Cisco Secure Accessの輸出規制および地理的制限

内容

はじめに

このドキュメントでは、Cisco Secure Accessのコンプライアンスおよび地理的制限をエクスポートする方法について説明します。

背景説明

シスコは、シスコの一般的な輸出法令遵守ポリシーに準拠し、ウクライナとの戦争に対応して、ロシア、ベラルーシ、クリミア、ルハンスク、ドネツク、シリア、キューバ、イラン、北朝鮮など、いくつかの国や地域からのセキュアなアクセスの購入、導入、およびアクセスを制限しています。

ドメイン ネーム サーバ (DNS)

- ロシア、ベラルーシ、クリミア、ルハンスク、ドネツク、シリア、キューバ、イラン、北朝鮮など、ジオブロッキングを行っている認定地域からのIPアドレスを発信元とするクエリのDNSサービスには、セキュリティポリシーまたはコンテンツフィルタリングポリシーは適用されません。レポート作成も無効になります。DNSクエリーは有効な応答を受信し、他の地域からのトラフィックと同じサービスレベルで処理されます。
- DNSに使用する場合、Secure Client口ーミングセキュリティモジュールは引き続きDNSトラフィックを解決します。

Webセキュリティ

- Webセキュリティサーバは、ブロックされた国または地域のいずれかから発信IPが到達するトラフィックを受け入れません。
- 既定のセキュアクライアントローミングセキュリティモジュール構成では、セキュアアクセスが利用できないときにインターネットに直接接続します。一部のお客様の設定は「fail

closed」モードで動作するため、ユーザがインターネットにアクセスできなくなる可能性があります。
- デフォルトのSecure Access Protected Access Credential(PAC)ファイルでは、セキュアアクセスが使用できないときにインターネットに直接接続されます。一部の特定のお客様の設定（デフォルトルートのない設定など）は「フェールクローズ」され、ユーザがインターネットアクセスを失う原因となる可能性があります。
- IPsecトンネルは、IPブロッキングまたはインターネットキーエクスチェンジ(IKE)クレデンシャルの失効によって切断されます。動作とユーザエクスペリエンスは、お客様の設定によって異なります。設定によっては、インターネットへの直接接続に戻るものもあれば、マルチプロトコルラベルスイッチング(MPLS)に戻るものもあり、ユーザがインターネットアクセスを失う原因となるものもあります。

ダッシュボードおよび管理アクセス

Secure Accessダッシュボードと APIは、リストされているリージョンのいずれかから接続しているユーザに対してブロックされます。

FAQ

1. ユーザがブロックされているのに、影響を受けるリージョンに含まれていない場合はどうすればいいですか。
   サポートに問い合わせて、喜んで調査してもらいます。

2. ジオブロッキングデータの精度はどの程度ですか。
   業界をリードする位置情報サービスは、特定のIPアドレスの国を特定するために使用されます。

3. IPアドレスに関連付けられた場所が間違っている場合は、何をする必要がありますか。
   修正要求を次のサービスに送信することを推奨します。

- https://www.maxmind.com/en/geoip-location-correction
- https://support.google.com/websearch/contact/ip/
- https://ipinfo.io/corrections
- https://www.ip2location.com/
- http://www.ipligence.com/

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。