

Dépannage des entrées du journal d'activité DNS avec décision bloquée

Table des matières

Problème

Un ou plusieurs de ces symptômes sont rapportés :

- Activity Search (Monitor > Activity Search, filtré sur les événements DNS) affiche Decision/Action = Blocked pour un domaine, mais la révision des règles d'accès à Internet ne révèle pas une règle qui le bloque évidemment.
- Le domaine ne figure dans aucune liste de destination de blocage gérée par l'administrateur.

Environnement

- Les informations contenues dans ce document sont basées sur :
 - Plate-forme cloud Cisco Secure Access (SSE)
 - Cisco Secure Client 5.x avec le module de sécurité d'itinérance déployé et enregistré auprès d'une organisation Secure Access

Résolution

Étape 1 : vérification de l'identité évaluée

- Confirmez l'identité contre laquelle la décision a été prise. Si l'événement indique une

identité de réseau, de site ou de tunnel au lieu de l'ordinateur ou de l'utilisateur itinérant attendu, la requête correspond à un ensemble de règles différent de celui examiné.

- Pour les utilisateurs itinérants, vérifiez que le périphérique est enregistré et signalez qu'il est protégé

Incompatibilité d'identité : Corrigez le déploiement afin que l'identité prévue soit appliquée (enregistrement du périphérique itinérant, correction du mappage AD/groupe d'utilisateurs ou ajustement de l'ensemble de règles d'identité réseau) au lieu de desserrer la règle qui correspond incorrectement.

Étape 2 :Recherchez une correspondance de catégorie de sécurité

- Si l'événement comporte une catégorie de sécurité (Malware, C2, Phishing, Domaines récemment vus, Tunnellisation DNS, etc.), le blocage provient des paramètres de sécurité de l'ensemble de règles correspondant : aucune liste de destination ou règle de contenu n'a besoin de référencer le domaine.
- Recherchez la réputation actuelle et la classification du domaine sur le portail Cisco Talos Intelligence à l'adresse <https://talosintelligence.com/> (recherche dans le Centre de réputation).
- Si la catégorisation ou la réputation indiquée dans Talos est incorrecte, envoyez une demande de litige/reclassification (ouvrir un dossier) à Talos directement via <https://talosintelligence.com/> afin que le domaine soit réévalué. Une fois que Talos a mis à jour la classification, la modification se propage à l'application Secure Access.

Étape 3 :Inspectez la chaîne CNAME

- Résolvez le domaine à partir d'un point de vue non filtré et inspectez la chaîne de réponse complète (par exemple, `dig +noall +answer <domain>` OU `nslookup -debug <domain>`).
- Vérifier chaque cible CNAME dans la chaîne par rapport aux listes de destination et à la catégorisation Talos ; une cible CNAME bloquée explique une décision bloquée sur un domaine interrogé apparemment propre

Étape 4 :Réévaluez la stratégie de haut en bas pour l'identité réelle

- Parcourez les règles d'accès à Internet dans l'ordre de l'identité à partir de l'étape 1, en vérifiant l'étendue de l'identité de chaque règle, planification, état activé et paramètres de sécurité/contenu/application, jusqu'à la règle par défaut incluse.
- Utilisez le Testeur de stratégie (par exemple, policy.test.sse.cisco.com/?=cisco.com) avec l'identité et la destination exactes pour voir quelle règle d'accès sécurisé signale comme la correspondance, et comparez-la à la règle nommée sur l'événement.

Cas particulier : Domaines récemment vus

Si la catégorie de sécurité de l'événement est Nouveaux domaines visibles (NSD)

Options de correction, par ordre de préférence :

Si le domaine est critique pour l'entreprise, ajoutez-le à une liste Autoriser la destination référencée par la règle applicable ; une entrée d'autorisation est prioritaire sur le bloc de sécurité NSD pour cette destination.

Désactiver le DNS chiffré (DoH) et QUIC

Les fonctions DNS et QUIC cryptées peuvent entraîner des lacunes de visibilité de la couche DNS qui contribuent à brouiller les résultats de la recherche d'activité : les requêtes résolues via le DoH du navigateur n'atteignent jamais les résolveurs Secure Access (ils sont donc totalement absents du journal), alors que les domaines du fournisseur DoH eux-mêmes peuvent apparaître comme des événements bloqués.

La désactivation de ces transports sur les points d'extrémité gérés garantit que tous les DNS restent inspectables et que le journal d'activité reflète le comportement réel des points d'extrémité.

DNS sur HTTPS (DoH) par navigateur

Google Chrome

- Manuel : accédez à <chrome://settings/security> et désactivez Utiliser le DNS sécurisé.

Microsoft Edge

- Manuel : accédez à `edge://settings/privacy` et désactivez Utiliser le DNS sécurisé.

Mozilla Firefox

- Manuel : Menu > Settings > Privacy & Security > DNS over HTTPS (ou Network Settings sur les versions antérieures) et sélectionnez Off / désélectionnez Enable DNS over HTTPS.
- Remarque : Les résolveurs Umbrella/Secure Access répondent au domaine canari Mozilla (use-application-dns.net) d'une manière qui signale à Firefox de maintenir le DoH désactivé par défaut ; Les paramètres d'objet de stratégie de groupe explicites sont toujours recommandés, car la configuration DoH définie par l'utilisateur remplace le contrôle Canary. Mise en garde : n'ajoutez pas les domaines kill-switch/canary Mozilla à une liste de destination de blocage — une réponse block-page A-record est considérée comme valide et peut amener Firefox à conserver ou à mettre à niveau son utilisation DoH.

QUIC (HTTP/3)

QUIC fonctionne sur UDP/443 et peut transporter à la fois le trafic Web général et DoH3 (DNS sur HTTP/3), en contournant les chemins d'inspection qui attendent TCP.

La désactivation de QUIC force les navigateurs à revenir à HTTP/2 ou HTTP/1.1 basé sur TCP, ce qui restaure une visibilité complète :

- Chrome / Périphérie : Manuel (non permanent, modifiable par l'utilisateur) : définissez `chrome://flags/#enable-quic` / `edge://flags/#enable-quic` sur Disabled.
- Firefox : définissez la préférence `network.http.http3.enable = false` (`about:config` ou `policy/AutoConfig`).

Si, après ces étapes, la règle correspondante signalée sur l'événement ne peut toujours pas être réconciliée avec la configuration, ouvrez un dossier auprès du TAC Cisco et fournissez l'exportation de l'événement de recherche d'activité (horodatage avec fuseau horaire, identités, règle correspondante, catégories, type d'enregistrement et domaine) ainsi que des captures d'écran des règles pertinentes et des listes de destinations.

Motif

Correspondance de catégorie de sécurité (intelligence Talos) - Le domaine est bloqué par un paramètre de sécurité (par exemple, Malware, Command and Control, Phishing, Cryptomining, DNS Tunneling ou domaines récemment vus) basé sur la réputation et la catégorisation de Cisco Talos, et non par une liste de destinations ou une règle de contenu configurée explicitement par l'administrateur. Il s'agit de la cause la plus fréquente de blocs « aucune correspondance évidente ».

Non-concordance d'attribution d'identité - La requête a été attribuée à une identité différente de celle attendue (identité réseau/site au lieu de l'ordinateur itinérant, un utilisateur/groupe AD différent, ou un périphérique non enregistré revenant à une stratégie de niveau réseau), de sorte qu'une règle différente — souvent plus stricte ou par défaut — correspond.

Ordre des règles et règle par défaut - Une règle plus large située plus haut dans la stratégie (ou la règle par défaut/fourre-tout en bas) correspond avant la règle Autoriser prévue ; la règle voulue peut également être désactivée, planifiée ou étendue à des identités qui n'incluent pas la source affectée.

Héritage de la liste de destinations : une liste de destinations Bloquer contient un domaine parent ([exemple.com](#)), qui couvre implicitement tous les sous-domaines ([app.exemple.com](#)), ou contient une adresse IP/CIDR vers laquelle le domaine est résolu. La recherche du seul nom de domaine complet exact dans les listes n'apparaît pas ici.

Blocage de la chaîne CNAME - Le domaine interrogé est autorisé, mais sa chaîne de résolution contient un CNAME vers un domaine (généralement un CDN, un tracker ou un hôte parqué/bloqué) qui est bloqué ; la décision est appliquée à la chaîne, et le journal affiche le domaine d'origine interrogé comme Bloqué.

Correspondance de catégorie d'application ou de contenu - Le domaine appartient à une application bloquée (contrôle d'application) ou à une catégorie de contenu à laquelle l'administrateur ne s'est pas associé ; la catégorisation peut différer de l'intuition (par exemple, un outil professionnel classé comme Partage de fichiers ou Proxy/Anonymiseur).

Changement récent de stratégie ou de catégorisation - La stratégie ou la catégorisation Talos a changé récemment ; l'événement en cours de révision précède (ou suit) la modification, ou la propagation de stratégie/synchronisation client n'était pas terminée au moment de la requête.

Autres informations utiles

- [Configuration des serveurs DNS internes pour Umbrella](#)

- [Configurer DNS sur HTTPS \(DoH\) avec Umbrella](#)
- [Ajouter un contrôleur de domaine dans Secure Access](#)
- [Informations sur la page de blocage Cisco Secure Access](#)
- [Assistance technique de Cisco et téléchargements](#)

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.