

決定がブロックされたDNSアクティビティログエントリのトラブルシューティング

内容

問題

次の1つ以上の症状が報告されます。

- アクティビティ検索 (Monitor > Activity Search、DNS eventsでフィルタリング) では、ドメインのDecision/Action = Blockedと表示されますが、インターネットアクセスルールを確認しても、明らかにブロックしているルールは判明しません。
- ドメインは、管理者が保持するどのブロック宛先リストにも存在しません。

環境

- このドキュメントの情報は、次のハードウェアに基づくものです。
 - Cisco Secure Access(SSE)クラウドプラットフォーム
 - Cisco Secure Client 5.x (Secure Access組織に導入および登録されたRoamingセキュリティモジュールを搭載)

解決方法

ステップ 1：評価されたIDを確認する

- 決定が行われたIDを確認します。イベントで、予期されるローミングコンピューターまたは

ユーザーではなく、ネットワーク、サイト、またはトンネルIDが示される場合、クエリは確認されたものとは異なるルールセットに一致しました。

- ローミングユーザの場合は、デバイスが登録され、保護として報告されていることを確認します

IDの不一致：一致しないルールを緩める代わりに、目的のIDが適用されるように展開を修正します（ローミングデバイスの登録、AD/ユーザグループマッピングの修正、またはネットワークIDルールセットの調整）。

手順2：セキュリティカテゴリの一致を確認します。

- イベントがセキュリティカテゴリ（マルウェア、C2、フィッシング、新しく見られたドメイン、DNSトンネリングなど）を含む場合、ブロックは一致したルールセットのセキュリティ設定から取得されます。宛先リストまたはコンテンツルールはドメインを参照する必要はありません。
- Cisco Talosインテリジェンスポータル(<https://talosintelligence.com/>)でドメインの現在のレピュテーションとカテゴリを検索します（レピュテーションセンターの検索）。
- Talosに表示される分類またはレピュテーションが正しくない場合、<https://talosintelligence.com/>からTalosにクレーム/再分類リクエストを直接提出（ケースをオープン）して、ドメインを再評価してください。Talosが分類を更新すると、その変更がセキュアアクセスに適用されます。

手順3:CNAMEチェーンを確認します。

- フィルタリングされていない観点からドメインを解決し、完全な応答チェーン（たとえば、`dig +noall +answer <domain>`または`nslookup -debug <domain>`）を調べます。
- チェーン内の各CNAMEターゲットを宛先リストとTalosカテゴリに照らし合わせて確認します。ブロックされたCNAMEターゲットは、明らかにクリーンなクエリ済みドメインでブロックされた決定を説明します

手順4：実際のIDに対するポリシーのトップダウンを再評価します。

- ステップ1のIDとしてインターネットアクセスルールを順番に確認し、各ルールのID範囲、

スケジュール、有効な状態、およびセキュリティ、コンテンツ、アプリケーションの設定を確認して、デフォルトルールまで進めます。

- ポリシーテスター (例 : policy.test.sse.cisco.com/?=cisco.com) を使用して、正確なIDと宛先を指定し、Secure Accessによってどのルールが一致としてレポートされるかを確認して、イベントで指定されたルールと比較します。

特殊なケース：新しく検出されたドメイン

イベントのセキュリティカテゴリが新しく認識されたドメイン(NSD)

修復オプション (優先順) :

そのドメインがビジネスに不可欠な場合、適用可能なルールによって参照される許可宛先リストにそのドメインを追加します。許可エントリは、その宛先のNSDセキュリティブロックよりも優先されます。

暗号化されたDNS(DoH)とQUICの無効化

暗号化されたDNSおよびQUICは、DNS層の可視性のギャップを引き起こし、混乱を招く可能性があります。アクティビティ検索結果：ブラウザDoH経由で解決されたクエリは、Secure Accessリゾルバに到達しません (そのため、ログには完全に欠落しています) 。一方、DoHプロバイダードメイン自体はBlockedイベントとして表示されます。

管理対象エンドポイントでこれらのトランスポートを無効にすると、すべてのDNSが検査可能な状態になり、アクティビティログに実際のエンドポイントの動作が反映されます。

ブラウザごとのDNS over HTTPS(DoH)

Google Chrome

- 手動 : <chrome://settings/security> に移動し、Use secure DNSをオフにします。

Microsoft Edge

- 手動 : edge://settings/privacyに移動し、Use secure DNSをオフにします。

Mozilla FireFox

- Manual: Menu > Settings > Privacy & Security > DNS over HTTPS (または、旧バージョンではNetwork Settings)を選択し、Offを選択するか、Enable DNS over HTTPSの選択を解除します。
- 注 : Umbrella/Secure Accessリゾルバは、Mozillaのカナリドメイン(use-application-dns.net)に対して、DoHをデフォルトでオフにするようにFirefoxに通知する方法で応答します。ユーザ設定のDoH設定によってカナリチェックが上書きされるため、依然として明示的なGPO設定が推奨されます。注意 : ブロック宛先リストにMozilla kill-switch/canaryドメインを追加しないでください。ブロックページのA-record応答が有効として扱われ、FirefoxでDoH使用率が維持またはアップグレードされる可能性があります。

QUIC(HTTP/3)

QUICはUDP/443上で動作し、一般的なWebトラフィック(DNS over HTTP/3)とDoH3(DNS over HTTP/3)の両方を伝送でき、TCPを期待するインスペクションパスをバイパスします。

QUICを無効にすると、ブラウザはTCPベースのHTTP/2またはHTTP/1.1にフォールバックされ、完全な可視性が復元されます。

- Chrome / Edge:手動 (非永続的、ユーザ変更可能) :chrome://flags/#enable-quic / edge://flags/#enable-quicをDisabledに設定します。
- Firefox:プリファレンスnetwork.http.http3.enable = false (about:configまたはpolicy/AutoConfig)を設定します。

これらの手順を実行しても、イベントで報告された一致するルールを設定と照合できない場合は、Cisco TACでケースをオープンし、アクティビティ検索イベントのエクスポート (タイムスタンプとタイムゾーン、ID、一致するルール、カテゴリ、レコードタイプ、ドメイン) と、関連するルールと宛先リストのスクリーンショットを提供します。

原因

セキュリティカテゴリー一致 (Talosインテリジェンス) – ドメインが、マルウェア、コマンドおよ

び制御、フィッシング、クリプトマイニング、DNSトンネリング、Newly Seen Domainsなどのセキュリティ設定によってブロックされます。Cisco Talosのレピュテーションと分類に基づいており、管理者が明示的に設定した宛先リストやコンテンツルールによってブロックされることはありません。これは、「明らかに一致しない」ブロックの最も頻繁な原因です。

Identity attribution mismatch：クエリの原因が予期されたIDとは異なるため（ローミングコンピュータの代わりにネットワーク/サイトID、別のADユーザ/グループ、またはネットワークレベルのポリシーにフォールバックする未登録デバイス）、異なる（多くの場合、より厳密またはデフォルトの）ルールが一致しました。

ルールの順序とデフォルトルール：ポリシー内で上位にあるより広範なルール（または最下部のdefault/catch-allルール）が、目的のAllowルールの前に一致します。目的のルールは、無効化、スケジュール設定、または影響を受ける送信元が含まれていないIDへのスコープ設定も可能です。

宛先リストの継承：ブロックの宛先リストには、親ドメイン(example.com)が含まれます。このドメインはすべてのサブドメイン(app.example.com)を暗黙的にカバーしているか、ドメインの解決先であるIP/CIDRが含まれています。正確なFQDNだけをリストで検索しても、この問題は発生しません。

CNAMEチェーンブロッキング：クエリされたドメインは許可されますが、解決チェーンには、ブロックされたドメイン（通常はCDN、トラッカー、またはパーク/ブロックされたホスト）へのCNAMEが含まれます。決定はチェーンに適用され、ログには最初にクエリされたドメインがブロックされたことが示されます。

アプリケーションまたはコンテンツカテゴリの一致：ドメインが、ブロックされたアプリケーション（アプリケーションコントロール）または管理者が関連付けていないコンテンツカテゴリに属している。カテゴリ化は、直感とは異なる場合がある（たとえば、ファイル共有またはプロキシ/アノニマイザとして分類されたビジネスツール）。

最近のポリシーまたはカテゴリの変更：ポリシーまたはTalosのカテゴリが最近変更されました。レビューのプレデート（またはポステート）中のイベントが変更されたか、クエリの時点でポリシーの伝達/クライアントの同期が完了しませんでした。

関連コンテンツ

- [Umbrella用の内部DNSサーバの設定](#)
- [Umbrellaを使用したDNS over HTTPS\(DoH\)の設定](#)
- [セキュアアクセスでのドメインコントローラの追加](#)

- [Cisco Secure Access Blockページ情報](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。