PACファイルのセキュアアクセスSWGプロキシ接続問題のトラブルシューティング

内容

お問い合わせ内容

SWG(Secure Web Gateway)プロキシURL swg-url-proxy-https-8xxxx.sseproxy.qq.opendns.comを使用してCisco Secure Access経由でWebサイトにアクセスしようとすると、接続エラーが発生します。

具体的な症状は次のとおりです。

- Web要求（https://www.google.comなど）がブラウザの接続エラーで失敗した
- アクティビティ検索ログにトラフィックが表示されない
- クライアントの送信元IP/クライアントの出力IPから宛先エンドポイントへのサーバのリセットが確認されました。
    - k8s-sigpro-sigpro-c10eb6eb-38fbeb0455191ac5.elb.eu-central-1.amazonaws.com
    - k8s-sigpro-sigpro-f8f3d861-14341dd91e659675.elb.eu-central-1.amazonaws.com
- 問題はCESTの午前9時30分頃に発生
- SWGホスト名のDNS解決が正常に機能していた
- ポート443のswg-url-proxy-https-8xxxx.sseproxy.qq.opendns.comへのTelnet接続に成功
- 外部ファイアウォールが宛先IPへの接続をブロックしていなかった

パケットキャプチャ分析により、プロキシから送られるTCP RSTパケットが明らかになり、プロキシレベルでの接続の終了が示されました。

環境

- テクノロジー：Cisco Secure Access(SSE)
- コンポーネント：Secure Web Gateway(SWG)
- SWGプロキシURL:swg-url-proxy-https-8385532.sseproxy.qq.opendns.com
- 該当ポート：443および80
- オリジナルNAT IP:20.x.x.x
- 更新されたNAT IP:21.x.x.x
- AWS ELBエンドポイント（例：eu-centralまたはus-east region）
- ブラウザをSWGプロキシに誘導するWPAD設定

解決策

問題は、正しいNAT IPアドレスを含むようにallow-list設定を更新することで解決されました。

次のセクションで説明する手順は、問題を特定して解決するために実行されました。

ステップ1：診断データの収集

トラフィックフローとプロキシ設定を分析するために、収集されたパケットキャプチャとWPADスクリプト設定。

さらに、主な手がかりはhttps://policy.test.sse.cisco.comで「401 unauthorized」エラーが表示されていたことです。これは、http接続要求がプロキシにヒットしているが、プロキシがポリシーを適用し、トラフィックを許可するために、OrgIDやその他のメタデータの詳細に基づいてユーザトラフィックを認証できないことを意味します。

ステップ2：トラフィック分析

パケットキャプチャの分析により、次のことが明らかになりました。

- プロキシからTCP RSTパケットが送信されました
- アクティビティ検索ログに失敗したトラフィックが表示されませんでした
- トラフィックフローの送信元IPが変更された

ステップ3:NAT IPアドレスの識別

調査の結果、NATパブリックIPアドレスが20.x.x.xから21.x.x.xに変更されていることがわかりました。変更されたIPはユーザCSA UIに登録済みネットワークとして追加され、SWGトラフィックはCSAポータルに正しいIPを登録した後、PACファイルの導入に向けて動作を開始しました。

ステップ4：許可リストの設定の更新

新しいNAT IPアドレス21.x.x.xからのトラフィックを許可するようにallow-list/firewallルールを更新。

ステップ5：検証

新しいNAT IPアドレスでallow-listを更新した後、通常のセキュアアクセストラフィックフローが復元され、SWGプロキシ経由でWeb要求が正常に機能し始めました。

原因

根本的な原因は、ユーザのNATパブリックIPアドレスが20.x.x.xから21.x.x.xに変更されたことです。セキュアアクセスSWGプロキシは、元のIPアドレスからのトラフィックのみを許可するように設定されているため、新しいIPアドレスからトラフィックが着信すると接続がリセットされます。これに加えて、主なヒントとしてhttps://policy.test.sse.cisco.comで「401 unauthorized」エラーが表示されていましたが、これはhttp接続要求がプロキシにヒットしていることを示しています。これはPCAPでも確認されていますが、プロキシはポリシーを適用し、トラフィックを許可するためにOrgIDやその他のメタデータの詳細に基づいてユーザトラフィックを認証できません。この結果、プロキシはTCP RSTパケットで接続を終了し、正常なWeb要求の処理を妨げました。

SWG PACファイルのWebトラフィックフローの問題を解決するために、ユーザCSA UIの登録済みネットワークに新しいNAT適用済みIPを追加。

関連コンテンツ

- 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。