2つのサイト間トンネル間のトラフィックのヘアピニングの設定

内容

はじめに

このドキュメントでは、1つのインターフェイスで2つのVPNトンネル間のVPNトラフィックを転送する方法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。
- ポリシーベースのサイト間VPNの基本的な知識
- ASAコマンドラインの経験

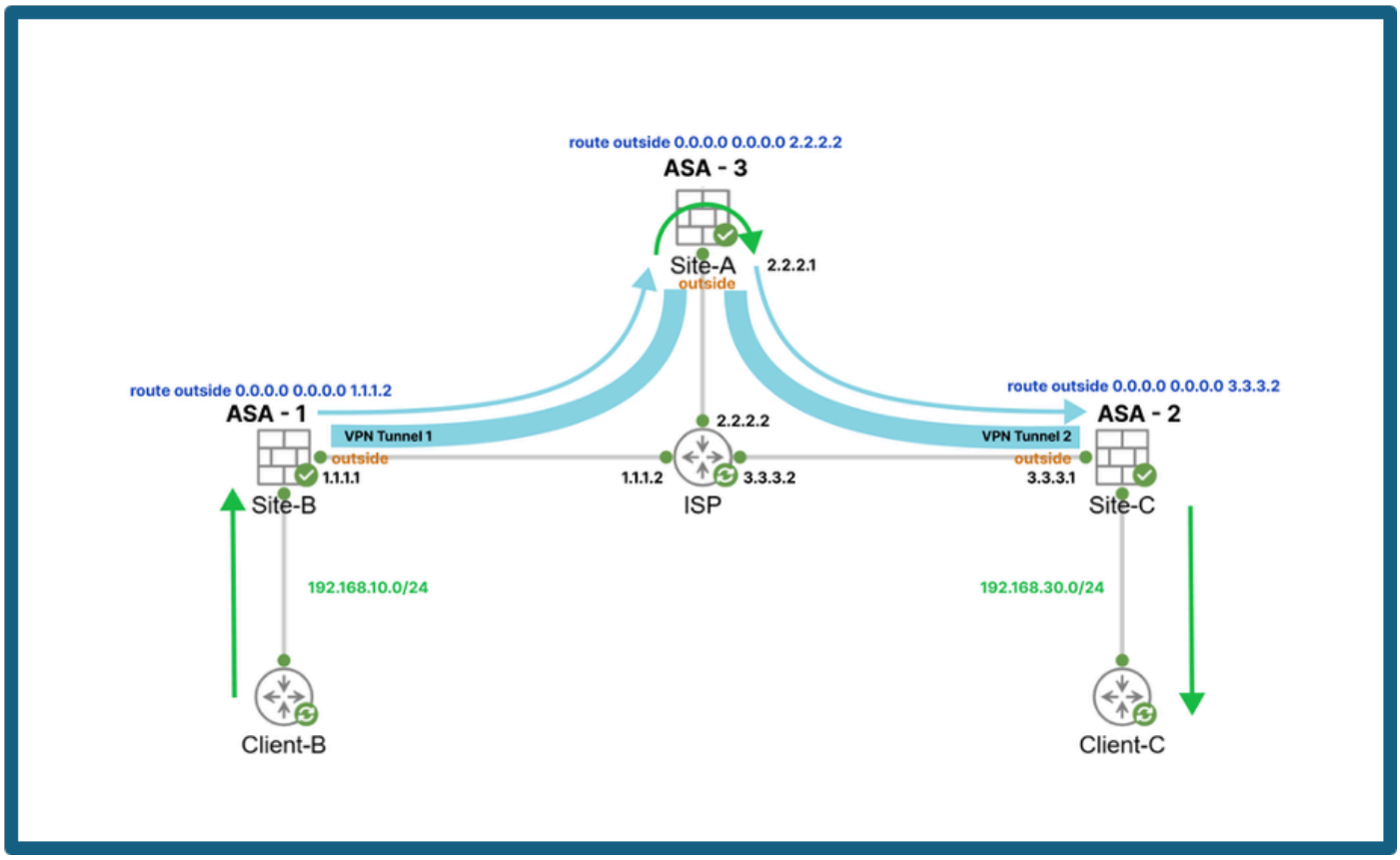
使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。
- 適応型セキュリティアプライアンス(ASA)バージョン9.20
- IKEv1

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ました。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。

トポロジ



トポロジ

背景説明

この設定は、1つのサイト間トンネルから同じデバイス上の別のサイト間トンネルにトラフィックをリダイレクトする方法を示しています。この設定を説明するために、サイトA、サイトB、およびサイトCを表す3つのASAを使用しました。

コンフィギュレーション

このセクションでは、ASA-1（サイトB）からASA-2（サイトC）へのトラフィックでASA-3（サイトA）を通過できるようにするために必要な設定の概要を説明します。

次の2つのVPNトンネルが設定されています。

- VPNトンネル1:Site-BとSite-A間のVPNトンネル
- VPNトンネル2:Site-CとSite-A間のVPNトンネル

ASAでポリシーベースのVPNトンネルを作成する方法の詳細については、『ASAとCisco IOS XEルータ間のサイト間IPSec IKEv1トンネルの設定』の「ASAの設定」を参照してください。

ASA（サイトB）の構成

ASA 1の外部インターフェイス上のVPNトンネル1の暗号アクセスリストで、Site-BネットワークからSite-Cネットワークへのトラフィックを許可する必要があります。
このシナリオでは、192.168.10.0/24 ~ 192.168.30.0/24です

暗号アクセスリスト：

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

Nat例外：

```
nat (inside,outside) source static192.168.10.0_24192.168.10.0_24 destination static192.168.30.0_24192.1
```

VPNトンネル1のクリプトマップ：

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 2.2.2.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map interface outside
```

ASA（サイトC）暗号設定

ASA 2の外部インターフェイスで、VPNトンネル2のcrypto access-list内のSite-Cネットワークか

らSite-Bネットワークへのトラフィックを許可します。
このシナリオでは、192.168.30.0/24 ~ 192.168.10.0/24です

暗号アクセスリスト：

```
object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
```

Nat例外：

```
nat (inside,outside) source static 192.168.30.0_24 192.168.30.0_24 destination static 192.168.10.0_24 1
```

VPNトンネル2のクリプトマップ：

```
crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 2.2.2.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

ASA（サイトA）暗号設定

VPN Tunnel 1のcrypto access-listでSite-Cネットワークから Site-Bネットワークへのトラフィックを許可し、Site-AのASAの外部インターフェイスでVPN Tunnel 2のcrypto access-listでSite-Bネットワークから Site-Cネットワークへのトラフィックを許可します。これは、_つのASAで設定した方向とは逆方向です。

このシナリオでは、VPNトンネル1では192.168.30.0/24 ~ 192.168.10.0/24、VPNトンネル2では192.168.10.0/24 ~ 192.168.30.0/24です

暗号アクセスリスト：

```
object network 192.168.30.0_24
subnet 192.168.30.0 255.255.255.0

object network 192.168.10.0_24
subnet 192.168.10.0 255.255.255.0

access-list 110 extended permit ip object 192.168.30.0_24 object 192.168.10.0_24
access-list 120 extended permit ip object 192.168.10.0_24 object 192.168.30.0_24
```

VPNトンネル1および2のクリプトマップ設定：

```
crypto map outside_map 10 match address 110
crypto map outside_map 10 set pfs
crypto map outside_map 10 set peer 1.1.1.1
crypto map outside_map 10 set ikev1 transform-set myset

crypto map outside_map 20 match address 120
crypto map outside_map 20 set pfs
crypto map outside_map 20 set peer 3.3.3.1
crypto map outside_map 20 set ikev1 transform-set myset

crypto map outside_map interface outside
```

これに加えて、セキュリティレベルが同じインターフェイスである外部から外部へのトラフィックをルーティングする必要があるため、次のようにコマンドを設定する必要があります。

```
same-security-traffic permit intra-interface
```

Site-BからSite-Cへのトラフィックフロー

トラフィックがSite-BからSite-c(192.168.10.0/24から192.168.30.0/24)に開始されると仮定します。

Site-B（送信元）

1. 192.168.10.0/24 network(Site-B)から開始され、192.168.30.0/24 network(Site-C)を宛先とするトラフィックは、設定されたルーティングテーブルに基づいて、ASA-1の外部インターフェイスにルーティングされます。

2. トラフィックがASA-1に到達すると、ASA-1で設定されているcrypto access-list 110に一致します。これにより、VPN Tunnel 1を使用したトラフィックの暗号化がトリガーされ、Site-Aに向け

てデータが安全に送信されます。

Site-A（中間）

1. Site-AのASAの外部インターフェイスにある192.168.10.0/24 to 192.168.30.0/24 arrivesからの暗号化トラフィック。
2. サイトAでは、元のペイロードを復元するために、トラフィックがVPNトンネル1によって復号化されます。
3. 復号化されたトラフィックは、Site-AのASAの外部インターフェイスでVPNトンネル2を使用して再暗号化されます。

Site-C（宛先）

1. 192.168.10.0/24 to 192.168.30.0/24 reachesからSite-CのASA-2の外部インターフェイスへの暗号化されたトラフィック。
2. ASA-2は、VPNトンネル2を使用してトラフィックを復号化し、パケットをSite-CのLAN側に転送し、192.168.30.0/24 network内の目的の宛先にパケットを配信します。

Site-CからSite-Bへのリバーストラフィックフロー

Site-C(192.168.30.0/24) and)から発信されSite-B(192.168.10.0/24)を宛先とする逆方向のトラフィックフローは、同じプロセスになりますが、逆方向になります。
1. Site-Cでは、トラフィックはVPNトンネル2によって暗号化されてからSite-Aに送信されます。
2. サイトAで、トラフィックがVPNトンネル2で復号化され、VPNトンネル1を使用して再暗号化されてから、サイトBに転送されます。
3. サイトBで、トラフィックはVPNトンネル1によって復号化され、192.168.10.0/24 networkに配信されます。

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。