

SSE NATaaS出力IP使用時にWebアプリケーションファイアウォールでブロックされる地理的制限のあるWebサイトにアクセスする

内容

お問い合わせ内容

Cisco Secure Access(SSE)を使用して特定のWebサイトにアクセスしようとする時、「sorry you have been blocked」というブロックメッセージが表示されます。

通常の家庭用Wi-Fi接続を使用すると、サイトにアクセスできます。リモートWebサイトでは特定のIPアドレス範囲からのアクセスのみが許可され、SSEの出力IPアドレスが許可された範囲から外れている可能性があります。

技術調査の結果、国に関係なく、WebサイトのWebアプリケーションファイアウォール(Cloudflare)がセキュアアクセスNATaaS出力IPの全範囲をブロックしていることが判明しました。この問題は再現可能であり、SSEの出力IPを使用している場合は常に発生します。

環境

- テクノロジー：Cisco Secure Access(SSE)とユニファイドポリシー（インターネットポリシー、プライベートポリシー、DLPポリシー、RBI、セキュリティプロファイル）
- アクセスパス：SSEの任意のデータセンター
- 地域限定Webサイト
- セキュリティ制御：宛先WebサイトのWebアプリケーションファイアウォール(Cloudflare)
- リモートネットワーク（SSE出力IP）とローカルネットワーク（ホームWi-Fi）からのインターネットアクセス
- 問題発生時にセキュアアクセスの導入に変更なし
- 確認されたエラーメッセージ：「sorry you have been blocked」

解決策

Cisco Secure Access NATaaSの出力IPをブロックしているリモートサイトが原因で生じるアクセスの問題に対処するには、次のワークフローを使用することをお勧めします。これらの手順により、ブロックの性質を特定し、潜在的な回避策や解決策を検討するための体系的なアプローチが保証されます。

ステップ1：エラーメッセージを確認し、動作をブロックする

SSE経由でサイトにアクセスする際は、次のメッセージに注意してください。

sorry you have been blocked

ステップ2：異なるネットワークからのWebサイトのアクセシビリティを検証する

Webサイトへのアクセス：

- すべてのSSEデータセンター（ブロック）
- 通常のホームWi-Fi接続（アクセス可能）

ステップ3：ブロッキングの原因となっているセキュリティコントロールを特定する

技術的検証：Cloudflare Web Application Firewall(WAF)は、セキュアアクセスNATaaS出力IPの全範囲をブロックしています。

ステップ4：エンドユーザが使用するアクセスパスの確認

セキュアアクセスにトラフィックを送信するために使用する方法を決定します。

- ローミングセキュリティモジュール
- RAVPNトンネル
- サイト間VPNトンネル
- PACの導入

ステップ5：バイパスまたは許可リストのオプションを確認する

次のオプションのいずれかが可能かどうかを確認します。

- SSE出力IPの許可リストを要求するビジネス関係または宛先Webサイトの管理者との連絡。
- SSEの出力IPは、次のドキュメントに記載されています。
- WAFによってブロックされない異なる出力IPを使用できる代替アクセスパス。
- SSEプロキシから問題のあるWebサイトをバイパス（正確な手順は、セキュアアクセスへのトラフィックの送信方法によって異なります）

ステップ6：確認事項と次のステップを文書化する

次の確認事項を文書化します。

エラーメッセージ

アクセスパスと対応する結果

許可されている場合は、リモートサイトの管理者と通信します。

原因

この問題の根本原因は、宛先WebサイトのWebアプリケーションファイアウォール(Cloudflare)がCisco Secure Access(SSE)のNATaaS出力IP範囲をアクティブにブロックしていることです。このブロックは、非イスラエルIPまたは位置情報フィルタリングに限定されません。むしろ、Cisco Secure Accessに関連する既知の出力IP範囲全体（おそらくリモートWebサイトのポリシーまたはセキュリティ設定の問題）を対象としています。その結果、実際の発信元の国やエンドユーザーの場所に関係なく、これらのIPから発信されるすべてのトラフィックが拒否されます。

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。