

Risoluzione dei problemi relativi alle voci del registro attività DNS con decisione bloccata

Sommario

Problema

Vengono riportati uno o più di questi sintomi:

- Ricerca attività (Monitoraggio > Ricerca attività, filtrata in base agli eventi DNS) mostra Decisione/Azione = Bloccato per un dominio, ma la revisione delle regole di accesso a Internet non rivela una regola che ovviamente la blocca.
- Il dominio non è presente in alcun elenco di destinazioni di blocco gestito dall'amministratore.

Ambiente

- Le informazioni fornite in questo documento si basano su:
 - Piattaforma cloud Cisco Secure Access (SSE)
 - Cisco Secure Client 5.x con il modulo Roaming Security distribuito e registrato in un'organizzazione Secure Access

Risoluzione

Passaggio 1. Verificare l'identità valutata

- Conferma l'identità contro cui è stata presa la decisione. Se nell'evento viene visualizzata un'identità di rete, di sito o di tunnel anziché il computer o l'utente comune previsto, la query corrisponderà a un set di regole diverso da quello esaminato.
- Per gli utenti in roaming, verificare che il dispositivo sia registrato e segnalare come protetto

Identità non corrispondente: Correggere la distribuzione in modo da applicare l'identità desiderata, ovvero registrare il dispositivo mobile, correggere il mapping AD/gruppo utenti o regolare il set di regole di identità di rete, anziché allentare la regola che non corrisponde correttamente.

Passaggio 2: Verificare che la categoria di protezione corrisponda

- Se l'evento include una categoria di protezione (Malware, C2, Phishing, Nuovi domini visualizzati, Tunneling DNS e così via), il blocco deriva dalle impostazioni di protezione del set di regole corrispondente. Nessun elenco di destinazione o regola di contenuto deve fare riferimento al dominio.
- Cercare la reputazione e la classificazione correnti del dominio sul portale Cisco Talos Intelligence all'indirizzo <https://talosintelligence.com/> (ricerca nel Reputation Center).
- Se la classificazione o la reputazione mostrata in Talos non è corretta, invia una richiesta di controversia/riclassificazione (apri una richiesta) a Talos direttamente tramite <https://talosintelligence.com/> in modo che il dominio venga rivalutato. Una volta che Talos aggiorna la classificazione, la modifica si propaga all'applicazione Secure Access.

Passaggio 3: Esaminare la catena CNAME

- Risolvere il dominio da una posizione privilegiata non filtrata ed esaminare la catena di risposte completa (ad esempio, digita `+noall +answer <domain> 0 nslookup -debug <domain>`).
- controllare ciascun oggetto CNAME nella catena confrontandolo con gli elenchi di destinazione e con la categorizzazione Talos; una destinazione CNAME bloccata spiega una decisione bloccata su un dominio interrogato apparentemente pulito

Passaggio 4: Rivalutare il criterio dall'alto verso il basso per l'identità effettiva

- Seguire le regole di accesso a Internet in ordine di identità dal passaggio 1, verificando

l'ambito di identità di ogni regola, pianificazione, stato abilitato e impostazioni di protezione/contenuto/applicazione, fino alla regola predefinita inclusa.

- Utilizzare Policy Tester (ad esempio, policy.test.sse.cisco.com/?=cisco.com) con l'identità e la destinazione esatte per verificare quale regola di Accesso sicuro segnala come corrispondenza e confrontarla con la regola indicata sull'evento.

Caso speciale: Domini visualizzati di recente

Se la categoria di protezione dell'evento è Nuovi domini visualizzati (NSD, Newly Seen Domains)

Opzioni di correzione in ordine di preferenza:

Se il dominio è business-critical, aggiungerlo a un elenco Consenti destinazione a cui fa riferimento la regola applicabile; una voce allow ha la precedenza sul blocco di sicurezza NSD per quella destinazione.

Disabilita DNS crittografato (DoH) e QUIC

Il DNS crittografato e la funzionalità QUIC possono causare gap di visibilità a livello DNS che contribuiscono a confondere i risultati della ricerca di attività: le query risolte tramite il browser DoH non raggiungono mai i resolver di accesso protetto (quindi risultano completamente mancanti nel log), mentre i domini del provider DoH stessi possono apparire come eventi Blocked.

La disattivazione di questi trasporti sugli endpoint gestiti garantisce che tutti i DNS rimangano ispezionabili e che il registro attività rifletta il comportamento effettivo dell'endpoint.

DNS su HTTPS (DoH) per browser

Google Chrome

- Manuale: passare a <chrome://settings/security> e disattivare Usa DNS sicuro.

Microsoft Edge

- Manuale: passare a `edge://settings/privacy` e disattivare Usa DNS sicuro.

Mozilla Firefox

- Manuale: Menu > Impostazioni > Privacy e sicurezza > DNS su HTTPS (o Impostazioni di rete sulle versioni precedenti) e selezionare Disattivato / deselezionare Abilita DNS su HTTPS.
- Nota: I resolver Umbrella/Secure Access rispondono al dominio canario Mozilla (use-application-dns.net) in un modo che indica a Firefox di mantenere il DoH disattivato per impostazione predefinita; le impostazioni esplicite dell'oggetto Criteri di gruppo sono ancora consigliate perché la configurazione DoH impostata dall'utente sostituisce il controllo canary. Attenzione: non aggiungere i domini kill-switch/canary Mozilla a un elenco di destinazione di blocco - una risposta di tipo blocco-pagina-record A viene considerata valida e può causare il mantenimento o l'aggiornamento dell'utilizzo di DoH da parte di Firefox.

RAPIDO (HTTP/3)

QUIC viene eseguito su UDP/443 e può trasmettere sia il traffico Web generale sia il protocollo DoH3 (DNS su HTTP/3), ignorando i percorsi di ispezione che prevedono TCP.

La disattivazione di QUIC forza i browser a tornare a HTTP/2 o HTTP/1.1 basati su TCP, ripristinando così la piena visibilità:

- Cromatura/Bordo: Manuale (non persistente, modificabile dall'utente): impostare `chrome://flags/#enable-quic` / `edge://flags/#enable-quic` su Disabled.
- Firefox impostare la preferenza `network.http.http3.enable = false` (`about:config` o `policy/AutoConfig`).

Se, dopo questi passaggi, la regola corrispondente segnalata sull'evento non può ancora essere riconciliata con la configurazione, aprire una richiesta con Cisco TAC e fornire l'esportazione evento Ricerca attività (timestamp con fuso orario, identità, regola corrispondente, categorie, tipo di record e dominio) insieme a screenshot delle regole e degli elenchi di destinazione pertinenti.

Causa

Corrispondenza categoria di sicurezza (intelligence Talos) - Il dominio è bloccato da un'impostazione di sicurezza, ad esempio Malware, Command and Control, Phishing, Cryptomining, Tunneling DNS o Nuovi domini visualizzati, in base alla reputazione e alla classificazione di Cisco Talos, non da un elenco di destinazione o da una regola di contenuto configurata esplicitamente dall'amministratore. Questa è la causa più frequente dei blocchi "senza corrispondenza ovvia".

Attributo di identità non corrispondente: la query è stata attribuita a un'identità diversa da quella prevista (identità di rete/sito invece del computer comune, un utente/gruppo AD diverso o un dispositivo non registrato che esegue il fallback a un criterio a livello di rete), quindi è stata soddisfatta una regola diversa, spesso più rigida o predefinita.

Ordine delle regole e regola predefinita: una regola più ampia a un livello superiore nel criterio (o la regola predefinita/catch-all alla fine) corrisponde prima della regola Allow prevista. la regola desiderata può inoltre essere disabilitata, pianificata o definita nell'ambito di identità che non includono l'origine interessata.

Ereditarietà elenco destinazioni - Un elenco Blocca destinazione contiene un dominio padre (example.com), che copre implicitamente tutti i sottodomini (app.example.com), o contiene un IP/CIDR risolto dal dominio. La ricerca negli elenchi del solo FQDN esatto non rileva questa condizione.

Blocco catena CNAME: il dominio sottoposto a query è consentito, ma la relativa catena di risoluzione contiene un CNAME a un dominio (in genere un CDN, un tracker o un host parcheggiato/bloccato) bloccato; la decisione viene applicata alla catena e il registro mostra il dominio originariamente interrogato come Bloccato.

Corrispondenza applicazione o categoria contenuto - Il dominio appartiene a un'applicazione bloccata (controllo applicazione) o a una categoria contenuto non associata dall'amministratore. la categorizzazione può differire dall'intuizione (ad esempio, uno strumento aziendale classificato come Condivisione file o Proxy/Anonimizzatore).

Modifica recente della politica o della classificazione - La politica o la classificazione Talos sono cambiate di recente; l'evento in esame è precedente o successivo alla modifica oppure la propagazione dei criteri o la sincronizzazione dei client non è stata completata al momento della query.

Contenuto correlato

- [Configura server DNS interni per Umbrella](#)
- [Configura DNS su HTTPS \(DoH\) con Umbrella](#)
- [Aggiungere un controller di dominio in Accesso sicuro](#)
- [Informazioni sulla pagina Cisco Secure Access Block](#)
- [Supporto tecnico Cisco e download](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).