Cisco Secure Accessでの重複サブネットを使用したサイト間接続

内容

はじめに

このドキュメントでは、Cisco Secure Accessオーバーラップサブネットソリューションについて説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Cisco Secure Access管理
- ファイアウォール/ルータ管理

Cisco では次の前提を満たす推奨しています。

- Cisco Secure Accessへの管理アクセス
- IPSecヘッドエンドデバイス（ファイアウォールまたはルータ）への管理アクセス

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

はじめる前に

この例では、同じIPサブネット192.168.200.0/24を持つ2つの異なるブランチサイトがあり、これらのブランチサイトは2つの異なるIPSecトンネル経由でCisco Secure Accessに接続されています。

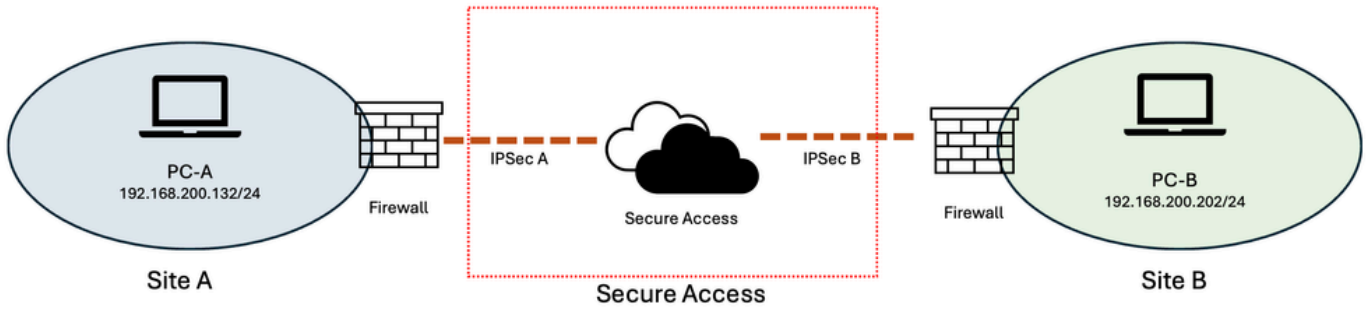

図 – ネットワーク図

目標は、「サイトA」のユーザが「サイトB」のリソースにアクセスできるようにすることです。その逆も同様です。

準備と計画

両方のサイトが同じIPサブネット(192.168.200.0/24)を使用しているため、重複アドレス空間によって2つのサイト間の直接通信が阻止されます。この重複を解決するために、各サイトのリソースを表す重複しない2つの仮想サブネットが割り当てられます。

この例では、次のとおりです。

- サイトA:10.30.30.0/24
- サイトB:10.40.40.0/24
- 両方のサイトの実際のサブネット：192.168.200.0/24

仮想サブネットはサイトごとに一意のアドレス空間を提供しますが、実際のリソースは引き続き既存の192.168.200.0/24アドレスを使用します。

サイトAのユーザがサイトBにあるリソースにアクセスする場合、ユーザは重複する192.40.40.0/24アドレス空間を直接使用するのではなく、サイトBの仮想サブネット(**10.168.200.0/24**)を介してリソースにアクセスします。

Cisco Secure Accessには、仮想アドレスを対応する実際のアドレスに変換できる1対1の宛先NAT(D-NAT)機能があります。D-NATアドレス範囲は、元のサブネットと同じサイズです。この例では、仮想ネットワークと実際のネットワークの両方が/24サブネットであり、仮想IPアドレスと実際のIPアドレスの間で1対1のマッピングを提供します。

例：

10.40.40.202 → 192.168.200.202

したがって、サイトAからの10.40.40.202宛ての要求はD-NATによって192.168.200.202に変換され、両方のサイトが同じ基盤IPサブネットを使用しているにもかかわらず、要求がサイトBの対応するリソースに到達できるようになります。

このアプローチでは、リソースの既存のIPアドレッシングを維持しながら、各サイトに対して重複しない仮想アドレス空間を効果的に作成します。また、仮想アドレスと実アドレスの間に一貫した1対1の関係が提供されるので、設定の理解、管理、およびトラブルシューティングが容易になります。

設定手順

Cisco Secure Accessの現在の設計と制限により、このシナリオを実現するには、IPSecトンネルの背後にあるヘッドエンドデバイスとCisco Secure Accessの両方で設定を行う必要があります。

ヘッドエンドデバイスは、Cisco Secure AccessへのIPSecトンネルを確立するファイアウォールまたはルータです。Cisco Secure AccessでD-NATを設定することに加えて、ヘッドエンドファイアウォールは、リターントラフィックに対して送信元NAT(S-NAT)も実行する必要があります。

したがって、この設定は次の2つのセクションで構成されます。

1. Cisco Secure Accessにおける宛先NAT(D-NAT)の設定」を参照してください。
2. ファイアウォールで送信元NAT(S-NAT)を設定し、リターントラフィックが仮想アドレス空間に確実に逆変換されるようにします。

Cisco Secure Accessの設定

ステップ1:Cisco Secure Access管理ポータルで、Connect > Network Connectionsの順に移動し、Network Tunnel Groupsタブを選択します。

ステップ2:重複するサブネットを使用するサイトのIPsecトンネルに関連付けられたネットワークトンネルグループを編集します。

この例では、

- IPSec-A =サイトAのネットワークトンネルグループ
- IPSec-B =サイトBのネットワークトンネルグループ

ステップ3:必要なNetwork Tunnel Groupの横にある3ドットメニューをクリックして、Editを選択します。

ステップ4:左側のメニューからRoutingタブを選択し、Network Address Translation（NAT；ネットワークアドレス変換）（まだイネーブルになっていない場合）をイネーブルにします。

ステップ5:Destination NAT Mappingsの下で、Add Mappingsをクリックします。

手順6:この表を使用して、各ネットワークトンネルグループのD-NATマッピングを設定します。

	サイトA - IPSecトンネル	サイトB - IPSecトンネル
宛先NAT-1	Site → セキュアアクセス 元のCIDR:10.40.40.0/24 変換後のCIDR:192.168.200.0/24	Site → セキュアアクセス 元のCIDR:10.30.30.0/24 変換後のCIDR:192.168.200.0/24
宛先NAT-2	セキュアなアクセス→サイト	セキュアなアクセス→サイト

	元のCIDR:192.168.200.0/24 変換後のCIDR:10.30.30.0/24	元のCIDR:192.168.200.0/24 変換後のCIDR:10.40.40.0/24
	 IPSecトンネルサイトA - D-NAT設定	 IPsecトンネルサイトB - D-NAT設定

注：各Network Tunnel Groupの設定を行った後、Saveをクリックします。確認ウィンドウが表示されたら、UPDATEと入力して変更を確認します。他のネットワークトンネルグループについても同じ手順を繰り返します

ファイアウォールの設定

ネットワークトンネルグループの背後にあるオーバーラップしたIPサブネットの処理に関する現在の制限のために、ファイアウォールの設定が必要です。

Cisco Secure Accessが着信パケットに対してD-NATを実行する場合、変換された宛先アドレスを使用して、パケットが宛先リソースに配信されます。ただし、このサブネットが重複するシナリオでは、リターントラフィックに対応する逆変換は自動的には実行されません。

その結果、リターントラフィックはファイアウォールで手動でソースNAT処理する必要があります。

主な要件は、宛先サーバで、サーバの実際のIPアドレスではなく、クライアントが最初にアクセスした仮想IPアドレスを使用してリターントラフィックが認識されることです。

例

次のように仮定します。

- サイトAクライアント：192.168.200.132
- サイトBのWebサーバ：192.168.200.202
- サイトBの仮想サブネット：10.40.40.0/24
- Webサーバの仮想アドレス：10.40.40.202

サイトAのクライアントが、https://10.40.40.202を使用してサイトBのWebサーバにアクセスしま

す。

Cisco Secure AccessがD-NAT 10.40.40.202 → 192.168.200.202を実行

パケットは192.168.200.202のWebサーバに到達します。

この問題はリターントラフィックで発生します。ファイアウォールに追加のNATがないと、WebサーバはSource: 192.168.200.202を使用して応答を生成します。

ただし、クライアントが宛先10.40.40.202への接続を開始しました。

したがって、クライアントに提示される送信元アドレスが仮想アドレス192.168.200.202 → 10.40.40.202に対応するように、リターントラフィックを変換する必要があります

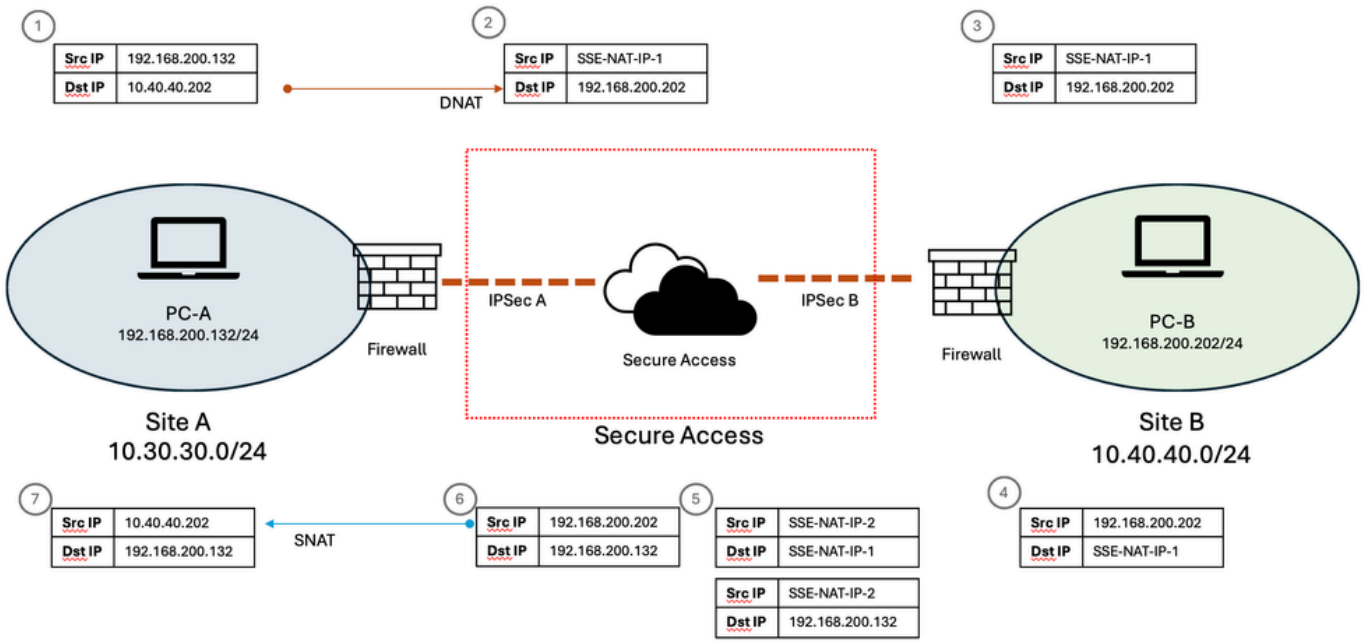

図 – ネットワークフロー

これを実現するために、ファイアウォールは、ネットワークトンネルグループに向けて送信されるトラフィックに対して送信元NATを実行します。

この例では、必要なマッピングは192.168.200.0/24 → 10.40.40.0/24です。

これにより、実アドレスとそれに対応する仮想アドレスの間に逆の1対1の関係が作成されます。

1対1 SNAT

ファイアウォールがサブネット全体で1対1の送信元NATをサポートしている場合、単一のNATルールで完全な/24アドレス範囲を表すことができます。

例：

実際のソース	翻訳済みソース
192.168.200.0/24	10.40.40.0/24

この結果、192.168.200.202 → 10.40.40.202 および192.168.200.203 → 10.40.40.203などのマッピングが生成されます

同じ1対1の関係がサブネット全体に適用されます。

1対1のSNATを使用しないファイアウォール

ファイアウォールがサブネット全体で1対1の送信元NATをサポートしていない場合は、必要なマッピングをそれぞれ個別に設定する必要があります。

たとえば、Webサーバの場合は次のようになります。

- 送信元IP:192.168.200.202
- 送信元インターフェイス：Network Tunnel Group
- トラフィックの方向：着信
- 変換された送信元IP:10.40.40.202

変換後の変換は、192.168.200.202 → 10.40.40.202となります。

仮想サブネット経由でのアクセスを必要とする各リソースに対して、同じアプローチを適用できます。

これにより、通信の両方向が仮想アドレッシング方式を維持し、クライアントが接続の確立時に使用したのと同じ仮想IPアドレスから応答を受信することが保証されます。

関連情報

Cisco Secure Access NATマッピング/ネットワークトンネルグループの設定
：https://securitydocs.cisco.com/docs/csa/olh/168842.dita

Cisco Secure Access Networkトンネルグループの設定とルーティングのリファレンス
：https://securitydocs.cisco.com/docs/csa/olh/118900.dita

Cisco Secure Accessトラブルシューティングおよび基本データ収集ガイド
：https://www.cisco.com/c/en/us/support/docs/security/secure-access/221240-troubleshoot-and-collect-basic-informati.html

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。