# Problemen met de zichtbaarheid van DNS/PTR-opzoekpakketten in FTD 7.4-pakketopnamen

## uitgeven

Wanneer het pakket wordt geblokkeerd door beveiligingsinformatie, worden DNS-query's niet weergegeven in de kwaadaardige domeinen die worden geblokkeerd door de FTD-beveiligingsinformatie. Verbindingsgebeurtenissen op de FTD-perimeter tonen het verkeer van de DNS-server die het domein bevraagt en bevestigen dat de FTD deze queryreacties blokkeert via beveiligingsinformatie. Dezelfde gebeurtenis toont echter ook een overeenkomst met een regel van het FTD-toegangsbeleid die doorgaans niet wordt verwacht. Het probleem lijkt verband te houden met de manier waarop Security Intelligence en PTR (reverse DNS) Lookup-pakketten op FTD's reageren bij het blokkeren van kwaadwillige domeinzoekopdrachten. Dit kan een gebeurtenis weergeven die overeenkomt met zowel een toegangsregel als beveiligingsinformatie.

## milieu

- Cisco Secure Firewall Firepower 7.4 (Firepower Management Center (FMC) / cdFMC / FDM) (van toepassing op alle systemen die gebruikmaken van beveiligingsinformatie)
- Softwareversie: 7.4.2 / 7.4.2.4 (van toepassing op alle systemen die gebruikmaken van veiligheidsinformatie)
- Perimeter Firepower-apparaat dat DNS-verkeer tussen Infoblox DNS-server en CIRA Cloud bewaakt
- Beveiligingsinformatie geconfigureerd om DNS crypto mining bedreigingen te blokkeren
- Laboratoriumtopologie met FPR2110- en FPR2100-apparatuur voor reproductie
- DNS-querytargeting domein: static.vdc.vn
- Dreigingsclassificatie: DNS crypto mining-dreiging
- Gebeurtenissen voor pakketopname en -verbinding geanalyseerd op Firepower-apparaat
- Infoblox DNS-server als interne DNS-infrastructuur

## resolutie

1. Analyseer verbindingsgebeurtenissen op de FTD om te bevestigen dat DNS-query's van de DNS-server naar het externe domein worden geblokkeerd door Security Intelligence vanwege een kwaadaardig domein. Een specifiek bron- en bestemming-IP-adres wordt genoteerd en de gebeurtenis kan zelfs een overeenkomst aangeven op een regel voor toegangsbeleid waarmee de eerste PTR-zoekopdracht van bron naar bestemming kan worden uitgevoerd. Dezelfde gebeurtenis toont echter ook een geblokkeerd door beveiligingsinformatie, terwijl de URL voor de query duidelijk wordt vermeld.

```
verbindingsgebeurtenis
```

Voorbeeld:

Domein: static.vdc.vn
Actie: geblokkeerd (DNS crypto mining dreiging)

2. Een pakketopname starten op het FTD dat zich richt op DNS-verkeer tussen de relevante IP-adressen. In een Wireshark-analyse van de opnames van het oorspronkelijke IP-adres wordt geen DNS-query gevonden die specifiek is voor het kwaadaardige domein in de uitvoer voor pakketopname.

```
FTD# capture CAP interface match udp host SRCIP host DESTIP eq 53
```

```
(geen uitvoer voor de verwachte pakketten)
```

- Volgens Cisco documentatie, Security Intelligence filtering is een vroege fase van toegangscontrole. Als een pakket overeenkomt met een Security Intelligence Block-lijst, kan het worden verwijderd voor verdere inspectie en voordat het wordt verwerkt door ander beleid (inclusief toegangscontrole, pakketregistratie, DNS-inspectie).
- Het filteren van Security Intelligence vindt plaats vóór een resource-intensieve inspectie.
- Pakketten die zijn geblokkeerd door Security Intelligence worden soms niet vastgelegd door standaard pakketafvangmechanismen op het apparaat.
- Voorfilterregels die zijn geëvalueerd voordat Security Intelligence wordt uitgevoerd, kunnen ook van invloed zijn op de zichtbaarheid.

3. Gebruik de url-si-debug-opdracht voor systeemondersteuning in de FTD CLISH om PTR-zoekopdrachten tussen bron- en bestemmings-IP's te traceren om te begrijpen hoe en waar het verkeer wordt verwerkt en geblokkeerd binnen de FTD en noteer de bronpoorten voor de pakketten.

```
> Systeemondersteuning URL-SI-debug
```

```
SRCIP 37046 -&gt; DSTIP 53 17 AS=0 ID=39 GR=1-1 InsightDnsListEventHandler: num_list_matched
[1], status 0x00010000, INSIGHT_FOUND (0x00010000) | SHMDB (1), static.vnpt.vn, si_list [
1048652 ]
SRCIP 49094 -&gt; DSTIP 53 17 AS=0 ID=42 GR=1-1 InsightDnsListEventHandler: num_list_matched
[1], status 0x00010000, INSIGHT_FOUND (0x00010000) | SHMDB (1), static.vnpt.vn, si_list [
1048652 ]
SRCIP 48508 -&gt; DSTIP 53 17 AS=0 ID=12 GR=1-1 InsightDnsListEventHandler: num_list_matched
[1], status 0x00010000, INSIGHT_FOUND (0x00010000) | SHMDB (1), static.vnpt.vn, si_list [
1048652 ]
```

4. Gebruik de bronpoorten als een verwijzing om te correleren met pakketopnames en logs van systeemondersteuningstrace. Dit is de beste methode om de bijbehorende ps te vinden. Zoals te zien is in dit volgende voorbeeld, worden de gerelateerde pakketten weergegeven als PTR (reverse DNS)-lookups in plaats van normale DNS-query's. Dit is de reden waarom de kwaadaardige domeinzoekopdracht niet kan worden gevonden bij het bekijken van opnames vanaf het oorspronkelijke IP-adres. Dit soort `pakketten raken een toegangsbeleid` dat op een gebeurtenis wordt weergegeven, zelfs als dezelfde verbinding wordt weergegeven als geblokkeerd door beveiligingsinformatie.

```
8847 2026-01-29 20:41:15.940854Z SRCIP DSTIP DNS 98 Standaardzoekopdracht 0x20ef PTR
23.172.189.113.in-addr.arpa OPT
9582 2026-01-29 20:41:18.348889Z SRCIP DSTIP DNS 98 Standaardzoekopdracht 0x8b58 PTR
23.172.189.113.in-addr.arpa OPT
10190 2026-01-29 20:41:21.556901Z SRCIP DSTIP DNS 98 Standaardzoekopdracht 0x636a PTR
23.172.189.113.in-addr.arpa OPT
11362 2026-01-29 20:41:24.652950Z SRCIP DSTIP DNS 99 Standaardzoekopdracht 0xf6f5 PTR
135.238.166.113.in-addr.arpa OPT
13670 2026-01-29 20:41:27.964885Z SRCIP DSTIP DNS 98 Standaardzoekopdracht 0xfb40 PTR
23.172.189.113.in-addr.arpa OPT
```

5. Controleer de antwoordpakketten voor deze PTR-zoekopdrachten vanaf de bestemming en het kwaadaardige domein kan worden gezien. Dit triggert de FTD om uiteindelijk de verbinding te blokkeren door middel van security intelligence, omdat het nu het kwaadaardige domein ziet.

```
981 2026-01-29 20:41:12.631818Z DSTIP SRCIP DNS 126 static.vnpt.vn Standaard queryrespons 0xc5c3
PTR 23.172.189.113.in-addr.arpa PTR static.vnpt.vn OPT
```

Coördineer met het klantenteam om te onderzoeken of er omgekeerde DNS-query's of onverwachte verkeerspatronen worden waargenomen voor bepaalde IP's die verband houden met de crypto-mijndreiging. Om specifiek verkeer toe te staan of verder te analyseren, voegt u de vereiste IP's toe aan de Do-Not-Block-lijst of laat u deze toe via prefilter, indien van toepassing. Dit kan latere inspectie en zichtbaarheid in pakketopname mogelijk maken.

- Voeg IP's toe aan de Do-Not-Block-lijst van Security Intelligence als verdere analyse vereist is.
- Als u de voorfilter toestaat, kan het verkeer het beveiligingsinformatieblok omzeilen.

## Oorzaak

De hoofdoorzaak is dat de PTR (reverse DNS) Lookup in eerste instantie door de FTD gaat via de toegangsregel omdat deze nog steeds in afwachting is van inspectie van veiligheidsinlichtingen. Het antwoordpakket voor de PTR-zoekopdracht bevat vervolgens de kwaadaardige domeinnaam. Wanneer een PTR-reactie overeenkomt met een vermelding in de lijst Security Intelligence Block (zoals gekoppeld aan DNS-crypto-mijndreiging), wordt het pakket verwijderd. Als gevolg hiervan wordt het schadelijke domein alleen gevonden in het antwoord op de PTR-zoekopdracht en gebeurtenissen tonen soms een overeenkomst op zowel een toegangsregel voor toestaan als een blok voor beveiligingsinformatie.

## Verwante inhoud

- Apparaatconfiguratiehandleiding van het Cisco Secure Firewall Management Center, 7.4: Informatie over beveiligingsinformatie
- Cisco Technical Support en downloads
- Cisco bug ID CSCwt16755 - DOC: PTR lookups passeren FTD door AC-beleid, maar respons wordt geblokkeerd door Security Intelligence

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.