

スプリットルーティング設定のためのセキュアアクセス宛先アドレス

内容

お問い合わせ内容

ハブスポークネットワークアーキテクチャのWindowsエンドポイントでCisco Secure Client(CSC)を使用してCisco Secure Access(CSA)を導入する場合、多くの組織では、スプリットルーティングを設定して、ハブ経由のヘアピニングではなくローカルスポークインターネット回線を介してスポークサイトのトラフィックがCSAに直接接続できるようにする必要があります。この設定では、CSAトンネルを確立する際に使用するすべてのシスコ宛先アドレスの知識が必要です。その結果、Fortigateファイアウォールなどのネットワークデバイスにルーティング例外（ブレイクアウト/スプリットルーティング）を定義できます。

具体的な要件は、CSCがTLS/DTLSトンネルを確立するときに使用するCSAエンドポイントのすべての宛先情報（IPアドレスまたはURL）を特定し、CSAトラフィックのハブスポークVPNトンネルをバイパスするルーティングポリシーを適切に設定できるようにすることです。

環境

- Cisco Secure Access(CSA)の導入
- WindowsエンドポイントでのCisco Secure Client(CSC)
- Fortigateファイアウォールを使用したハブスポーク型ネットワークトポロジ
- CSAへのTLS/DTLSトンネル接続

解決策

Cisco Secure Access接続のスプリットルーティングを設定するには、次のセクションで説明する

宛先情報をFortigateデバイスで設定し、CSAエンドポイントへの直接接続を可能にする必要があります。

CSA宛先ドメインおよびポート

プライマリドメイン

`*.vpn.sse.cisco.com`

必要なポートとプロトコル

- TCP/UDP 443:TLS/DTLSトンネルの確立に使用
- UDP 500/4500:IPSecトンネルの確立に使用
- TCP 80:VPN証明書失効チェックに使用

Fortigateの設定方法

CSAドメイン(`*.vpn.sse.cisco.com`)および指定されたポートを宛先とするトラフィックが、ハブスポークVPNトンネルではなく、ローカルスポークインターネット回線を通じて転送されるように、Fortigateデバイスのルーティングポリシーを設定します。これにより、次のコードスニペットで説明するトラフィックフローが有効になります。

望ましいトラフィックフロー

Spoke Site → CSA Tunnel Connection → CSA-mediated Internet Communication

ハブサイトを通過するトラフィックフローの代わりに

Spoke Site → Hub Site → CSA Tunnel Connection → CSA-mediated Internet Communication

重要な考慮事項

CSAの接続先は実行時に動的に決定されます。つまり、スタティックルーティングの設定では、特定のIPアドレスを事前に決定することはできません。`*.vpn.sse.cisco.com`を使用するドメインベースのアプローチは、スプリットルーティングポリシーを設定する最も信頼性の高い方法です。

最新の宛先とポートの要件については、新しいソフトウェアリリースで更新される可能性が高いため、Cisco Secure Accessの公式のドキュメントを参照してください。

原因

ハブスポークネットワークトポロジでは、スポークサイトからのインターネットに向かうトラフィックはすべて、通常、デフォルトでハブサイト経由でルーティングされます。CSCを使用してCSAを実装する場合、このデフォルトのルーティング動作では、CSAトンネルのトラフィックがCSAエンドポイントに到達する前にハブサイトをヘアピニングするため、遅延や帯域幅の非効率性が生じる可能性があります。CSAエンドポイント選択の動的な性質により、スプリットルーティング機能を適切に実行するには、静的なIPベースのルールではなく、ドメインベースのルーティングポリシーが必要です。

関連コンテンツ

- [Cisco Secure Accessに関するドキュメント – 接続要件](#)
- [Cisco Secure Accessに関するドキュメント：ネットワーク設定](#)
- [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。