セキュアアクセストラフィックのステアリング動作と例外リストの設定

内容

お問い合わせ内容

デフォルトの例外設定でUse ZTA to secure all internet destinations設定を使用する場合、Cisco Secure Access Traffic Steeringの動作について詳しく説明する必要があります。次の点に関して具体的な質問が発生します。

- トラフィック操作の決定がDNS解決後の宛先IPアドレスに基づいているかどうか。
- ステアリングプロセスでのDNSトラフィック自体の処理方法。
- 例外リストのデフォルトの.localドメインエントリ以外に、追加のローカルドメインエントリを設定する必要があるかどうか。

この設定は、Connect > End User Connectivity > Zero Trust Access > (Zero Trust Access Profiles) > Secure Internet Access > Traffic Steering > Use ZTA to secure all internet destinationsにあります。

デフォルトの例外リストには、プライベートIPアドレス範囲（クラスA、B、およびC）と.localドメインが含まれており、ユーザはこれらの設定の動作動作を理解する必要があります。

環境

- シスコセキュアアクセス
- ゼロトラストアクセス(ZTA)の設定
- トラフィックステアリング機能の有効化
- プライベートIP範囲および.localドメインを含むデフォルト例外リスト

解決策

Cisco Secure Access Traffic Steeringの動作は、次のように動作します。

トラフィック操作の決定プロセス

トラフィック操作の決定は、DNS解決後の宛先IPアドレスに基づいて行われます。システムは、DNS名前解決の結果である実際の宛先IPを評価して、トラフィックをゼロトラストアクセスセキュリティスタック経由で転送する必要があるかどうかを判断します。

DNSトラフィック処理

DNSクエリ自体は、トラフィックステアリングの対象にはなりません。エンドポイントが内部DNSサーバをポイントするDHCP経由でDNSサーバ割り当てを受信すると（通常はプライベートIPアドレスを使用）、これらのDNS通信はトラフィック誘導メカニズムをバイパスし、ローカルで処理されます。

例外リストの設定

デフォルトの例外リストには次のものが含まれます。

- プライベートIPアドレス範囲(クラスA:10.0.0.0/8、クラスB:172.16.0.0/12、クラスC:192.168.0.0/16)
- ローカルドメイン

カスタムのローカルドメイン（内部ドメイン名）を使用している組織では、内部トラフィックがセキュリティスタックを不必要に通過しないようにするため、例外リストに追加のドメインエントリを追加する必要があります。デフォルトの.localエントリは、標準のローカルネットワーク検出プロトコルを対象としますが、組織のすべての内部ドメインを含まない場合もあります。

設定の確認

設定が正しいことを確認するには、次の手順を実行します。

Connect > End User Connectivity > Zero Trust Access > Secure Internet Access > Traffic Steeringの順に選択します。

例外リストを確認して、組織の内部インフラストラクチャに固有の、必要なすべてのプライベートIP範囲とローカルドメイン名が例外リストに含まれていることを確認します。

原因

これは、Cisco Secure Access Traffic Steering機能の動作に関する情報を要求するものです。明確にする必要があるのは、トラフィック操作ロジックの複雑さ、およびDNS解決、IPベースのルーティング決定、例外処理メカニズムの相互作用によるものです。

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。