
- milieu
- resolutie
- Oorzaak
- Gerelateerde inhoud

---

uitgifte

Wanneer een internettoegangsbeleid is geconfigureerd met een regel voor het toestaan van DNS-verkeer, gevolgd door een regel voor het weigeren van een regel onderaan het beleid, komen DNS-verzoeken mogelijk niet overeen met de regel voor het verlenen van een vergunning. In plaats daarvan worden de DNS-verzoeken beoordeeld aan de hand van volgende regels en kunnen ze uiteindelijk worden geblokkeerd door het algemene blok.

Een beleid kan bijvoorbeeld als volgt worden geconfigureerd:

1. Vergunning — DNS-verkeer / elke bestemming
2. Ontkennen — Elk protocol / elke bestemming

In deze configuratie komt het DNS-verkeer niet overeen met de beoogde machtigingsregel en kan het worden geblokkeerd door de daaropvolgende regel Een willekeurige weigering weigeren.

Waarom dit verwarrend kan zijn

Met Cisco Secure Access kunnen beheerders toepassingsprotocollen selecteren, zoals:

- DNS
- DNS via HTTPS (DoH)
- DNS over TLS (DoT)

bij het configureren van een beleidsregel voor internettoegang.

Dit kan leiden tot de verwachting dat DNS-verkeer altijd onafhankelijk kan worden toegestaan of geweigerd met behulp van een applicatieprotocolvoorwaarde. DNS-verkeer is echter onderworpen aan specifiek beleid-evaluatiegedrag en toepassingsprotocol of servicegebaseerde voorwaarden (serviceobject) worden mogelijk niet geëvalueerd zoals verwacht in deze regelconfiguratie.

milieu

- Dit probleem is van toepassing op omgevingen met:
    - Cisco Secure Access (SSE)
    - Internettoegangsbeleid met meerdere regels
    - Een combinatie van op protocol/toepassing gebaseerde regels en een laatste regel voor een weigering
    - DNS-verkeer dat naar verwachting overeenkomt met een vorige machtigingsregel, maar in plaats daarvan wordt geblokkeerd door een volgende regel of het algemene blok

resolutie

Er is momenteel geen ondersteunde configuratie die garandeert dat een DNS-regel Permit Any/Any overeenkomt met DNS-verkeer, onafhankelijk van elkaar, wanneer deze wordt gevolgd door een regel Deny Any/Any in deze beleidsstructuur.

Klanten moeten op de hoogte zijn van deze beperking van de beleidsevaluatie bij het ontwerpen van internettoegangsbeleid dat een definitieve regel voor het weigeren van elke toegang bevat.

Als DNS-verkeer moet worden toegestaan, moet het beleid worden ontworpen met behulp van ondersteunde regelvoorwaarden die van toepassing zijn op het DNS-verkeer dat wordt geëvalueerd.

Oorzaak

DNS-verkeer wordt niet op dezelfde manier beoordeeld aan de hand van servicegebaseerde voorwaarden als algemeen toepassingsverkeer.

Wanneer een beleidsregel voorwaarden bevat die niet kunnen worden toegepast op het DNS-verkeer dat wordt geëvalueerd, komt de regel niet overeen. De beleidsevaluatie gaat dan verder naar de volgende toepasselijke regel.

Voorbeeld:

```
Rule 1: Permit DNS / Any
            |
            |-- DNS traffic does not match
            |
Rule 2: Deny Any / Any
            |
            |-- DNS traffic matches
            |
          BLOCK
```

Daarom garandeert het plaatsen van een DNS-regel voor vergunningen direct boven een regel voor het weigeren van een of meer DNS-verkeer niet dat het DNS-verkeer wordt toegestaan.

Gerelateerde inhoud

https://securitydocs.cisco.com/docs/csa/olh/121998.dita

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.