

Troubleshoot DNS Activity Log Entries with Decision Blocked

Contents

Issue

One or more of these symptoms are reported:

- Activity Search (Monitor > Activity Search, filtered to DNS events) shows **Decision/Action = Blocked** for a domain, but reviewing the Internet Access rules does not reveal a rule that obviously blocks it.
- The domain is not present in any Block destination list the administrator maintains.

Environment

- The information in this document is based on:
 - Cisco Secure Access (SSE) cloud platform
 - Cisco Secure Client 5.x with the Roaming Security Module deployed and registered to a Secure Access organization

Resolution

Step 1. Verify the identity that was evaluated

- Confirm which identity the decision was made against. If the event shows a network, site, or tunnel identity instead of the expected roaming computer or user, the query matched a different rule set than the one reviewed.
- For roaming users, verify the device is registered and reporting as Protected

Identity mismatch: Correct the deployment so the intended identity is applied — register the roaming device, fix AD/user-group mapping, or adjust the network identity rule set — instead of loosening the rule that incorrectly matched.

Step 2: Check for a security category match

- If the event carries a security category (Malware, C2, Phishing, Newly Seen Domains, DNS Tunneling, and so on), the block came from the security settings of the matched rule set — no destination list or content rule needs to reference the domain.
- Look up the current reputation and categorization of the domain on the Cisco Talos Intelligence portal at <https://talosintelligence.com/> (Reputation Center lookup).
- If the categorization or reputation shown in Talos is incorrect, submit a dispute/reclassification request (open a case) with Talos directly through <https://talosintelligence.com/> so the domain is re-evaluated. Once Talos updates the classification, the change propagates to Secure Access enforcement.

Step 3: Inspect the CNAME chain

- Resolve the domain from an unfiltered vantage point and inspect the full answer chain (for example, `dig +noall +answer <domain>` OR `nslookup -debug <domain>`).
- Check each CNAME target in the chain against the destination lists and against Talos categorization; a blocked CNAME target explains a Blocked decision on an apparently clean queried domain

Step 4: Re-evaluate the policy top-down for the actual identity

- Walk the Internet Access rules in order **as the identity from Step 1**, checking the identity scope of each rule, schedule, enabled state, and security/content/application settings, down to and including the default rule.
- Use the **Policy Tester** (eg - policy.test.sse.cisco.com/?=cisco.com) with the exact identity and destination to see which rule Secure Access reports as the match, and compare it to the rule named on the event.

Special Case: Newly Seen Domains

If the security category on the event is **Newly Seen Domains (NSD)**

Remediation options, in order of preference:

If the domain is business-critical, add it to an **Allow destination list** referenced by the applicable rule; an allow entry takes precedence over the NSD security block for that destination.

Disable Encrypted DNS (DoH) and QUIC

Encrypted DNS and QUIC can cause DNS-layer visibility gaps that contribute to confusing Activity Search results: queries resolved over browser DoH never reach the Secure Access resolvers (so they are missing from the log entirely), while the DoH provider domains themselves can appear as Blocked events.

Disabling these transports on managed endpoints ensures all DNS remains inspectable and the Activity Log reflects actual endpoint behavior.

DNS over HTTPS (DoH) per Browser

Google Chrome

- Manual: navigate to `chrome://settings/security` and turn off **Use secure DNS**.

Microsoft Edge

- Manual: navigate to `edge://settings/privacy` and turn off **Use secure DNS**.

Mozilla Firefox

- Manual: **Menu > Settings > Privacy & Security > DNS over HTTPS** (or Network Settings on older versions) and select *Off* / deselect **Enable DNS over HTTPS**.
- Note: Umbrella/Secure Access resolvers answer Mozilla canary domain (use-application-dns.net) in a way that signals Firefox to keep DoH off by default; explicit GPO settings are still recommended because user-set DoH configuration overrides the canary check. Caution: do not add the Mozilla kill-switch/canary domains to a block destination list — a block-page A-record response is treated as valid and can cause Firefox to keep or upgrade its DoH usage.

QUIC (HTTP/3)

QUIC runs over **UDP/443** and can carry both general web traffic and DoH3 (DNS over HTTP/3), bypassing inspection paths that expect TCP.

Disabling QUIC forces browsers to fall back to TCP-based HTTP/2 or HTTP/1.1, which restores full visibility:

- **Chrome / Edge:** Manual (non-persistent, user-changeable): set `chrome://flags/#enable-quic` / `edge://flags/#enable-quic` to *Disabled*.
- **Firefox:** set the preference `network.http.http3.enable = false` (about:config or policy/AutoConfig).

If, after these steps, the matched rule reported on the event still cannot be reconciled with the configuration, open a case with Cisco TAC and provide the Activity Search event export (timestamp with timezone, identities, matched rule, categories, record type, and domain) together with screenshots of the relevant rules and destination lists.

Cause

Security category match (Talos intelligence) – The domain is blocked by a security setting — for example Malware, Command and Control, Phishing, Cryptomining, DNS Tunneling, or **Newly Seen Domains** — based on Cisco Talos reputation and categorization, not by any destination list or content rule the administrator configured explicitly. This is the most frequent cause of "no obvious match" blocks.

Identity attribution mismatch – The query was attributed to a different identity than expected (network/site identity instead of the roaming computer, a different AD user/group, or an unregistered device falling back to a network-level policy), so a different — often stricter or default — rule matched.

Rule order and the default rule – A broader rule higher in the policy (or the default/catch-all rule at the bottom) matched before the intended Allow rule; the intended rule can also be disabled, scheduled, or scoped to identities that do not include the affected source.

Destination list inheritance – A Block destination list contains a parent domain (example.com), which implicitly covers all subdomains (app.example.com), or contains an IP/CIDR that the domain resolves to. Searching the lists for the exact FQDN alone does not surface this.

CNAME chain blocking – The queried domain is permitted, but its resolution chain contains a CNAME to a domain (commonly a CDN, tracker, or parked/blocked host) that is blocked; the decision is applied to the chain, and the log shows the originally queried domain as Blocked.

Application or content category match – The domain belongs to a blocked application (application control) or content category the administrator did not associate with it; categorization can differ from intuition (for example, a business tool categorized as File Sharing or Proxy/Anonymizer).

Recent policy or categorization change – The policy or the Talos categorization changed recently; the event under review predates (or postdates) the change, or policy propagation/client sync had not completed at the time of the query.

Related Content

- [Configure Internal DNS Servers for Umbrella](#)
- [Configure DNS over HTTPS \(DoH\) with Umbrella](#)
- [Add a Domain Controller in Secure Access](#)
- [Cisco Secure Access Block Page Information](#)
- [Cisco Technical Support & Downloads](#)