

ChromeOS SWGのWeb保護が機能せず、アクティビティ検索にWebログが継続的に表示されない

内容

問題

組織でSecure Web Gateway(SWG)保護が有効と表示されているにもかかわらず、ChromeOSユーザのWebログが生成されませんでした。影響を受けるChromeOSエンドポイントでは、DNSレベルの保護のみが表示され、アクティビティ検索インターフェイスにSWG/Webログアクティビティは表示されませんでした。SWG保護のステータスが有効であると示している間、ユーザはWebトラフィックログがまったく表示されなくなっていました。

調査中、診断ログで、エンドポイントhttp://407.checkumbrella.comへの同期エラーが繰り返し発生し、HTTP 407 (プロキシ認証が必要) エラー応答が返されていることが判明しました。ChromeOSクライアント/拡張機能がプロキシサービスで正しく認証できず、SWG保護が正しくアクティブ化されず、その後Webログが生成されません。

環境

- シスコセキュアアクセス
- Cisco Secure Accessクライアント/拡張機能を備えたChromeOSエンドポイント
- ChromeOS管理用Google管理コンソール

解決方法

この問題は、影響を受けるChromeOSユーザを含むGoogle管理組織単位(OU)の基本認証認証(BAUTH)認証スキームを有効にし、ポリシーのリロードを実行してSWG保護を有効にすることに

よって解決されました。

ステップ1：ログの収集と分析

HARキャプチャを収集し（ネットワークおよびコンソールログを確認）、同期障害の根本原因を特定します。Cisco Secure Accessサービスとの同期を試みたときに、ログに繰り返し認証エラーが記録されました。

ステップ2:Google管理OUの基本認証を有効にします

Google管理コンソールで、影響を受けるChromeOSユーザが含まれている組織単位(OU)に移動し、基本認証認証スキームを有効にします。これにより、ChromeOSクライアント/拡張機能がCisco Secure Accessプロキシサービスで正しく認証されるようになります。

ステップ3：ポリシーのリロードおよび検証

基本認証を有効にした後、影響を受けるChromeOSデバイスでポリシーのリロードを実行します。保護ステータスをチェックして、SWG保護がアクティブになることを確認します。SWG保護は、DNSレベルの保護だけでなく、アクティブとして表示される必要があります。

ステップ4：検証

影響を受けるChromeOSユーザからのWebブラウジングのアクティビティをテストし、Webログが生成され、アクティビティ検索インターフェイスに表示されることを確認します。ログには、適切なWebトラフィック検査とSWGサービスを介したログインが示されている必要があります。

原因

ChromeOSクライアント/拡張機能で、該当ユーザを含むGoogle管理組織単位(OU)の基本認証認証スキームが無効にされています。基本認証を有効にしないと、ChromeOSデバイスがCisco

Secure Accessプロキシサービスで正しく認証されず、同期試行中にHTTP 407 (プロキシ認証が必要) エラーが発生します。これにより、SWG保護が適切にアクティブ化されなくなり、デバイスがDNSのみの保護にフォールバックし、Webログの生成が妨げられました。

関連コンテンツ

- [Cisco Secure Accessの基本情報のトラブルシューティングと収集](#)
- [Cisco Secure Access Chromebookクライアント](#)
- [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。