

Problemen oplossen met DNS-activiteitenlogboekvermeldingen met beslissing geblokkeerd

Inhoud

uitgifte

Een of meer van deze symptomen worden gemeld:

- Activity Search (Monitor > Activity Search, gefilterd op DNS-gebeurtenissen) toont Decision/Action = Blocked voor een domein, maar het bekijken van de regels voor internettoegang onthult geen regel die het duidelijk blokkeert.
- Het domein is niet aanwezig in een Blokdoellijst die de beheerder onderhoudt.

milieu

- De informatie in dit document is gebaseerd op:
 - Cisco Secure Access (SSE)-cloudplatform
 - Cisco Secure Client 5.x met de Roaming Security Module geïmplementeerd en geregistreerd bij een organisatie voor beveiligde toegang

resolutie

Stap 1. Controleer de identiteit die is geëvalueerd

- Bevestig tegen welke identiteit de beslissing is genomen. Als de gebeurtenis een netwerk-, site- of tunnelidentiteit weergeeft in plaats van de verwachte zwervende computer of gebruiker, kwam de query overeen met een andere regelset dan die welke is beoordeeld.
- Controleer voor roamende gebruikers of het apparaat is geregistreerd en rapporteert als beveiligd

Identiteitsmismatch: corrigeer de implementatie zodat de beoogde identiteit wordt toegepast — registreer het roamingapparaat, corrigeer de toewijzing van AD/gebruikersgroepen of pas de set netwerkidentiteitsregels aan — in plaats van de regel los te maken die onjuist is afgestemd.

Stap 2: Controleer of er een beveiligingsrubriekmatch is

- Als de gebeurtenis een beveiligingscategorie bevat (Malware, C2, Phishing, Newly Seen Domains, DNS Tunneling, enzovoort), is het blok afkomstig van de beveiligingsinstellingen van de overeenkomende regelset - er hoeft geen bestemmingslijst of inhoudsregel naar het domein te verwijzen.
- Zoek de huidige reputatie en categorisering van het domein op de Cisco Talos Intelligence portal op <https://talosintelligence.com/> (Reputation Center lookup).
- Als de categorisatie of reputatie die in Talos wordt getoond onjuist is, dient u rechtstreeks via <https://talosintelligence.com/> een geschil/herclassificatieverzoek in (open een zaak) met Talos zodat het domein opnieuw wordt geëvalueerd. Zodra Talos de classificatie heeft bijgewerkt, wordt de wijziging doorgevoerd naar Secure Access-handhaving.

Stap 3: Inspecteer de CNAME keten

- Los het domein op vanuit een ongefilterd uitkijkpunt en inspecteer de volledige antwoordketen (bijvoorbeeld `graaf +noall +answer <domain>` of `nslookup -debug <domain>`).
- Controleer elk CNAME-doel in de keten tegen de bestemmingslijsten en tegen Talos-categorisatie; een geblokkeerd CNAME-doel verklaart een geblokkeerde beslissing over een ogenschijnlijk schoon gequery-domein

Stap 4: Herevalueer het beleid top-down voor de werkelijke identiteit

- Loop de regels voor internettoegang in volgorde als de identiteit van stap 1, controleer het bereik van de identiteit van elke regel, planning, ingeschakelde status en instellingen voor beveiliging/inhoud/toepassing, tot en met de standaardregel.
- Gebruik de Policy Tester (bijv. policy.test.sse.cisco.com/?=cisco.com) met de exacte identiteit en bestemming om te zien welke regel Secure Access rapporteert als de match, en vergelijk deze met de regel die op de gebeurtenis wordt genoemd.

Speciale case: nieuw geziene domeinen

Als de beveiligingscategorie op het evenement Nieuw gezien domeinen (NSD) is

Opties voor herstel, in volgorde van voorkeur:

Als het domein bedrijfskritiek is, voegt u het toe aan een bestemmingslijst Toestaan waarnaar wordt verwezen door de toepasselijke regel; een toegangsvermelding heeft voorrang op het NSD-beveiligingsblok voor die bestemming.

Versleutelde DNS (DoH) en QUIC uitschakelen

Gecodeerde DNS en QUIC kunnen leiden tot zichtbaarheidstekorten in de DNS-laag die bijdragen aan verwarrende zoekresultaten voor activiteiten: zoekopdrachten die zijn opgelost via de browser DoH bereiken nooit de Secure Access-resolvers (dus ze ontbreken volledig in het log), terwijl de DoH-provider-domeinen zelf kunnen verschijnen als geblokkeerde gebeurtenissen.

Het uitschakelen van deze transporten op beheerde eindpunten zorgt ervoor dat alle DNS controleerbaar blijft en dat het activiteitenlog het werkelijke eindpuntgedrag weergeeft.

DNS via HTTPS (DoH) per browser

Google Chrome

- Handleiding: ga naar <chrome://settings/security> en schakel Veilig DNS gebruiken uit.

Microsoft Edge

- Handleiding: ga naar `edge://settings/privacy` en schakel Veilig DNS gebruiken uit.

Mozilla Firefox

- Handleiding: Menu > Instellingen > Privacy en beveiliging > DNS via HTTPS (of Netwerkinstellingen op oudere versies) en selecteer Uit / deselecteer DNS via HTTPS inschakelen.
- Opmerking: Umbrella / Secure Access-resolvers beantwoorden het canarische domein van Mozilla (use-application-dns.net) op een manier die Firefox signaleert om DoH standaard uit te houden; expliciete GPO-instellingen worden nog steeds aanbevolen omdat de door de gebruiker ingestelde DoH-configuratie de kanariecontrole overschrijft. Let op: voeg de Mozilla kill-switch/canary-domeinen niet toe aan een blokbestedingslijst - een blokpagina A-record-reactie wordt als geldig beschouwd en kan ervoor zorgen dat Firefox zijn DoH-gebruik behoudt of bijwerkt.

QUIC (HTTP/3)

QUIC loopt over UDP/443 en kan zowel algemeen webverkeer als DoH3 (DNS over HTTP/3) vervoeren, waarbij inspectiepaden die TCP verwachten worden omzeild.

Door het uitschakelen van QUIC worden browsers gedwongen terug te vallen op TCP-gebaseerde HTTP/2 of HTTP/1.1, waardoor de volledige zichtbaarheid wordt hersteld:

- Chrome / Edge: Handmatig (niet-persistent, door de gebruiker te wijzigen): stel `chrome://flags/#enable-quic` / `edge://flags/#enable-quic` in op Uitgeschakeld.
- Firefox: stel het voorkeursnetwerk in `http.http3.enable = false` (over:config of policy/AutoConfig).

Als na deze stappen de overeenkomende regel die over de gebeurtenis wordt gerapporteerd, nog steeds niet kan worden aangesloten met de configuratie, opent u een kwestie met Cisco TAC en geeft u de export van de gebeurtenis Activity Search (tijdstempel met tijdzone, identiteiten, overeenkomende regel, categorieën, recordtype en domein) samen met screenshots van de relevante regels en bestemmingslijsten.

Oorzaak

Security category match (Talos-intelligentie) – Het domein wordt geblokkeerd door een beveiligingsinstelling - bijvoorbeeld Malware, Command and Control, Phishing, Cryptomining, DNS Tunneling of Newly Seen Domains - op basis van de reputatie en categorisering van Cisco Talos, niet door een bestemmingslijst of inhoudsregel die de beheerder expliciet heeft geconfigureerd. Dit is de meest voorkomende oorzaak van "geen duidelijke match" blokken.

Mismatch van identiteitsattributie – De zoekopdracht werd toegeschreven aan een andere identiteit dan verwacht (netwerk-/site-identiteit in plaats van de roamingcomputer, een andere AD-gebruiker/groep of een niet-geregistreerd apparaat dat terugvalt op een beleid op netwerkniveau), dus een andere — vaak strengere of standaardregel kwam overeen.

Regelvolgorde en de standaardregel – Een bredere regel hoger in het beleid (of de standaard/catch-all regel onderaan) die is gematcht vóór de beoogde regel Toestaan; de beoogde regel kan ook worden uitgeschakeld, gepland of afgebakend naar identiteiten die de betreffende bron niet bevatten.

Bestemmingslijst overerving – Een bestemmingslijst voor een blok bevat een bovenliggend domein (example.com), dat impliciet alle subdomeinen (app.example.com) omvat, of een IP/CIDR bevat waarnaar het domein overgaat. Het doorzoeken van de lijsten voor de exacte FQDN alleen komt hier niet aan het licht.

CNAME chain blocking – Het queried domein is toegestaan, maar de resolutieketen bevat een CNAME naar een domein (meestal een CDN, tracker of geparkeerde / geblokkeerde host) dat is geblokkeerd; de beslissing wordt toegepast op de keten, en het log toont het oorspronkelijk queried domein als geblokkeerd.

Toepassings- of inhoudscategorie overeenkomen – Het domein behoort tot een geblokkeerde toepassing (toepassingsbesturing) of inhoudscategorie die de beheerder er niet aan heeft gekoppeld; categorisatie kan verschillen van intuïtie (bijvoorbeeld een bedrijfstool die is gecategoriseerd als Bestandsdeling of Proxy/Anonymizer).

Recente beleids- of categorisatiewijziging - Het beleid of de Talos-categorisatie is onlangs gewijzigd; de gebeurtenis die wordt beoordeeld dateert van vóór (of na) de wijziging, of beleidspropagatie / klantsynchronisatie was niet voltooid op het moment van de zoekopdracht.

Gerelateerde inhoud

- [Interne DNS-servers configureren voor paraplu](#)
- [DNS configureren via HTTPS \(DoH\) met Umbrella](#)
- [Een domeincontroller toevoegen in Secure Access](#)
- [Informatie over Cisco Secure Access Block Page](#)
- [Cisco Technical Support en downloads](#)

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.