

Fehlerbehebung bei DNS-Aktivitätsprotokolleinträgen mit gesperrter Entscheidung

Inhalt

Problem

Eines oder mehrere dieser Symptome werden berichtet:

- Die Aktivitätssuche (Überwachen > Aktivitätssuche, nach DNS-Ereignissen gefiltert) zeigt die Entscheidung/Aktion = Gesperrt für eine Domäne an. Beim Überprüfen der Internetzugriffsregeln wird jedoch keine Regel angezeigt, die diese offensichtlich blockiert.
- Die Domäne ist in keiner vom Administrator verwalteten Zielblockliste vorhanden.

Umwelt

- Die Informationen in diesem Dokument basieren auf:
 - Cisco Secure Access (SSE) Cloud-Plattform
 - Cisco Secure Client 5.x mit implementiertem und bei einer Secure Access-Organisation registriertem Roaming-Sicherheitsmodul

Auflösung

Schritt 1: Überprüfen der bewerteten Identität

- Bestätigen Sie, gegen welche Identität die Entscheidung getroffen wurde. Wenn das Ereignis eine Netzwerk-, Standort- oder Tunnelidentität anstelle des erwarteten Roaming-Computers oder -Benutzers anzeigt, stimmte die Abfrage mit einem anderen Regelsatz überein als der überprüfte.
- Für Roaming-Benutzer stellen Sie sicher, dass das Gerät registriert ist und als geschützt gemeldet wird.

Identitätskonflikt: Korrigieren Sie die Bereitstellung so, dass die beabsichtigte Identität angewendet wird - registrieren Sie das Roaming-Gerät, korrigieren Sie die AD/Benutzergruppenzuordnung, oder passen Sie den Regelsatz für die Netzwerkidentität an -, anstatt die falsch zugeordnete Regel zu lockern.

Schritt 2: Überprüfen der Übereinstimmung mit der Sicherheitskategorie

- Wenn das Ereignis eine Sicherheitskategorie trägt (Malware, C2, Phishing, neu erkannte Domänen, DNS-Tunneling usw.), stammt der Block aus den Sicherheitseinstellungen des übereinstimmenden Regelsatzes. Es muss keine Zielliste oder Inhaltsregel auf die Domäne verweisen.
- Die aktuelle Reputation und Kategorisierung der Domäne finden Sie im Cisco Talos Intelligence-Portal unter <https://talosintelligence.com/> (Reputationscenter-Suche).
- Wenn die in Talos angegebene Kategorisierung oder Reputation nicht korrekt ist, reichen Sie einen Streitfall/eine Neuklassifizierungsanfrage (eröffnen Sie ein Ticket) bei Talos direkt über <https://talosintelligence.com/> ein, damit die Domain neu bewertet wird. Sobald Talos die Klassifizierung aktualisiert, wird die Änderung auf die Durchsetzung von Secure Access übertragen.

Schritt 3: Überprüfen der CNAME-Kette

- Lösen Sie die Domäne von einem ungefilterten Aussichtspunkt aus auf, und überprüfen Sie die gesamte Antwortkette (z. B. `dig +noall +answer <domain>` oder `nslookup -debug <domain>`).
- Überprüfen Sie jedes CNAME-Ziel in der Kette anhand der Ziellisten und der Talos-Kategorisierung. Ein blockiertes CNAME-Ziel erklärt eine Blockierungsentscheidung für eine anscheinend unschädliche abgefragte Domäne.

Schritt 4: Richtlinie von oben nach unten für die tatsächliche Identität neu bewerten

- Gehen Sie die Internet Access-Regeln in der Reihenfolge als Identität aus Schritt 1 durch, und überprüfen Sie den Identitätsbereich jeder Regel, jeden Zeitplan, den aktivierten Status sowie die Sicherheits-, Content- und Anwendungseinstellungen bis hin zur Standardregel.
- Verwenden Sie den Richtlinien tester (z. B. policy.test.sse.cisco.com/?=cisco.com) mit der genauen Identität und dem genauen Ziel, um festzustellen, welche Regel Secure Access-Berichte übereinstimmen, und vergleichen Sie sie mit der auf dem Ereignis benannten Regel.

Sonderfall: Neu erkannte Domänen

Wenn die Sicherheitskategorie des Ereignisses "Newly Seen Domains (NSD)" (Neu erkannte Domänen) ist

Sanierungsoptionen, nach Priorität sortiert:

Wenn die Domäne geschäftskritisch ist, fügen Sie sie einer Zulassungszielliste hinzu, auf die die entsprechende Regel verweist. Eine allow-Eingabe hat Vorrang vor dem NSD-Sicherheitsblock für dieses Ziel.

Verschlüsselten DNS (DoH) und QUIC deaktivieren

Verschlüsselter DNS und QUIC können Sichtbarkeitslücken in der DNS-Schicht verursachen, die zu verwirrenden Ergebnissen der Aktivitätssuche beitragen: über den Browser aufgelöste Anfragen DoH erreichen niemals die Secure Access-Resolver (daher fehlen sie vollständig im Protokoll), während die DoH-Provider-Domänen selbst als gesperrte Ereignisse angezeigt werden können.

Durch das Deaktivieren dieser Transporte auf verwalteten Endpunkten wird sichergestellt, dass alle DNS-Server inspizierbar bleiben und das Aktivitätsprotokoll das tatsächliche Verhalten der Endpunkte widerspiegelt.

DNS über HTTPS (DoH) pro Browser

Google Chrome

- Handbuch: navigieren Sie zu `chrome://settings/security`, und deaktivieren Sie Sicheres DNS verwenden.

Microsoft Edge

- Handbuch: navigieren Sie zu `edge://settings/privacy`, und deaktivieren Sie Sicheres DNS verwenden.

Mozilla Firefox

- Handbuch: Menü > Einstellungen > Datenschutz und Sicherheit > DNS über HTTPS (oder Netzwerkeinstellungen bei älteren Versionen), und wählen Sie Aus/Deaktivieren DNS über HTTPS aktivieren.
- Anmerkung: Umbrella/Secure Access-Resolver antworten Mozilla-Kanariendomäne (use-application-dns.net) auf eine Weise, die Firefox signalisiert, DoH standardmäßig auszuschalten; Explizite GPO-Einstellungen werden weiterhin empfohlen, da die vom Benutzer festgelegte DoH-Konfiguration die Kanarienüberprüfung überschreibt. Vorsicht: fügen Sie die Mozilla Kill-Switch-/Kanariendomänen nicht zu einer Block-Zielliste hinzu — eine Block-Page-A-Record-Antwort wird als gültig behandelt und kann dazu führen, dass Firefox seine DoH-Nutzung beibehält oder aktualisiert.

QUIC (HTTP/3)

QUIC läuft über UDP/443 und kann sowohl allgemeinen Web-Datenverkehr als auch DoH3 (DNS über HTTP/3) übertragen und so Prüfpfade umgehen, die TCP erwarten.

Wenn QUIC deaktiviert wird, müssen Browser auf TCP-basiertes HTTP/2 oder HTTP/1.1 zurückgreifen, wodurch die volle Transparenz wiederhergestellt wird:

- Chrom/Rand: Manuell (nicht persistent, vom Benutzer änderbar): setzen Sie `chrome://flags/#enable-quic` / `edge://flags/#enable-quic` auf Disabled.
- Firefox: Legen Sie die Einstellung `network.http.http3.enable = false` fest (`about:config` oder `policy/AutoConfig`).

Wenn nach diesen Schritten die für das Ereignis gemeldete übereinstimmende Regel immer noch

nicht mit der Konfiguration abgeglichen werden kann, öffnen Sie ein Ticket beim Cisco TAC, und stellen Sie den Ereignisexport für die Aktivitätssuche (Zeitstempel mit Zeitzone, Identitäten, übereinstimmenden Regeln, Kategorien, Datensatztyp und Domäne) zusammen mit Screenshots der relevanten Regeln und Ziellisten bereit.

Ursache

Übereinstimmung der Sicherheitskategorie (Talos-Informationen) - Die Domäne wird durch eine Sicherheitseinstellung blockiert, z. B. Malware, Command-and-Control, Phishing, Cryptomining, DNS Tunneling oder neu erkannte Domänen. Diese Einstellung basiert auf der Reputation und Kategorisierung von Cisco Talos und nicht auf einer vom Administrator ausdrücklich konfigurierten Zielliste oder Inhaltsregel. Dies ist die häufigste Ursache für "keine offensichtlichen Übereinstimmungen".

Identitätsattribut-Diskrepanz - Die Abfrage wurde einer anderen Identität zugeordnet als erwartet (Netzwerk-/Standortidentität anstelle des Roaming-Computers, ein anderer AD-Benutzer/eine andere AD-Gruppe oder ein nicht registriertes Gerät, das auf eine Richtlinie auf Netzwerkebene zurückgreift), sodass eine andere — oft strengere oder standardmäßige — Regel zugeordnet wurde.

Regelreihenfolge und Standardregel - Eine umfassendere Regel höher in der Richtlinie (oder die Standard-/catch-all-Regel am unteren Rand), die vor der beabsichtigten Zulassungsregel abgeglichen wurde. Die beabsichtigte Regel kann auch deaktiviert, geplant oder auf Identitäten beschränkt werden, die die betroffene Quelle nicht enthalten.

Vererbung der Zielliste - Eine Zielliste für die Sperrung enthält eine übergeordnete Domäne (example.com), die implizit alle Unterdomänen (app.example.com) **abdeckt**, oder enthält eine IP/CIDR, in die die Domäne aufgelöst wird. Die Suche in den Listen nach dem genauen FQDN allein ist hierfür nicht geeignet.

CNAME-Kettenblockierung - Die abgefragte Domäne ist zulässig, aber ihre Auflösungskette enthält einen CNAME für eine Domäne (in der Regel ein CDN, Tracker oder geparkter/blockierter Host), die blockiert ist. Die Entscheidung wird auf die Kette angewendet, und das Protokoll zeigt die ursprünglich abgefragte Domäne als Blocked an.

Übereinstimmung mit Anwendung oder Inhaltskategorie - Die Domäne gehört zu einer blockierten Anwendung (Anwendungskontrolle) oder Inhaltskategorie, die der Administrator nicht zugeordnet hat. Kategorisierung kann von Intuition abweichen (z.B. ein Business Tool, das als File Sharing oder Proxy/Anonymizer kategorisiert ist).

Jüngste Policy- oder Kategorisierungsänderung - Die Policy- oder die Talos-Kategorisierungsänderung wurde kürzlich geändert. Das überprüfte Ereignis geht der Änderung voraus (oder aktualisiert sie), oder die Richtlinienpropagierung/Clientsynchronisierung war zum Zeitpunkt der Abfrage nicht abgeschlossen.

Verwandte Inhalte

- [Interne DNS-Server für Umbrella konfigurieren](#)
- [DNS über HTTPS \(DoH\) mit Umbrella konfigurieren](#)
- [Hinzufügen eines Domänencontrollers in sicherem Zugriff](#)
- [Cisco Secure Access - Blockseiteninformationen](#)
- [Technischer Support und Downloads von Cisco](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.