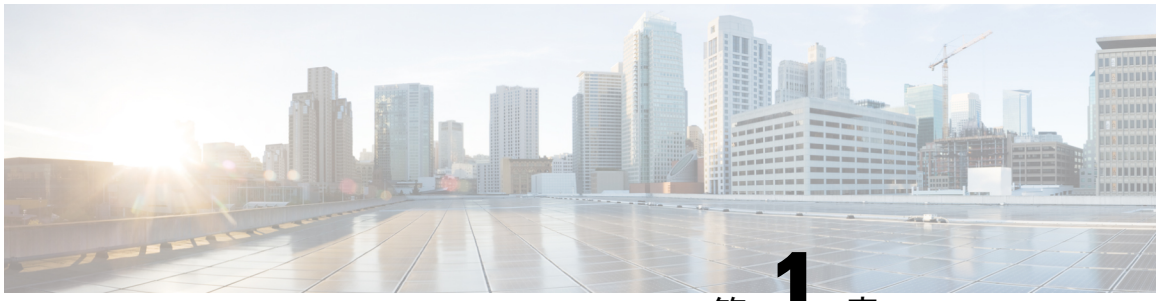
Cisco Catalyst SD-WAN NAT コンフィギュレーション ガイド、Cisco IOS XE Catalyst SD-WAN リリース 17.x

初版：2021 年 10 月 8 日

最終更新：2024 年 4 月 30 日

シスコシステムズ合同会社
〒107-6227 東京都港区赤坂9-7-1 ミッドタウン・タワー
http://www.cisco.com/jp
お問い合わせ先：シスコ コンタクトセンター
0120-092-255 （フリーコール、携帯・PHS含む）
電話受付時間：平日 10:00～12:00、13:00～17:00
http://www.cisco.com/jp/go/contactcenter/

目 次



第 1 章

最初にお読みください

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

参考資料

- Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations [英語]
- Cisco Catalyst SD-WAN Device Compatibility [英語]

ユーザーマニュアル

- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17 [英語]

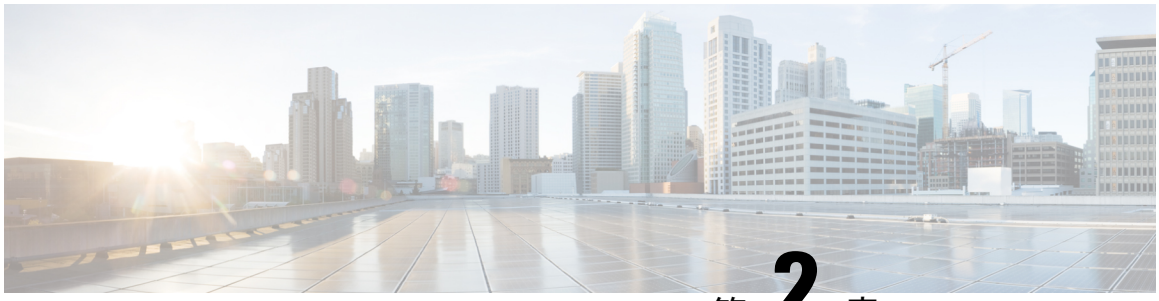
通信、サービス、およびその他の情報

- Cisco Profile Manager で、シスコの E メールニュースレターおよびその他の情報にサインアップしてください。
- ネットワーク運用の信頼性を高めるための最新のテクニカルサービス、アドバンストサービス、リモートサービスについては、シスコサービスにアクセスしてください。
- 安全かつ検証されたエンタープライズクラスのアプリ、製品、ソリューション、サービスをお求めの場合は、CiscoDevnet にアクセスしてください。

- Cisco Press 出版社による一般的なネットワーク、トレーニング、認定関連の出版物を入手するには、Cisco Press にアクセスしてください。
- 特定の製品または製品ファミリの保証情報を探すには、Cisco Warranty Finder にアクセスしてください。
- リリースで未解決および解決済みのバグをご覧になる場合は、Cisco Bug Search Toolにアクセスしてください。
- サービス リクエストを送信するには、シスコ サポートにアクセスしてください。

マニュアルに関するフィードバック

シスコのテクニカルドキュメントに関するフィードバックを提供するには、それぞれのオンラインドキュメントの右側のペインにあるフィードバックフォームを使用してください。



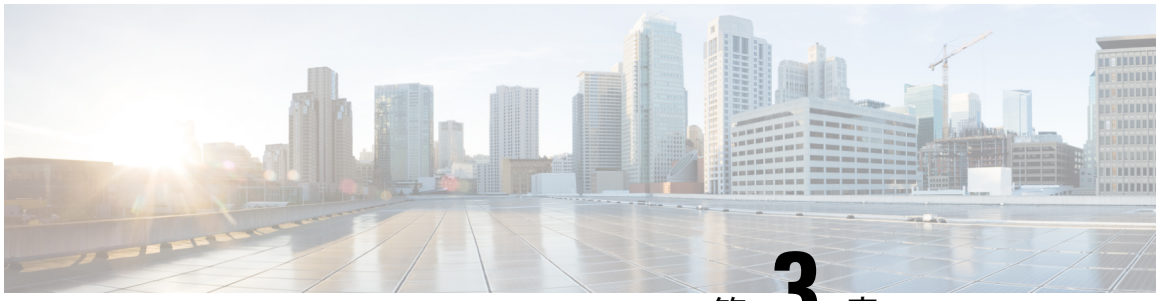
第 2 章

Cisco IOS XE（SD-WAN）の新機能

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

（注） シスコでは、リリースごとに Cisco Catalyst SD-WAN ソリューションを継続的に強化しています。また、コンテンツも最新の強化に合致したものとなるように努めています。次の表に、コンフィギュレーション ガイド、コマンドリファレンスガイド、およびハードウェア設置ガイドに記載されている新機能と変更された機能を示します。Cisco Catalyst SD-WAN ソリューションに関係する追加機能と修正については、リリースノートの「解決されたバグおよび未解決のバグ」セクションを参照してください。

What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x [英語]



第 3 章

NAT の設定

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

NAT の設定

Cisco IOS XE Catalyst SD-WAN には、次のタイプのネットワークアドレス変換（NAT）設定が含まれます。

- NAT ダイレクト インターネット アクセス（DIA）：トラフィックを中央サイトやデータセンターにルーティングするのではなく、リモートサイトがトラフィックをインターネットに直接ルーティングできるようにします。
- NAT サービス側：ネットワークオーバーレイのサービスホストとの間で送受信されるデータトラフィックに、内部および外部 NAT を設定できます。サービス側 NAT は、構成された一元化されたデータポリシーと一致する、内部および外部ホストアドレスのデータトラフィックを変換します。

NAT は、IP アドレスを保護するように設計されています。NAT では、登録されていない IP アドレスを使用するプライベート IP ネットワークがインターネットに接続できるようにします。NAT はデバイス上で動作し、通常は 2 つのネットワークを接続します。パケットが別のネットワークに転送される前に、NAT は内部ネットワークのプライベート（グローバルに一意ではない）アドレスを正当なアドレスに変換します。

NAT は、単一のデバイスがインターネット（またはパブリックネットワーク）とローカルネットワーク（またはプライベートネットワーク）の間のエージェントとして機能することを可能にします。それは、ネットワークの外部に対してコンピュータのグループ全体を表すために必要な一意の IP アドレスは 1 つだけです。

（注） NAT がメンテナンス操作を実行するときは、NAT データベースをロックする必要があります。NAT データベースがロックされている場合、NAT は変換用のパケットを処理しません。通常、NAT メンテナンス操作は 1 秒未満から数秒以内です。通常、未変換パケットを送信する NAT は問題になりません。これらのパケットは ISP によってドロップされるためです。

次のコマンドを設定して、NAT データベースの更新時に NAT がパケットをドロップするようにします。

```
ip nat service modify-in-progress drop
```

NAT ダイレクト インターネット アクセス

表 *1:* 機能の履歴

機能名	リリース情報	説明
ループバック インターフェイスとしての NAT プール、スタティック NAT、および NAT のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.2.1r Cisco vManage 20.1.1	この機能は、ループバック インターフェイス アドレスの NAT 設定、ダイレクト インターネット アクセス（DIA）の NAT プールサポート、およびスタティック NAT をサポートします。
OMP を介した NAT ルートのアドバタイズ	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a	この機能を使用すると、Cisco Catalyst SD-WAN オーバーレイ管理プロトコル（OMP）を介して NAT ルートをブランチ ルータにアドバタイズできます。この機能は、Cisco SD-WAN Manager デバイス CLI テンプレートを介してのみ設定できます。

機能名	リリース情報	説明
IPv6 トンネルを介した NAT DIA IPv4 のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1	この機能は、IPv6 ネットワークの使用時に IPv4 クライアントが IPv4 サーバーにアクセスするためのサポートを提供します。 IPv4 トラフィックは、IPv6 トンネルを介してインターネットにルーティングされます。 CLI または CLI アドオンテンプレートを使用して、IPv6 トンネルを介して NAT DIA IPv4 を設定できます。
NAT DIA を使用した PPP ダイヤラインターフェイスのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能により、次の Point-to-Point Protocol（PPP）ダイヤラインターフェイスのサポートが追加されます。PPP over Ethernet（PPPoE）、PPP over Asynchronous Transfer Mode（PPPoA）、および PPP over Ethernet Asynchronous Transfer Mode（PPPoEoA）。 PPP ダイヤラインターフェイスを使用して、IPv4 サービスおよびサイトにアクセスできます。
HSRP によるスタティック NAT マッピングのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能を使用すると、両方のホットスタンバイルータプロトコル（HSRP）ルータが同じスタティック NAT マッピングで構成されている場合、アクティブデバイスのみがスタティック NAT マッピングエントリのアドレス解決プロトコル（ARP）要求に応答します。HSRP アクティブデバイスからスタンバイデバイスにフェールオーバーするトラフィックは、フェールオーバーする前に ARP 要求がタイムアウトするのを待つ必要はありません。

機能名	リリース情報	説明
NAT DIA およびゾーンベースのファイアウォールの ALG サポート	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能は、アプリケーションパケットのペイロード内の IP アドレスを変換するアプリケーション レベル ゲートウェイ（ALG）のサポートを提供します。ドメインネームシステム（DNS）、FTP、Session Initiation Protocol（SIP）などの特定のプロトコルでは、パケットペイロード内の IP アドレスとポート番号の変換に NAT ALG が必要です。
NAT DIA によるポートフォワーディングのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1	この機能を使用すると、1つ以上のポート転送ルールを定義して、外部ネットワークから特定のポートで受信したパケットを送信し、内部ネットワーク上のデバイスに到達させることができます。 Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 より前は、ポートフォワーディングはサービス側の NAT でのみ利用可能でした。
NAT 高速ロギングのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco vManage リリース 20.9.1 — Also Cisco IOS XE リリース 17.6.4 以降の 17.6.x リリース Cisco vManage リリース 20.6.4 以降の 20.6.x リリース	この機能は、NAT によるすべての変換の高速ロギング（HSL）を有効または無効にする機能を提供します。 デバイス CLI テンプレートまたは CLI アドオン機能テンプレートを使用して、NAT HSL を設定できます。
既知の Cisco Catalyst SD-WAN ポートの送信元ポート保持に対するサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a Cisco vManage リリース 20.10.1	この機能により、NAT 時に既知の Cisco Catalyst SD-WAN ポートを保持できます。

機能名	リリース情報	説明
宛先 NAT のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a Cisco vManage リリース 20.11.1	この機能は、WAN エッジデバイスを通過するパケットの宛先アドレスを変更します。宛先 NAT はプライベートアドレス宛てのトラフィックを、変換された宛先パブリック IP アドレスにリダイレクトするために使用されます。
ループバック インターフェイスを使用した NAT DIA によるポートフォワーディング	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a Cisco vManage リリース 20.11.1	この機能は、ループバック インターフェイスを使用した NAT DIA によるポートフォワーディングをサポートします。 デバイス CLI テンプレートまたは CLI アドオン機能テンプレートを使用して、ループバック インターフェイスを設定できます。
NAT DIA およびゾーンベースのファイアウォールの ALG サポート拡張	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a Cisco vManage リリース 20.11.1	NAT DIA の ALG サポートは、次のプロトコルに対応するように拡張されています。 • 簡易ファイル転送プロトコル（TFTP） • ポイントツーポイント トンネリング プロトコル（PPTP） • Sun リモートプロシージャ コール（SUNRPC） • Skinny Client Control Protocol（SCCP） • H.323

機能名	リリース情報	説明
複数の NAT タイプの設定のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a Cisco Catalyst SD-WAN Manager リリース 20.14.1	この機能は、複数の NAT タイプ（インターフェイス、ループバック インターフェイス、またはダイレクト インターネット アクセス（DIA）の NAT プール）の設定をサポートします。 一元管理型データポリシーを使用して、エッジルータから出る DIA トラフィックのさまざまな NAT タイプを組み合わせるためのルールを割り当てます。NAT を完全にバイパスすることもできます。

NAT DIA に関する情報

NAT DIA を使用すると、ブランチサイトは、検査のために中央サイトを経由するのではなく、トラフィックをインターネットに直接ルーティングできます。これにより、クラウドベースのアプリケーションは、不要な帯域幅を使用することなく、インターネットやクラウドサービスプロバイダーに直接アクセスできます。

NAT DIA フロースティッキネス

サポートされる最小リリース：Cisco IOS XE リリース 17.6.1a、Cisco vManage リリース 20.6.1

NAT DIA がアプリケーション一致の集中型データポリシーで設定されている場合、パスの変更により、NAT DIA ポリシーの対象となるアプリケーションフローがリセットされる可能性があります。たとえば、アプリケーションリストに一致するデータポリシーがあり、アクションが NAT DIA である場合、最初のいくつかのパケットはディープ パケット インスペクション（DPI）によって識別されない可能性があります。したがって、NAT DIA アプリケーションポリシーに一致しないパケットは、Cisco Catalyst SD-WAN オーバーレイパスへのルーティングに従います。フローが識別されると、フローの後のパケットは、データポリシーで定義されている NAT DIA パスを使用します。このパス変更により、フローがリセットされます。これは、パスが異なると、サーバーへのクライアント送信元またはポートの組み合わせが異なることを意味し、サーバーは不明な TCP フローをリセットします。

NAT パスのフローレベル状態を記録するために、フロースティッキネス機能が有効になっています。フローの最初のパケットが非 NAT の場合、このフローの残りのパケットは非 NAT パスを使用します。最初のパケットフローが NAT DIA パスを経由する場合、このフローの残りのパケットは NAT DIA パスを使用します。これは、NAT DIA データポリシーではデフォルトで有効になっています。

フロースティッキネスを無効にするには、CLI アドオンテンプレートを使用してローカライズされたポリシーで **flow-stickiness-disable** コマンドを使用します。

インターフェイス上の複数の NAT DIA 方式

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a、Cisco Catalyst SD-WAN Manager リリース 20.14.1

NAT 設定には、インターフェイス オーバーロード、インターフェイス DIA プール、またはインターフェイスループバックを含めることができます。1つのインターフェイスに複数のNATプールを許可し、プールに一致しないトラフィックにはデフォルトのインターフェイスを設定できるため、NAT DIA を設定するための堅牢なオプションが提供されます。Cisco IOS XE Catalyst SD-WAN デバイス を設定すると、内部サブネットからの NAT DIA トラフィックは 1 つのパブリック IP アドレスに割り当てられ、他のすべての NAT DIA トラフィックはデフォルトのインターフェイスにフォールバックします。

たとえば、電話機の特定サブネットの IP を大部分のインターネットトラフィックとは異なるパブリックアドレスに変換する NAT を適用する必要がある場合があります。また、音声にパブリッククラウドサービスを使用し、音声サブネットのすべてのトラフィックで特定の IP アドレスを使用する必要がある場合もあります。これらのシナリオでは、特定のDIAトラフィック用に複数の NAT プールが必要であり、通常のトラフィック用のデフォルト NAT インターフェイスも必要です。

CLI コマンド、機能テンプレート、または設定グループを使用して、複数の NAT DIA 方式を設定できます。複数の NAT タイプを使用してインターフェイスを設定した後、match-action 条件に基づいてルールを作成するための一元管理型トラフィックポリシーを設定します。設定されたポリシー一致条件と指定した終了 DIA インターフェイスに基づいて、ポリシーは送信元アドレス変換に適切な NAT 方式を選択します。

複数の NAT DIA 方式が存在する場合、トラフィックは任意の DIA インターフェイスで終了でき、対応する NAT タイプが選択されます。トラフィックが特定の NAT DIA インターフェイスを通過するようにするには、ローカルTLOCオプションを含めるように一元管理型トラフィックポリシーを設定し、NAT DIA インターフェイスに優先 TLOC カラーを割り当てます。一致条件に基づいて、ポリシーは出力の優先カラーに関連付けられた DIA インターフェイスを選択します。

（注）
- この機能は IPv4 アドレスのみをサポートします。
- 特定の一致条件（データポリシーのシーケンス）では、複数の送信元 DIA インターフェイスまたは送信元 DIA プールを同じ一致インターフェイスに対応させることはできません。ただし、別のシーケンスで指定できます。たとえば、デフォルトの NAT タイプがインターフェイス オーバーロードの場合、同じインターフェイスの 2 番目の方式（match-interface）をインターフェイス オーバーロードにすることはできません。ただし、2 番目の方式は、NAT プールまたはループバック インターフェイスにすることができます。

NAT DIA の利点

- 優れたアプリケーション パフォーマンスを実現
- 帯域幅の消費と遅延の削減に貢献
- 帯域幅コストの削減に貢献
- リモートサイトでの DIA による、ブランチオフィスのユーザーエクスペリエンスの向上

NAT DIA の制限事項

- NAT64：
  - NAT DIA プールは NAT64 ではサポートされていません。
- 複数の NAT DIA：
  - インターフェイスごとに複数の NAT DIA プールをサポートするには、Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a 以降が必要です。
- 複数の NAT マッピング：
  - NAT マッピングには、インターフェイス過負荷、インターフェイス DIA プール、またはインターフェイスループバックを含めることができます。同じインターフェイスでの複数の NAT マッピングには、Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a 以降が必要です。
- 共有 IP アドレス：
  - NAT プールで使用される IP アドレスは、インターフェイスアドレスまたはスタティック アドレス マッピングと共有できません。
- WAN インターフェイスには少なくとも 1 つの NAT が必要：
  - 少なくとも 1 つの形式の NAT が WAN インターフェイスで有効になっていない場合、Cisco SD-WAN Manager はサービス側 VPN である [Cisco VPN] テンプレートに NAT DIA ルートを設定しません。
- 非トンネルトラフィック
  - NAT DIA または非トンネルトラフィックは、L3 TLOC 拡張ではサポートされません。
- ポート割り当て制限
  - 単一の IP アドレスに NAT DIA を設定する場合、TCP および UDP プロトコル用にそれぞれ約 55,000 個のポートを変換でき、合計で最大 110,000 個のポート変換が可能です。

- 複数の IP アドレス（NAT プール）に NAT DIA を設定する場合、プール内の IP アドレスごとに約 62,000 個のポートを TCP および UDP プロトコル用に変換できます。NAT プールからの IP アドレスはランダムに選択され、ラウンドロビン方式に基づいていません。

NAT DIA の設定

NAT DIA を有効にするためのワークフロー

1. 既存の [Cisco VPN Interface Ethernet] テンプレートを編集して、NAT を有効にします。Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a から、インターフェイスに複数の NAT タイプを設定できます。
   1. インターフェイスの過負荷（デフォルト）を設定します。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a から、設定した最初の NAT タイプが **Cisco VPN インターフェイス イーサネット**のデフォルトまたはプライマリ NAT 方式になります。インターフェイス オーバーロード、NAT プール、またはループバック インターフェイスのいずれかです。

そのインターフェイスに設定する追加の NAT タイプは、セカンダリ NAT 方式になります。

   2. NAT プールを設定します。
   3. ループバック インターフェイスを設定します。

      ループバック インターフェイスの設定の詳細については、「NAT プールおよびループバック インターフェイスの設定」を参照してください。
   4. （オプション） スタティック NAT を設定します。

      スタティック NAT の設定の詳細については、「サービス側スタティック NAT の設定」を参照してください。

2. [Cisco VPN] テンプレートを使用して NAT DIA ルートを設定します。これは、サービス VPN からのユーザートラフィックをインターネット トランスポートに直接転送するために使用されるサービス側 VPN テンプレートです。

NAT プールとループバック インターフェイスの設定

NAT プールは、必要に応じて NAT 変換に割り当てられる IPv4 アドレスの範囲です。

ループバック インターフェイスと呼ばれるソフトウェアのみのインターフェイスを指定して、物理インターフェイスをエミュレートできます。ループバック インターフェイスは、デバイス上の仮想インターフェイスであり、無効にするまでアップ（アクティブ）のままです。Cisco

IOS XE Catalyst SD-WAN リリース 17.14.1a から、インターフェイスに複数の NAT タイプを設定できます。

設定グループを使用した NAT DIA の設定

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]** を選択します。
2. 設定グループ名の横にある […] をクリックし、[Edit] を選択します。
3. [Transport & Management Profile] をクリックします。
4. [Actions] で […] をクリックして、**VPN0** 機能を編集します。
5. [Add Sub-Feature] をクリックし、[Ethernet Interface] を選択します。
6. [NAT] をクリックします。
7. [IPv4 Settings] をクリックします。
8. [NAT] ドロップダウンリストで、スコープを [Default] から [Global] に変更し、[On] をクリックして NAT を有効にします。
9. 次のいずれかのオプションを選択して、[NAT Type] を設定します。
   - interface
   - pool
   - loopback

   Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a から、[Add Multiple NAT] をクリックして、さらに NAT プールを設定します。

   デフォルトは [Interface] オプションです。
10. [NAT Type] フィールドで、[Pool] オプションをクリックし、次の NAT プールパラメータを入力します。

表 *2 : NAT* プールパラメータ

パラメータ名	説明
範囲の開始	NAT プールの開始 IP アドレスを入力します。 **1.** フィールドを有効にするには、スコープを [Default] から [Global] に変更します。 **2.** NAT プールの開始 IP アドレスを入力します。

パラメータ名	説明
範囲の終了	NAT プールの終了 IP アドレスを入力します。 **1.** フィールドを有効にするには、スコープを [Default] から [Global] に変更します。 **2.** NAT プールの最後の IP アドレスを入力します。
Prefix Length	NAT プールのプレフィックス長を入力します。
[UDP Timeout]	UDP セッションを介した NAT 変換がタイムアウトする時刻を入力します。 範囲：1 ～ 8947 分 デフォルト：1 分
[TCP Timeout]	TCP セッションを介した NAT 変換がタイムアウトする時刻を入力します。 範囲：1 ～ 8947 分 デフォルト：60 分（1 時間）

11. ループバック インターフェイスを設定します。Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a から、[Add Multiple NAT] をクリックして、複数のループバック インターフェイスを設定します。

[NAT Type] フィールドで、[Loopback] オプションをクリックし、ループバック インターフェイスの名前を入力します。

（注） 特定の一致条件（データポリシーのシーケンス）では、複数の送信元 DIA インターフェイスまたは送信元 DIA プールを同じ一致インターフェイスに対応させることはできません。ただし、別のシーケンスで指定できます。たとえば、デフォルトの NAT タイプがインターフェイス オーバーロードの場合、同じインターフェイスの 2 番目の方式（match-interface）をインターフェイス オーバーロードにすることはできません。ただし、2 番目の方式は、NAT プールまたはループバック インターフェイスにすることができます。

12. [Save] をクリックします。

ポリシーグループを使用した一致パラメータとアクションパラメータの設定

設定グループを使用して複数の NAT タイプを設定した後、match-action 条件を適用するように [Application & Priority SLA] ポリシーを設定します。NAT DIA トラフィックが一元管理型データポリシーの一致部分の条件に一致した場合、パケットは受け入れられます。その後、受け入れられたパケットにアクションパラメータを関連付けることができます。詳細については、「Application and Priority SLA」を参照してください。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Policy Groups]** > **[Application & Priority SLA]** を選択します。
2. ポリシーグループ名の横にある [...] をクリックし、[Edit] を選択します。
3. ページの右上隅にある [Advanced Layout] ボタンをクリックして、詳細ビューに切り替えます。
4. [Add Traffic Policy] をクリックし、新しいトラフィックポリシーの詳細を入力して、[Accept] を選択します。
5. [Add] をクリックします。
6. [Add Rules] をクリックし、トラフィックの名前とシーケンスを入力します。詳細については、「Configure Traffic Rules」[英語] を参照してください。
7. [Add Match] をクリックして、一致条件をルールに関連付けます。詳細については、「Match Parameters - Data Policy」を参照してください。
8. [Add Action] をクリックし、[NAT VPN] を選択して、前の手順で指定した一致条件に NAT DIA アクションを関連付けます。
   - [DIA Pool]：NAT DIA プールのカンマ区切りリストを入力します。最大 4095 個の NAT プールを入力できます。
   - [DIA Interface]：NAT DIA インターフェイスのカンマ区切りリストを入力します。
   - [ByPass]：トラフィックは、送信元 IP アドレスに NAT を適用せずに、パブリックインターネットに関連付けられた DIA インターフェイスから出ます。

機能テンプレートを使用した NAT DIA の設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Cisco VPN Interface Ethernet] テンプレートを編集するには、テンプレート名の横にある [...] をクリックし、[Edit] を選択します。

4. [NAT] をクリックします。
5. [IPv4] をクリックします。
6. [NAT] ドロップダウンリストで、スコープを [Default] から [Global] に変更し、[On] をクリックして NAT を有効にします。
7. インターフェイスの過負荷を設定します。

   [NAT Type] フィールドで、[Interface] がインターフェイス過負荷モードに対して有効になっていることを確認します。

   デフォルトは [Interface] オプションです。
8. NAT プールを設定します。Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a から、[Add Multiple NAT] をクリックして、さらに NAT プールを設定します。

   [NAT Type] フィールドで、[Pool] オプションをクリックし、次の NAT プールパラメータを入力します。

表 *3 : NAT* プールパラメータ

パラメータ名	説明
[NAT Pool Range Start]	NAT プールの開始 IP アドレスを入力します。 1. フィールドを有効にするには、スコープを [Default] から [Global] に変更します。 2. NAT プールの開始 IP アドレスを入力します。
[NAT Pool Range End]	NAT プールの終了 IP アドレスを入力します。 1. フィールドを有効にするには、スコープを [Default] から [Global] に変更します。 2. NAT プールの最後の IP アドレスを入力します。
[NAT Pool Prefix Length]	NAT プールのプレフィックス長を入力します。

パラメータ名	説明
Overload	[On] をクリックして、ポートごとの変換を有効にします。デフォルトは [On] です。 （注） [Overload] が [Off] に設定されている場合、ダイナミック NAT のみがエンドデバイスで設定されます。ポートごとの NAT は設定されていません。
[UDP Timeout]	UDP セッションを介した NAT 変換がタイムアウトする時刻を入力します。 範囲：1 ～ 8947 分 デフォルト：1 分
[TCP Timeout]	TCP セッションを介した NAT 変換がタイムアウトする時刻を入力します。 範囲：1 ～ 8947 分 デフォルト：60 分（1 時間）

9. ループバック インターフェイスを設定します。Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a から、[Add Multiple NAT] をクリックして、複数のループバック インターフェイスを設定します。

[NAT Type] フィールドで、[Loopback] オプションをクリックし、次の値を入力します。

表 *4 : NAT* ループバックパラメータ

パラメータ	説明
[NAT Inside Source Loopback Interface]	ループバック インターフェイスの IP アドレスを指定します。
[UDP Timeout]	UDP セッションを介した NAT 変換がタイムアウトする時刻を入力します。 デフォルト設定：1 分範囲：1 ～ 65536 分
[TCP Timeout]	TCP セッションを介した NAT 変換がタイムアウトする時刻を入力します。 デフォルトは 60 分（1 時間）です。範囲：1 ～ 65536 分

（注） 1 つの仮想インターフェイスで NAT 設定を持つ 1 つのテンプレートのデバイスを、別の仮想インターフェイスで NAT 設定を持たない別のテンプレートに移動する場合、NAT 設定を再度有効にする前に、最初に NAT 設定を無効にしてから仮想インターフェイスを削除する必要があります。デバイスが最初に接続されたテンプレートで NAT を無効にします。

10. [更新（Update）] をクリックします。

一元管理型データポリシーを使用した一致パラメータとアクションパラメータの設定

機能テンプレートを使用して複数の NAT タイプを設定した後、match-action 条件を適用するように一元管理型データポリシーでトラフィックルールを設定します。NAT DIA トラフィックが一元管理型データポリシーの一致部分の条件に一致した場合、パケットは受け入れられます。その後、受け入れられたパケットにアクションパラメータを関連付けることができます。トラフィックポリシーの設定に関する詳細については、「Configure Traffic Rules」を参照してください。トラフィック ポリシーを作成したら、一致条件とアクション条件を指定します。

1. トラフィックデータポリシーを設定します。詳細については、「Configure Traffic Rules」[英語] を参照してください。
2. トラフィックデータポリシーでカスタムシーケンスタイプを作成したら、[Sequence Rule] をクリックし、新しいトラフィックポリシーの詳細を設定し、[Accept] を選択します。
3. 一致条件を設定します。詳細については、「Match Parameters - Data Policy」を参照してください。
4. **[Actions]** > **[Accept]** の順にクリックします。
5. [NAT VPN] をクリックし、次の NAT DIA アクションから選択して、前の手順で指定した一致条件に関連付けます。
   - [ByPass]：トラフィックは、送信元 IP アドレスに NAT を適用せずに、パブリックインターネットに関連付けられた DIA インターフェイスから出ます。
   - [Pool]：NAT DIA プールのカンマ区切りリストを入力します。最大 4095 個の NAT プールを入力できます。
   - [Interface]：NAT DIA インターフェイスのカンマ区切りリストを入力します。最大 4 つのインターフェイスを入力できます。

CLI を使用した複数の NAT タイプの設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a、Cisco Catalyst SD-WAN Manager リリース 20.14.1

1. NAT DIA インターフェイスを設定します。

```
interface interface-name
 ip address ip-address prefix/length
 no ip redirects
```

```
 load-interval interval-number
 negotiation auto
 ip nat outside
 !
```

2. デフォルトの NAT 方式が NAT プールであり、代替またはセカンダリ NAT 方式がインターフェイス オーバーロードである複数の NAT DIA 方式を設定します。

   ```
   ip nat inside source list list-name pool pool-name overload egress-interface
   interface-name
   ```

3. **match-interface** キーワードを使用して、代替またはセカンダリ NAT 方式を設定します。ここで、代替またはセカンダリ NAT 方式はインターフェイス オーバーロードです。

   ```
   ip nat inside source list list-name interface interface-name overload match-interface
    interface-name
   ```

   match-interface キーワードの詳細については、『*Cisco Catalyst SD-WAN Qualified Command Reference Guide*』の ip nat inside source コマンドを参照してください。

次に、デフォルトの NAT 方式が NAT プールを使用し、代替またはセカンダリ NAT 方式が match-interface によるインターフェイス オーバーロードを使用する、複数の NAT DIA を設定するための設定例を示します。

```
interface GigabitEthernet1
 ip address 10.1.1.1 255.255.255.0
 no ip redirects
 load-interval 30
 negotiation auto
 ip nat outside
 !
 ip nat inside source list dia-list pool natpool1 overload egress-interface
GigabitEthernet1
 ip nat inside source list dia-list interface GigabitEthernet1 overload match-interface
 GigabitEthernet1
```

次に、デフォルトの方式が NAT プールまたはインターフェイス オーバーロードである場合に、代替またはセカンダリ NAT 方式としてループバック インターフェイスを設定する例を示します。

```
interface GigabitEthernet1
 ip address 10.1.1.1
 no ip redirects
 load-interval 30
 negotiation auto
 ip nat outside
 !
 ip nat inside source list dia-list interface Loopback10 overload match-interface
GigabitEthernet1
 ip nat inside source list dia-list interface Loopback11 overload match-interface
GigabitEthernet1
```

次に、デフォルトの方式がインターフェイス オーバーロードまたは NAT プールである場合に、NAT プールを代替方式またはセカンダリ方式として設定する例を示します。

```
interface GigabitEthernet1
 ip address 10.1.1.1
 no ip redirects
 load-interval 30
 negotiation auto
 ip nat outside
 !
```

```
ip nat pool natpool10 10.10.10.10 10.10.10.10 prefix-length 24
ip nat inside source list dia-list pool natpool1 overload match-interface GigabitEthernet1

ip nat inside source list dia-list pool natpool2 overload match-interface GigabitEthernet1
```

トラフィックデータポリシーの設定

機能テンプレートを使用して複数の NAT タイプを設定した後、match-action 条件を適用するように一元管理型データポリシーでトラフィックルールを設定します。NAT DIA トラフィックが一元管理型データポリシーの一致部分の条件に一致した場合、パケットは受け入れられます。

次に、トラフィックデータポリシーを設定するための設定例を示します。

```
data-policy data-policy-name
  vpn-list list-name
   sequence sequence-number
    match source-data-prefix-list data-prefix list-name
    !
    action accept
     count vpn-list-name
     nat use-vpn 0
     nat source-dia-pool pool-id
     nat source-dia-interface interface-name
    !
   !
   default-action drop
  !
```

次に、トラフィックデータポリシーの設定例を示します。

```
data-policy MULTIPLE-NAT-DIA-TRAFFIC
  vpn-list VPN1
   sequence 1
    match source-data-prefix-list NAT-DIA-PREFIX-LIST
    !
    action accept
     count VPN1-TRAFFIC
     nat use-vpn 0
     nat source-dia-pool 1
         !
   !
   default-action drop
  !
```

トラフィックデータポリシーの設定の詳細については、「Configure Centralized Policies Using the CLI」を参照してください。

次に、上記のトラフィックデータポリシーに対応する設定例を示します。デフォルトの NAT 方式はインターフェイス オーバーロードであり、代替またはセカンダリ NAT 方式は NAT プールです。

```
interface GigabitEthernet1
 ip address 10.1.1.1 255.255.255.0
 no ip redirects
 load-interval 30
 negotiation auto
 ip nat outside
 !
 ip nat inside source list dia-list pool natpool1 overload match-interface GigabitEthernet1
```

```
ip nat inside source list dia-list interface GigabitEthernet1 overload
```

NAT DIA ルートの設定

すべてのサービス VPN は、パケットを DIA トラフィック用のトランスポート VPN にルーティングします。サービス側 VPN の NAT DIA ルートを設定します。

（注） サービス側 VPN である [Cisco VPN] テンプレートで IPv4 DIA ルートを設定します。

Cisco VPN テンプレートを使用した NAT DIA ルートの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]**を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Cisco VPN] テンプレートを編集するには、テンプレート名の横にある **...** をクリックし、[Edit] を選択します。
4. [IPv4 Route] をクリックします。
5. [New IPv4 Route] をクリックします。
6. [Prefix] フィールドに、NAT の IPv4 プレフィックスを入力します。
7. [Gateway] フィールドで、[VPN] をクリックします。
8. [Enable VPN] ドロップダウンリストで、スコープを [Default] から [Global] に変更し、[On] をクリックして VPN を有効にします。
9. [更新（Update）] をクリックします。

CLI を使用した NAT DIA ルートの設定

以下は、NAT DIA ルートを設定するための設定例です。

```
Device(config)# interface GigabitEthernet3
ip address 192.0.2.1 255.255.255.0
ip nat outside
no shut

interface GigabitEthernet2
vrf forwarding 1
ip address 10.0.0.1 255.255.255.0
no shut
```

```
ip nat route vrf 1 0.0.0.0 0.0.0.0 global
ip route 0.0.0.0 0.0.0.0 192.0.2.2
```

NAT DIA ルート設定の確認

次に、**show ip route** コマンドの出力例を示します。

```
Device# show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
```

次に、**show ip route vrf 1** コマンドの出力例を示します。

```
Device# show ip route vrf 1

Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
```

OMP を介した NAT ルートのアドバタイズ

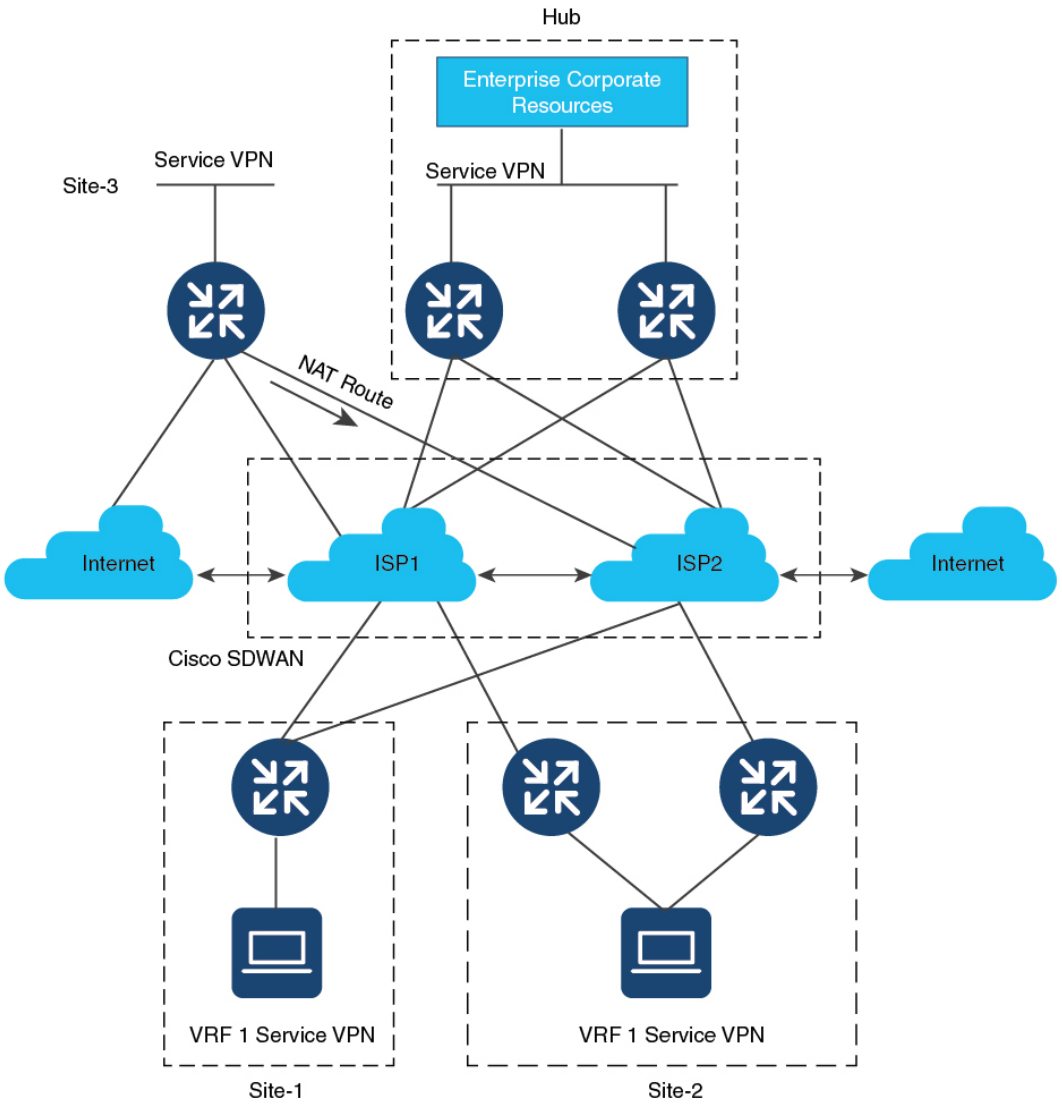
次のセクションでは、OMP を介した NAT ルートのアドバタイズについて説明します。

OMP を介した NAT ルートのアドバタイズに関する情報

Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降、OMP を介してアドバタイズされるように NAT DIA デフォルトルートを設定できます。OMP はすべての Cisco IOS XE Catalyst SD-WAN デバイス でデフォルトで有効になっているため、OMP を明示的に設定または有効にする必要はありません。オーバーレイネットワークが機能するには、OMP が動作可能である必要があります。OMP を無効にすると、オーバーレイネットワークが無効になります。

NAT64 アドバタイズメントがネットワーク上の指定された Cisco IOS XE Catalyst SD-WAN デバイス のいずれかに設定されている場合、OMP は NAT デフォルトルートをブランチにアドバタイズします。ブランチはデフォルトルートを受け取り、それを使用してすべての DIA トラフィックのハブに到達します。Cisco IOS XE Catalyst SD-WAN デバイス は、すべての DIA トラフィックのインターネットゲートウェイとして機能します。

図 *1 : OMP* を使用した *NAT* ルートのアドバタイズ



CLI を使用した OMP による NAT ルートのアドバタイズの有効化

OMP を介してデフォルトルートをアドバタイズするには、**sdwan omp** コマンドを使用します。

次の設定を使用して、OMP を介して NAT ルートをアドバタイズします。

（注） このコマンドは、デバイス CLI テンプレートのみを使用してテストされています。

```
ip nat route vrf 1 0.0.0.0 0.0.0.0 global
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet3 overload
sdwan
 omp
  address-family vrf 1
```

```
   advertise network 0.0.0.0/0
interface GigabitEthernet3
 ip nat outside
```

（注） NAT DIA が設定されている場合にのみ、NAT ルートがアドバタイズされるようにします。

advertise network キーワードは、OMP への NAT ルートのアドバタイズメントを設定する際に必須です。

CLI を使用した OMP による NAT ルートのアドバタイズの確認

デフォルトルート情報を表示するには、**show sdwan omp routes** コマンドを使用します。

```
Device# show sdwan omp routes

Code:
C -> chosen
I -> installed
Red -> redistributed
Rej -> rejected
L -> looped
R -> resolved
S -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA -> On-demand inactive
U -> TLOC unresolved
                          PATH                ATTRIBUTE
VPN PREFIX      FROM PEER ID LABEL STATUS    TYPE       TLOC IP  COLOR        ENCAP
  PREFERENCE
10 0.0.0.0/0          10.1.1.3 23 1002 C,I,R     installed 10.1.1.10 biz-internet ipsec
         -
                      10.1.1.3 24 1002 R         installed 10.1.1.30 biz-internet ipsec
         -
10 10.2.0.0/16        10.1.1.3 27 1002 C,I,R     installed 10.1.1.10 biz-internet ipsec
         -
                      10.1.1.3 28 1002 R         installed 10.1.1.30 biz-internet ipsec
         -
10 172.254.32.76/30   10.1.1.3 26 1002 C,I,R     installed 10.1.1.30 biz-internet ipsec
         -
10 172.254.51.124/30  10.1.1.3 25 1002 C,I,R     installed 10.1.1.30 biz-internet ipsec
         -
10 172.254.249.164/30 10.1.1.3 22 1002 C,I,R     installed 10.1.1.10 biz-internet ipsec
         -
10 172.254.252.12/30  10.1.1.3 21 1002 C,I,R     installed 10.1.1.10 biz-internet ipsec
         -
10 172.30.1.0/24       0.0.0.0 75 1002 C,Red,R          installed 10.1.1.26 gold
  ipsec         -
                       0.0.0.0 76 1002 C,Red,R          installed 10.1.1.26 silver
  ipsec         -
                       10.1.1.3 29 1002 Inv,U      installed 10.1.1.36 gold
ipsec         -
                       10.1.1.3 30 1002 Inv,U      installed 10.1.1.36 silver
ipsec         -
```

スポークで作成された NAT DIA ルートに関する情報を表示するには、 **show ip route vrf 1** コマンドを使用します。

```
Device# show ip route vrf 10

Routing Table: 10
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, 0 - OSPF, IA - OSPF inter area N1 - OSPF NSSA external
type 1, N2 - OSPF NSSA external type 2  El - OSPF external type 1, E2 - OSPF external
type m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT IA i - IS-IS, su - IS-IS summary,
Ll - IS-IS level-1, L2 - IS-IS level-2 is - IS-IS inter area, * - candidate default, U
- per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, 1 - LISP a - application route
+ - replicated route, % - next hop override, p - overrides from PfR & - replicated local
 route overrides by connected

Gateway of last resort is 10.1.1.10 to network 0.0.0.0

m 0.0.0.0/0 [251/0] via 10.1.1.10,2d16h, Sdwan-system-intf
        10.0.0.0/16 is subnetted, 1 subnets
```

show sdwan omp routes コマンドを使用して、スポークのデフォルトルートを表示します。

```
Device# show sdwan omp routes vpn 10

Code:
C -> chosen
I -> installed
Red -> redistributed
Rej -> rejected
L -> looped
R -> resolved
S -> stale
Ext -> extranet
Inv -> invalid
Stg -> staged
IA -> On-demand inactive
U -> TLOC unresolved
                          PATH            ATTRIBUTE
VPN PREFIX      FROM PEER ID LABEL STATUS TYPE    TLOC IP COLOR        ENCAP
PREFERENCE
10 0.0.0.0/0           10.1.1.3 23 1002 C,I,R installed 10.1.1.10 biz-internet ipsec
      -
                       10.1.1.3 24 1002 R     installed 10.1.1.30 biz-internet ipsec
      -
```

IPv6 トンネルを介した NAT DIA IPv4

次のセクションでは、IPv6 トンネルを介した NAT DIA IPv4 の設定について説明します。

IPv6 トンネルを介した NAT DIA IPv4 に関する情報

IPv6 トンネルを介した NAT DIA IPv4 により、IPv6 専用デバイスは IPv4 Web サイトおよびサービスにアクセスできます。

トラフィックフローは、オーバーレイネットワークのサービス側（LAN）からトランスポート側（WAN）です。

サービス側の送信 IPv4 アドレスは、トンネルインターフェイスでパブリック IPv4 アドレスに変換されます。

デバイス CLI または CLI アドオンテンプレートを使用して、IPv6 トンネル経由で NAT DIA IPv4 を設定します。

IPv6 トンネルを介した NAT DIA IPv4 の利点

- IPv6 専用デバイスからの IPv4 アクセスを提供します。
- IPv6 トンネルを介した IPv4 トラフィックのルーティングをサポートします。
- トンネルインターフェイスで、サービス側送信元IPv4 アドレスからパブリック IPv4 アドレスへの変換をサポートします。

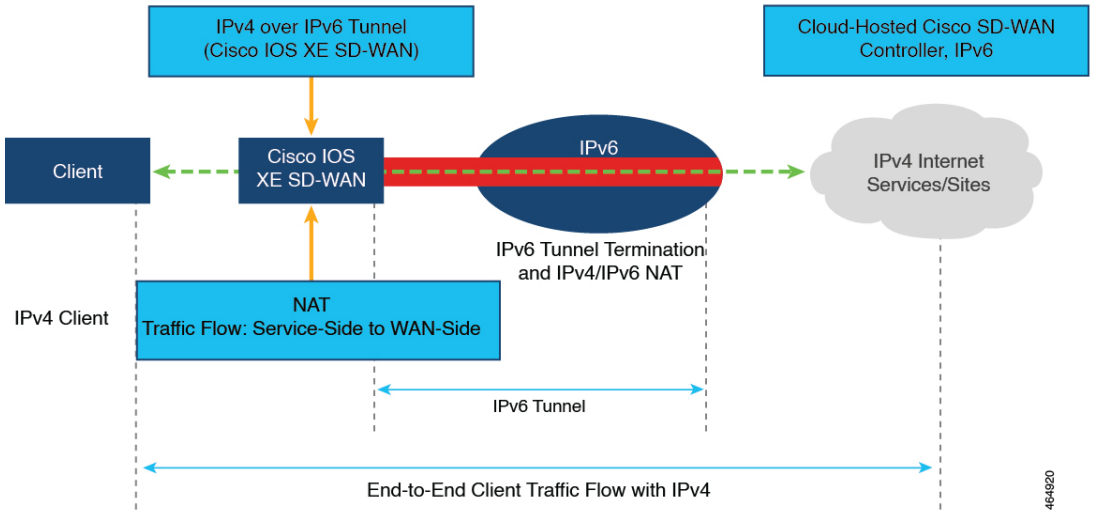
IPv6 トンネルを介した NAT DIA IPv4 の制限事項

- NAT DIA トラッカーはサポートされていません。
- 統合脅威防御（UTD）はサポートされていません。
- トンネルインターフェイスでのキープアライブトラフィックはサポートされていません。

IPv6 トンネルを介した NAT DIA IPv4 の使用例

顧客は IPv6 専用のデバイスを持っていますが、IPv4 の Web サイトとサービスにアクセスする必要があります。このシナリオをサポートするには、IPv4 トラフィックをインターネットに転送するために IPv6 トンネルを使用します。

図 *2 : IPv6* トンネルサポートを介した *NAT DIA IPv4*

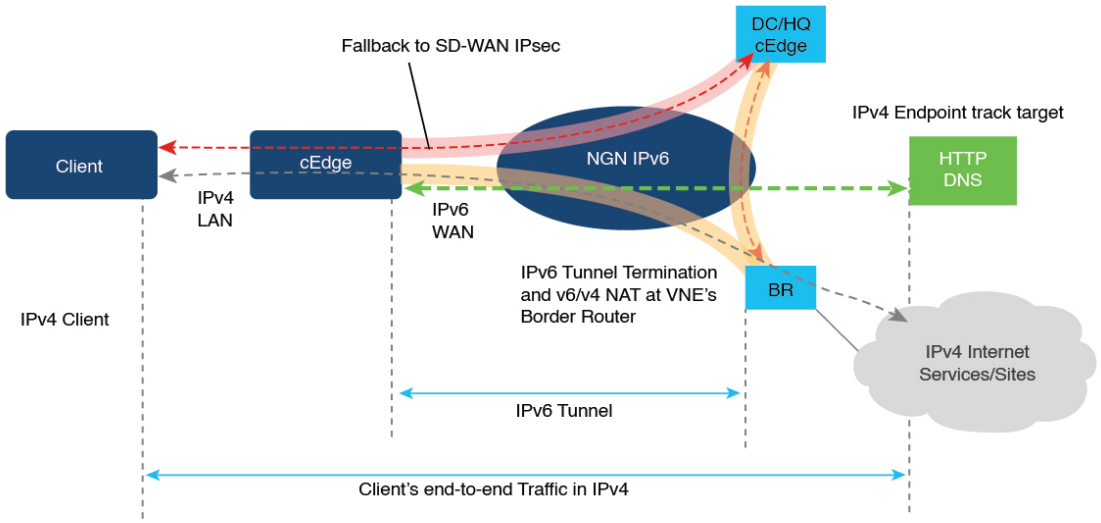


サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a および Cisco vManage リリース 20.11.1

ボーダールータは、IPv6 トラフィックと IPv4 トラフィック間のゲートウェイとして機能し、スタティック IPv6 トンネルを介して IPv4 方向のトラフィックを送信します。ボーダールータ

と IPv6 トンネルが到達不能な場合、WAN エッジデバイスは IPv6 トンネルが非アクティブであるかどうかを判断できないため、トラフィックを再ルーティングできません。

IPv4 DIA トラッカーを IPv6 トンネルとボーダールータに関連付けると、WAN エッジデバイスは、トラッカーのステータスに基づいて IPv6 トンネルがアクティブかどうかを判断できます。IPv4 トラッカーが非アクティブの場合、関連付けられた IPv6 トンネルも非アクティブになり、トラフィックはルーティングテーブルに基づいて代替パスに再ルーティングされます。IPv4 トラッカーがアクティブな場合、関連付けられている IPv6 トンネルもアクティブになり、トラフィックは IPv6 トンネルで再開されます。



IPv6 トンネルを介して NAT DIA IPv4 を設定するためのワークフロー

Cisco SD-WAN Manager の設定

1. 既存の [Cisco VPN Interface Ethernet] テンプレートを編集して、NAT を有効にします。
   1. インターフェイスの過負荷（デフォルト）を設定します。
   2. NAT プールを設定します。

      NAT プールの設定の詳細については、「NAT プールとループバック インターフェイスの設定」を参照してください。

2. [Cisco VPN] テンプレートを使用して NAT DIA ルートを設定します。

   NAT DIA ルートの設定の詳細については、「NAT DIA ルートの設定」を参照してください。

CLI 設定

1. IPv6 トンネルを介して IPv4 を設定します。
2. トンネルインターフェイスで **ip nat outside** コマンドを設定します。
3. IPv6 トンネルを介して IPv4 トラフィックをルーティングするための NAT DIA ルートを設定します。

CLI を使用した IPv6 トンネル経由の NAT DIA IPv4 の設定

1. IPv6 トンネルのグローバルデフォルトルートを設定します。

```
Device(config)# interface Tunnel1000
Device(config-if)# ip address 10.1.15.15 255.255.255.0
Device(config-if)# ip mtu 1460
Device(config-if)# ip tcp adjust-mss 1420
Device(config-if)# load-interval 30
Device(config-if)# tunnel source GigabitEthernet3
Device(config-if)# tunnel mode ipv6
Device(config-if)# tunnel destination 2001:DB8:A1:10::10
Device(config-if)# tunnel route-via GigabitEthernet3 mandatory
Device(config-if)# tunnel path-mtu-discovery
!
Device(config)# ip route 0.0.0.0 0.0.0.0 Tunnel1000
```

2. **ip nat outside** コマンドを使用して、IPv6 トンネルを介して IPv4 を設定します。

```
Device(config)# interface Tunnel1000
Device(config)# ip nat outside
```

3. NAT プールとインターフェイス過負荷モードを使用して、IPv6 トンネルを介して IPv4 を設定します。

```
Device(config)# interface Tunnel1000
Device(config)# ip nat inside source list nat-dia-vpn-hop-access-list interface
Tunnel1000 overload
```

または

```
Device(config)# ip nat pool natpool10 203.0.113.1 203.0.113.25 prefix-length 24
Device(config)# ip nat inside source list nat-dia-vpn-hop-access-list pool natpool10
 overload egress-interface Tunnel1000
```

4. サービス側 VPN 内で NAT DIA ルートを設定します。

```
Device(config)# ip nat route vrf 10 0.0.0.0 0.0.0.0 global
```

（注） 一元化されたデータポリシーを使用して NAT DIA ルートを設定している場合は、**nat use-vpn 0** コマンドを使用します。

CLI を使用した IPv6 トンネル経由の NAT DIA IPv4 の設定（Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a リリース以降）

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a および Cisco vManage リリース 20.11.1

CLI テンプレートの使用の詳細については、CLI テンプレートおよび CLI アドオン機能テンプレートを参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

IPv4 NAT DIA トラッカーを使用して、IPv6 トンネルを介した NAT DIA IPv4 を設定できます。NAT DIA トラッカーの詳細については、「NAT DIA トラッカー （68 ページ）」を参照してください。

1. エンドポイントのステータスをトラッキングするためのエンドポイントトラッカーを設定します。

   endpoint-tracker *tracker-name*

2. エンドポイントの IP アドレスを設定します。

   endpoint-ip *ip-address*

3. トラッカーのトラッカータイプを設定します。

   tracker-type *interface-name*

4. IPv6 トンネル経由の NAT DIA IPv4 を設定します。

   詳細については、CLI を使用した IPv6 トンネル経由の NAT DIA IPv4 の設定 （29 ページ）を参照してください。

IPv4 DIA トラッカーを使用して IPv6 トンネル経由の NAT DIA IPv4 を設定するための完全な設定例を次に示します。

```
endpoint-tracker test1
 endpoint-ip 10.0.12.13
 tracker-type interface

   interface Tunnel5
   ip address 192.168.9.2 255.255.255.0
   ip nat outside
   endpoint-tracker test1
   tunnel source GigabitEthernet8
   tunnel mode ipv6
    tunnel destination 2A00:B00::1D1E:CA68
    tunnel path-mtu-discovery

    interface GigabitEthernet8
    no ip address
    negotiation auto
    ipv6 address 2A00:B00::1D1E:CA58/64
```

```
    no mop enabled
    no mop sysid

ip nat inside source list nat-dia-vpn-hop-access-list interface Tunnel5 overload

ip nat route vrf 1 0.0.0.0 0.0.0.0 global
ip route 0.0.0.0 0.0.0.0 Tunnel5
```

CLI アドオンテンプレートを使用した IPv6 トンネルによる NAT DIA IPv4 の設定

はじめる前に

新しいCLIアドオンテンプレートを作成するか、既存のCLIアドオンテンプレートを編集します。

CLI Add-on Feature Templates の詳細については、「CLI Add-on Feature Templates」を参照してください。

CLI アドオンテンプレートを使用した IPv6 トンネルによる NAT DIA IPv4 の設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. [Add template] をクリックします。
4. デバイスリストからデバイスを選択します。
5. OTHER TEMPLATES 領域で、CLI Add-On Template をクリックします。
6. [CLI Add-On Template] エリアで、設定を入力します。
7. 次の設定例に示すように、IPv6 トンネルを介して IPv4 を設定します。

```
interface Tunnel1000
 no shutdown
 ip address 203.0.113.1 255.255.255.0
 ip nat outside
 load-interval 30
 tunnel source GigabitEthernet1
 tunnel destination 2001:DB8:A1:10::10
 tunnel mode ipv6
 tunnel path-mtu-discovery
 tunnel route-via GigabitEthernet1 mandatory
!
ip nat inside source list nat-dia-vpn-hop-access-list interface Tunnel1000 overload
ip route 0.0.0.0 0.0.0.0 Tunnel1000 203.0.113.2
ip nat route vrf 10 0.0.0.0 0.0.0.0 global
```

8. **[Save（保存）]** をクリックします。

   作成した CLI アドオンテンプレートが [CLI Configuration] に表示されます。
9. CLI アドオンテンプレートをデバイスにアタッチします。

IPv6 トンネル設定を介した NAT DIA IPv4 の確認

NAT DIA ルートエントリの確認

次に、**show ip nat route-dia** コマンドの出力例を示します。

```
Device# show ip nat route-dia
route add [1] addr [0.0.0.0] vrfid [2] prefix len [0]
route add [1] addr [0.0.0.0] vrfid [4] prefix len [0]
```

出力例では、2 つの NAT ルートアドバタイズメントが有効になっています。

NAT DIA ルーティング テーブル エントリの確認

次に、**show ip route vrf 1 nat-route** コマンドの出力例を示します。

```
Device# show ip route vrf 1 nat-route
Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

n*Nd  0.0.0.0/0 [6/0], 00:40:17, Null0
```

この出力例では、n*Nd 0.0.0.0/0 が構成済みの NAT DIA ルートです。

IP 変換の表示

次に、**show ip nat translations** コマンドの出力例を示します。

```
Device# show ip nat translations
show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  203.0.113.1:5201      10.20.24.150:5201     10.20.25.150:5201     10.20.25.150:5201
icmp 203.0.113.1:25440     10.20.24.150:25440    10.20.25.150:25440    10.20.25.150:25440
Total number of translations: 2
```

出力例には、2 つの変換があります。

IP NAT グローバル統計の確認

次に、**show ip nat statistics** コマンドの出力例を示します。

```
Device# show ip nat statistics
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Outside interfaces:
  Tunnel1000
Inside interfaces:
Hits: 1012528  Misses: 56
Expired translations: 3
```

```
Dynamic mappings:
-- Inside Source
[Id: 3] access-list nat-dia-vpn-hop-access-list interface Tunnel1000 refcount 2
nat-limit statistics:
 max entry: max allowed 0, used 0, missed 0
In-to-out drops: 0  Out-to-in drops: 0
Pool stats drop: 0  Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
```

出力例では、トンネル 11000 に 2 つの変換があります。

show ip nat statistics コマンドの出力には、設定したすべての IP アドレスプールと NAT マッピングに関する情報が表示されます。

NAT グローバル統計のクリア

clear ip nat statistics コマンドを使用して、NAT グローバル統計をクリアします。

```
Device# clear ip nat global statistics
```

NAT の統計情報の表示

次に、**show platform hardware qfp active feature nat datapath stats** コマンドの出力例を示します。

```
Device# show platform hardware qfp active feature nat datapath stats
Total active translations: 2 (0 static, 2 dynamic; 2 extended)
Outside interfaces:
  Tunnel1000
Inside interfaces:
Hits: 1012528  Misses: 56
Expired translations: 3
Dynamic mappings:
-- Inside Source
[Id: 3] access-list nat-dia-vpn-hop-access-list interface Tunnel1000 refcount 2
nat-limit statistics:
 max entry: max allowed 0, used 0, missed 0
In-to-out drops: 0  Out-to-in drops: 0
Pool stats drop: 0  Mapping stats drop: 0
Port block alloc fail: 0
IP alias add fail: 0
Limit entry add fail: 0
```

NAT グローバルカウンタの確認：データパスマップ

次に、**show platform hardware qfp active feature nat datapath map** コマンドの出力例を示します。

```
Device# show platform hardware qfp active feature nat datapath map
I/f Map Table

if_handle 65529 next 0x0 hash_index 220
laddr 0.0.0.0 lport 0 map 0xdec942c0 refcnt 0
gaddr 203.60.10.1 gport 0 proto 0 vrfid 0x0
src_type 1 flags 0x80100 cpmapid 3
I/f Map Table End
edm maps 0
mapping id 1 pool_id 0 if_handle 0xfff9 match_type 0 source_type 1 domain 0 proto 0 Local
 IP 0.0.0.0,
```

```
Local Port 0 Global IP 203.60.10.1 Global Port 0 Flags 0x80100 refcount 0 cp_mapping_id
 3
next 0x0 hashidx 50 vrfid 0 vrf_tableid 0x0 rg 0 pap_enabled 0 egress_ifh 0x14
```

NAT グローバルカウンタの確認：セッションダンプ

次に、**show platform hardware qfp active feature nat datapath sess-dump** コマンドの出力例を示します。

```
Device# show platform hardware qfp active feature nat sess-dump
id 0xdd70c1d0 io 10.20.24.150 oo 10.20.25.150 io 5201 oo 5201 it 203.0.113.1 ot
10.20.25.150 it 5201 ot 5201 pro 6 vrf 4 tableid 4 bck 65195 in_if 0 out_if 20 ext_flags
 0x1 in_pkts 183466 in_bytes 264182128 out_pkts 91731 out_bytes 2987880flowdb in2out fh
 0x0 flowdb out2in fh 0x0
id 0xdd70c090 io 10.20.24.150 oo 10.20.25.150 io 25965 oo 25965 it 203.0.113.1 ot
10.20.25.150 it 25965 ot 25965 pro 1 vrf 4 tableid 4 bck 81393 in_if 0 out_if 20 ext_flags
 0x1 in_pkts 27 in_bytes 38610 out_pkts 27 out_bytes 38610flowdb in2out fh 0x0 flowdb
out2in fh 0x0
```

IPv6 トンネルを介した NAT DIA IPv4 の設定例

```
Device# show sdwan running-config | section Tunnel1000|GigabitEthernet1
interface GigabitEthernet1
 ip address 10.1.15.15 255.255.255.0
 no ip redirects
 load-interval 30
 negotiation auto
 ipv6 address 2001:DB8:A1:F::F/64
 ipv6 enable
 ipv6 nd ra suppress all
 service-policy output shape_GigabitEthernet1
!
interface Tunnel1000
 no shutdown
 ip address 203.0.113.1 255.255.255.0
 ip nat outside
 load-interval 30
 tunnel source GigabitEthernet1
 tunnel destination 2001:DB8:a1:10::10
 tunnel mode ipv6
 tunnel path-mtu-discovery
 tunnel route-via GigabitEthernet1 mandatory
!
ip nat inside source list nat-dia-vpn-hop-access-list interface Tunnel1000 overload
ip route 0.0.0.0 0.0.0.0 Tunnel1000 203.0.113.2
ip nat route vrf 10 0.0.0.0 0.0.0.0 global
```

NAT DIA を使用したダイヤラインターフェイス

次のセクションでは、NAT DIA を使用したダイヤラインターフェイスの設定について説明します。

NAT DIA でのダイヤラインターフェイスの使用に関する情報

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

この機能は、NAT DIA 使用例の Point-to-Point Protocol（PPP）ダイヤラインターフェイスのサポートを提供します。ダイヤラインターフェイスを使用して、IPv4インターネットサービスおよびサイトにアクセスします。

ダイヤラインターフェイスは、デフォルトルーティング情報、カプセル化プロトコル、使用するダイヤラプールなど、クライアントからのトラフィックを処理する方法を指定します。

次のダイヤラインターフェイスがサポートされています。

- Point-to-Point Protocol over Ethernet（PPPoE）
- Point-to-Point Protocol over Asynchronous Transfer Mode（PPPoA）
- Point-to-Point Protocol over Ethernet over Asynchronous Transfer Mode（PPPoEoA）

PPPoE の設定の詳細については、『*Cisco Catalyst SD-WAN Systems and Interfaces Guide, Cisco IOS XE Catalyst SD-WAN* リリース *17.x*』の「PPPoE の設定」セクションを参照してください。

NAT DIA の TCP 最大セグメントサイズの調整

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 から始めて、TCP セッションのドロップを防ぐために、TCP 最大セグメントサイズ（MSS）の値を調整できます。

TCP MSS の設定の詳細については、『*Cisco Catalyst SD-WAN Systems and Interfaces Guide, Cisco IOS XE Catalyst SD-WAN* リリース *17.x*』の「Configure TCP MSS and Clear Dont Fragment」セクションを参照してください。

NAT DIA でダイヤラインターフェイスを使用する利点

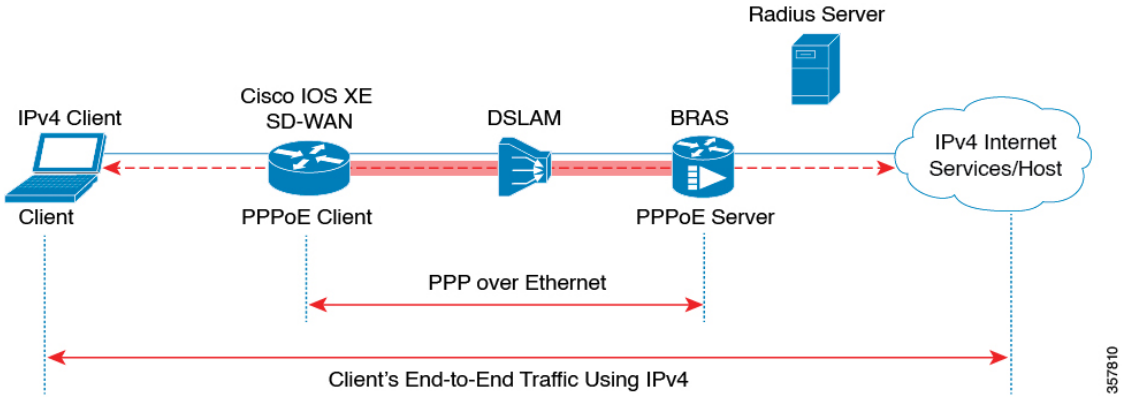
- NAT DIA によるインターフェイス過負荷モードのサポート
- NAT DIA を使用したルートベースおよびデータポリシーベースの構成のサポート
- NAT プールとループバックのサポート
- スタティック NAT 設定のサポート
- スタティック NAT ポート転送のサポート
- 着信コールまたは発信コールの要件に基づいた物理インターフェイスのさまざまな特性
- NAT DIA によるダイヤラインターフェイス経由のスタティックまたはネゴシエートされた IP アドレスのサポート

NAT DIA ダイヤラインターフェイスのワークフロー

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

次の図は、IPv4 クライアントトラフィックがダイヤラインターフェイスを介してルーティングされ、IPv4 インターネットサイトおよびサービスに到達する方法を示しています。

図 *3 : NAT DIA* ダイヤラ インターフェイス サポートのワークフロー



NAT DIA でダイヤラインターフェイスを使用する場合の制限事項

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

- ダイヤラインターフェイスでは NAT DIA のみがサポートされています。
- ダイヤラインターフェイスではサービス側 NAT はサポートされていません。
- デバイス CLI または CLI アドオンテンプレートを使用する場合、PPPoE ジャンボフレームは 1800 バイトに制限されます。
- 次の PPPoA ダイヤラ インターフェイス カプセル化の設定はサポートされていません。Cisco SD-WAN Manager 機能テンプレートを使用した AAL5MUX、AAL5SNAP、AAL5NLPID、または bridge-dot1q です。これらの PPPoA カプセル化を設定する場合は、CLI テンプレートを使用してカプセル化を設定する必要があります。
- NAT DIA トラッカーは、**ip unnumbered** インターフェイスを持つダイヤラインターフェイスではサポートされていません。
- NAT DIA パスの設定は、WAN インターフェイスのループバックではサポートされていません。

CLI テンプレートを使用した NAT DIA でダイヤラインターフェイスの設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

CLI テンプレートの使用の詳細については、CLI テンプレートおよび CLI アドオン機能テンプレートを参照してください。

1. NAT DIA を有効にして PPPoE ダイヤラインターフェイスを設定します。

Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 から使用できる **dialer down-with-vInterface** コマンドは、PPP セッションが停止したときにダイヤラインターフェイスを停止します。

```
interface interface-type-number
 pppoe enable group global
 pppoe-client dial-pool-number dialer-pool-number
!
interface Dialer dialer-number
 description interface vers le BAS
 mtu bytes
 ip address negotiated
 ip mtu bytes
 ip nat outside
 encapsulation encapsulation-type
 ip tcp adjust-mss bytes
 dialer pool dialer-pool-number
 dialer down-with-vInterface
 ppp chap hostname hostname
 ppp chap password password
 ppp authentication chap callin
 ppp ipcp route default
 service-policy output shape_Dialer dialer-number
```

2. インターフェイス オーバーロード モードでダイヤラインターフェイスを介して **ip nat outside** を有効にします。

```
interface Dialer dialer-number
ip nat outside
ip nat inside source list nat-dia-vpn-hop-access-list interface Dialer dialer-number
 overload
```

3. サービス側 VPN の NAT DIA ルートを設定します。

   サービス側 VPN の NAT DIA ルートの設定に関する詳細については、「NAT DIA ルートの設定」を参照してください。

   または

   一元化されたデータポリシーを使用して、サービス側 VPN の NAT DIA ルートを設定します。

```
ip nat route vrf vrf-id route-prefix prefix-mask global
```

（注） Pool-overload-config を使用した NAT マッピングと同じトランザクションでダイヤラインターフェイスが削除されると、追加の非 NAT 設定が生成されます。次に示すように、異なるトランザクションを使用して各 NAT 設定を個別に削除します。

```
Device(config)# no ip nat inside source list global-list pool natpool-Dialer100-0 overload
 egress-interface Dialer100
Device(config)# commit

Device(config)# no interface Dialer100
Device(config)# commit
```

NAT DIA でダイヤラインターフェイスを設定するための完全な設定例を次に示します。

```
interface Dialer100
 mtu 1492
 ip address negotiated
 ip nat outside
 encapsulation ppp
 ip tcp adjust-mss 1452
 dialer pool 100
 dialer down-with-vInterface
 endpoint-tracker tracker-google
 ppp authentication chap callin
 ppp chap hostname branch1.ppp1
 ppp chap password 7 01100F175804
 ppp ipcp route default
 service-policy output shape_GigabitEthernet0/0/1
!
interface GigabitEthernet0/0/1
 no ip redirects
 pppoe enable group global
 pppoe-client dial-pool-number 100
!
sdwan
 interface Dialer100
  tunnel-interface
   encapsulation ipsec weight 1
   color mpls restrict
  exit
 exit
ip nat inside source list nat-dia-vpn-hop-access-list interface Dialer100 overload
ip nat route vrf 10 0.0.0.0 0.0.0.0 global
```

ダイヤラインターフェイス設定の確認

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

次のセクションでは、ダイヤラインターフェイスの設定を確認する方法について説明します。

NAT DIA IP ルート設定の確認

次に、**show ip route vrf** コマンドの出力例を示します。

```
Device# show ip route vrf 10
Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PfR
& - replicated local route overrides by connected

Gateway of last resort is 0.0.0.0 to network 0.0.0.0

n*Nd 0.0.0.0/0 [6/0], 4d01h, Null0
10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
```

出力例では、`n*Nd 0.0.0.0/0` が設定済みの NAT DIA ルートです。

IP アドレスの変換の確認

次に、**show ip nat translations** コマンドの出力例を示します。

```
Device# show ip nat translations
Pro   Inside global       Inside local        Outside local     Outside global
tcp   192.0.2.1:80        10.10.0.100:8080    ---                ---
---   192.0.2.2.198       10.10.0.254         ---                ---
tcp   192.0.2.1:8000      10.10.0.253:23      ---                ---
tcp   192.0.2.25:25185    10.0.0.1:43878      203.0.113.1:80     203.0.113.1:80
tcp   192.0.2.3:48871     10.0.0.2:48871      203.0.113.2:80     203.0.113.2:80
tcp   192.0.2.3:63242     10.0.0.2:63242      203.0.113.2:80     203.0.113.2:80
tcp   192.0.2.3:52929     10.0.0.2:52929      203.0.113.2:80     203.0.113.2:80
tcp   192.0.2.4:25184     10.0.0.4:28456      203.0.113.1:80     203.0.113.1:80
udp   192.0.2.3:64681     10.0.0.2:64681      203.0.113.1:53     203.0.113.1:53
udp   192.0.2.3:65504     10.0.0.2:64670      203.0.113.1:53     203.0.113.1:53
tcp   192.0.2.25:25186    10.0.0.1:28455      203.0.113.1:80     203.0.113.1:80
Total number of translations: 11
```

サンプル出力では、11 の変換があります。

PPPoE セッションの表示

次に、**show pppoe session** コマンドの出力例を示します。

```
Device# show pppoe session
     1 client session

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st      Type
    N/A    391  84b2.61cc.9903  Gi0/0/1.100           Di100 Vi2        UP
                c884.a1f4.b981  VLAN: 100                   UP
```

この出力例では、PPPoE ダイヤラ インターフェイスが UP と表示されています。

次に、**show ppp all** コマンドの出力例を示します。

```
Device# show ppp all
Interface/ID OPEN+ Nego* Fail-     Stage    Peer Address    Peer Name
------------ --------------------- -------- --------------- --------------------
Vi2          LCP+ IPCP+ CDPCP-     LocalT   172.16.100.1    SDWAN-AGGREGE
```

PPP ネゴシエーション情報の確認

次に、**show interfaces Dialer** コマンドの出力例を示します。

```
Device# show interfaces Dialer100
Dialer100 is up, line protocol is up
  Hardware is Unknown
  Internet address is 172.16.100.101/32
  MTU 1492 bytes, BW 56 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 255/255, rxload 255/255
  Encapsulation PPP, LCP Closed, loopback not set
  Keepalive set (10 sec)
  DTR is pulsed for 1 seconds on reset
  Interface is bound to Vi2
  Last input 00:09:05, output 00:00:09, output hang never
  Last clearing of "show interface" counters 1w0d
  Input queue: 0/375/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: weighted fair
  Output queue: 0/1000/64/0 (size/max total/threshold/drops)
     Conversations  0/0/16 (active/max active/max total)
     Reserved Conversations 0/0 (allocated/max allocated)
```

```
     Available Bandwidth 56 kilobits/sec
  5 minute input rate 42220429000 bits/sec, 23 packets/sec
  5 minute output rate 1520154000 bits/sec, 23 packets/sec
     755339342 packets input, 2706571669546067 bytes
     696497150 packets output, 97523835049377 bytes
Bound to:
Virtual-Access2 is up, line protocol is up
  Hardware is Virtual Access interface
  Internet address will be negotiated using IPCP
  MTU 1492 bytes, BW 56 Kbit/sec, DLY 20000 usec,
     reliability 255/255, txload 177/255, rxload 177/255
  Encapsulation PPP, LCP Open
  Stopped: CDPCP
  Open: IPCP
```

この出力例では、`Dialer100` が稼働しており、回線プロトコルが稼働しています。`Virtual-Access2` も稼働しており、回線プロトコルも稼働しています。

NAT DIA でダイヤラインターフェイスを使用するための設定例

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

この例は、NAT プール、内部スタティック NAT 、およびポートフォワーディングでのダイヤラインターフェイスの設定を示しています。

```
ip nat pool natpool10 203.0.113.1 203.0.113.25 prefix-length 24
ip nat inside source list nat-dia-vpn-hop-access-list interface Dialer100 overload
ip nat inside source list nat-dia-vpn-hop-access-list pool natpool10 overload
egress-interface Dialer100
ip nat inside source static 10.10.80.254 10.1.1.198 vrf 10 egress-interface Dialer100
ip nat inside source static tcp 10.10.80.100 8080 interface Dialer100 8080 vrf 10
ip nat inside source static tcp 10.10.80.253 23 10.1.1.200 8201 vrf 10 egress-interface
Dialer100
```

HSRP による NAT DIA スタティック NAT マッピング

次のセクションでは、HSRP を使用した NAT DIA スタティック NAT マッピングの設定について説明します。

HSRP によるスタティック NAT マッピングについて

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

HSRPは、ファーストホップIPデバイスのフェールオーバーを透過的に実行できるように設計された First-Hop Redundancy Protocol（FHRP）です。デフォルトゲートウェイの IP アドレスが設定されたネットワーク上の IP ホストにファーストホップのルーティング冗長性を確保することによって、ハイアベイラビリティを提供します。HSRP は、ルータグループ内のアクティブデバイスとスタンバイデバイスを識別するために使用されます。

HSRP 設定の詳細については、『*Cisco Catalyst SD-WAN Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x*』の「Hot Standby Router Protocol (HSRP)」の章を参照してください。

ARP でのアドレス解決

Address Resolution Protocol（ARP）は、ホストのハードウェアアドレスをホストの既知の IP アドレスから検出します。このハードウェアアドレスは Media Access Control（MAC）アドレスとも呼ばれます。ARP が保持するキャッシュ（テーブル）では、MAC アドレスが IP アドレスにマッピングされています。

Gratuitous ARP

ホストが自身の IP アドレスを解決するために ARP 要求を送信する場合、それは Gratuitous ARP と呼ばれます。ARP 要求パケットでは、送信元と宛先の IP アドレスは、同じ送信元 IP アドレス自体で満たされています。宛先 MAC アドレスはイーサネット ブロードキャスト アドレスです。

ルータがアクティブになると、影響を受ける LAN セグメントに HSRP 仮想 MAC アドレスを含む Gratuitous ARP パケットをブロードキャストします。セグメントがイーサネットスイッチを使用する場合、スイッチは仮想 MAC アドレスの場所を変更できます。これによりパケットが、アクティブでなくなったルータの代わりにアクティブルータに流れます。ルータがデフォルトの HSRP MAC アドレスを使用する場合、エンドデバイスは、gratuitous ARP を必要としません。

HSRP によるスタティック NAT マッピング

1. NAT スタティックマッピングで設定され、デバイスが所有するアドレスに対して ARP クエリがトリガーされると、NAT はこの HSRP グループに設定された仮想 MAC アドレスで応答します。2 つのデバイスがアクティブおよびスタンバイとして動作します。HSRP グループに属するように、アクティブデバイスとスタンバイデバイスの NAT 内部インターフェイスを設定します。
2. アクティブルータとスタンバイルータの両方が同じスタティック NAT マッピングで設定されている場合、アクティブデバイスだけがスタティック NAT マッピングエントリの ARP 要求に応答します。HSRP アクティブデバイスからスタンバイデバイスにフェールオーバーするトラフィックは、フェールオーバーする前に ARP 要求がタイムアウトするのを待つ必要はありません。
3. 新しい HSRP アクティブデバイスは、ARP 要求がタイムアウトするのを待たずに、スタティック NAT マッピングエントリの所有権を自動的に再開します。HSRP アクティブデバイスは、スタティック NAT マッピングエントリの Gratuitous ARP 要求も送信します。これは、**ip nat outside source static** コマンドにマッピングされている HSRP グループ名を利用して行われます。

HSRP を使用したスタティック NAT マッピングの詳細については、『*IP Addressing: NAT Configuration Guide*』を参照してください。

HSRP によるスタティック NAT マッピングの利点

- トラフィックはフェイルオーバーする前に ARP エントリがタイムアウトするのを待機する必要がないため、冗長性が確保されます

- HSRP アクティブルータのみが、NAT アドレスで設定されたルータへの着信 ARP 要求に応答します。

HSRP によるスタティック NAT マッピングの制約事項

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

- NAT64 および NAT66 は、HSRP を使用したスタティック NAT マッピングではサポートされていません。
- IPv6アドレスはサポートされていません。サポートされているのは IPv4 アドレスだけです。
- サービス側オブジェクトトラッカーは、外部スタティック NAT ではサポートされていません。
- 両方の HSRP ルータ（アクティブとスタンバイ）は、同じグループ名と同じスタティック NAT マッピングを持つ必要があります。

CLI テンプレートを使用した HSRP によるスタティック NAT マッピングの設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

CLI テンプレートの使用の詳細については、CLI テンプレートおよび CLI アドオン機能テンプレートを参照してください。

1. ハイアベイラビリティのために、HSRP グループ名と **redundancy** キーワードを指定した **ip nat outside** を使用して、アクティブおよびスタンバイ HSRP ルータを設定します。

```
interface interface-type-number
 no shutdown
 vrf forwarding vrf-name
 ip address ip-address ip-address
 standby version number
 standby group-number ip ip-address
 standby group-number name hsrp_lan
 standby group-number preempt
 standby group-number priority priority-value
 standby group-number timers msec timer-value timer-value
 negotiation auto
exit
!
ip nat inside source list global interface interface-type-number overload
ip nat outside source static ip-address ip-address vrf vrf-name redundancy hsrp_lan
 match-in-vrf
```

（注） 冗長性キーワードは、`ip nat outside source static` コマンドでのみサポートされています。`ip nat inside source static` コマンドでは、`redundancy` キーワードはサポートされていません。

HSRP アクティブルータとスタンバイルータの両方に、同じ HSRP グループ名と同じスタティック NAT マッピングを設定します。

宛先 NAT の **ip nat outside** コマンドの設定に加えて、送信元 IP を変換するための **ip nat inside** コマンドを設定します。

サービス側からインターネットにパケットを送信すると、NAT DIA は宛先 IP アドレス（プライベート IP アドレスの場合もある）をパブリック IP アドレスに変換します。これは、宛先 NAT と呼ばれます。

2. **ip nat outside** 機能をサポートする一元化されたデータポリシーを構成します。宛先 NAT 宛てのトラフィックは、ポリシーシーケンスに該当しない場合があります。

```
policy
data-policy policy-name
vpn-list vpn_list
sequence number
match
source-ip ip-address
!
action accept
nat use-vpn 0
!
!
sequence number
match
source-ip      ip-address
destination-ip ip-address
!
action accept
nat pool pool-number
!
!
default-action accept
!
!
lists
vpn-list vpn_list
vpn vpn-name
vpn vpn-name
!
!
```

一元化されたポリシーの `nat use-vpn 0` 部分により、宛先 IP が変換された後に、一致するトラフィックが VPN 0 に送信されます。

次に、HSRP を使用してスタティック NAT マッピングを設定するための完全な設定例を示します。

```
!
interface GigabitEthernet1
ip address 209.165.201.96 255.255.255.0
ip nat outside
standby version 2
standby 300 ip 209.165.201.34
standby 300 priority 120
standby 300 preempt
standby 300 name hsrp_wan
!
```

```
interface GigabitEthernet3
vrf forwarding 2
ip address 192.168.0.96 255.255.255.0
standby version 2
standby 500 ip 192.168.0.94
standby 500 priority 120
standby 500 preempt
standby 500 name hsrp_lan
!
!
ip nat inside source list global interface GigabitEthernet1 overload
!
ip nat outside source static 209.165.201.1 192.168.0.1 vrf 2 redundancy hsrp_lan
match-in-vrf
!
```

一元化されたデータポリシーを使用して HSRP でスタティック NAT マッピングを設定するための完全な構成例を次に示します。

```
policy
data-policy test_policy
vpn-list vpn_list
sequence 10
match
source-ip 192.168.0.0/24
!
action accept
nat use-vpn 0
!
!
sequence 20
match
source-ip      192.168.0.0/24
destination-ip 209.195.201.0/32
!
action accept
nat pool 1
!
!
default-action accept
!
!
lists
vpn-list vpn_list
vpn 0
vpn 2
!
!
```

HSRP を使用したスタティック NAT マッピングの確認

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

次のセクションでは、HSRP を使用したスタティック NAT 設定の確認について説明します。

HSRP グループ名に関連付けられた IP アドレスの表示

次に、**show ip nat redundancy** コマンドの出力例を示します。

```
Device# show ip nat redundancy
IP             Redundancy-Name    ID     Use-count
192.168.0.200  hsrp_lan           0      1
```

上記の出力は、HSRP グループ名に関連付けられた IP アドレスを示しています。

Use-count 列の数字は、この IP アドレスを使用するスタティック NAT CLI の数を示します。

HSRP グループ名に関連付けられた IP アドレスを表示するための新しいコマンド **show ip nat redundancy** が追加されました。詳細については、『*Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide*』を参照してください。

変換された IP アドレスの表示

次に、**show ip nat translations** コマンドの出力例を示します。

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  ---                   ---                   192.168.0.200         209.165.201.1

icmp 192.168.0.1:174       192.168.0.1:174       192.168.0.200:174     209.165.201.1:174
icmp 192.0.2.1:174         192.168.0.1:174       209.165.201.1:174     209.165.201.1:174
icmp 192.168.0.1:174       192.168.0.1:174       192.168.0.200:174     209.165.201.1:174
Total number of translations: 4
```

上記の出力は、4 つの変換があることを示しています。

HSRP スタンバイルータの情報の表示

次に、スタンバイルータの情報を表示する **show standby** コマンドの出力例を示します。

```
Device# show standby
GigabitEthernet1 - Group 300 (version 2)
  State is Active
    1 state change, last state change 22:33:42
  Virtual IP address is 209.165.201.1
  Active virtual MAC address is 0000.0c9f.f12c (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f12c (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 1.584 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 120 (configured 120)
  Group name is "hsrp_wan" (cfgd)
  FLAGS: 1/1
GigabitEthernet3 - Group 500 (version 2)
  State is Active
    5 state changes, last state change 00:00:18
  Virtual IP address is 192.168.0.94
  Active virtual MAC address is 0000.0c9f.f1f4 (MAC In Use)
    Local virtual MAC address is 0000.0c9f.f1f4 (v2 default)
  Hello time 3 sec, hold time 10 sec
    Next hello sent in 0.544 secs
  Preemption enabled
  Active router is local
  Standby router is unknown
  Priority 120 (configured 120)
  Group name is "hsrp_lan" (cfgd)
  FLAGS: 1/1
```

仮想 MAC アドレスを使用して ARP テーブルの NAT IP アドレスを表示する

次に、**show arp vrf** コマンドの出力例を示します。

```
Device# show arp vrf 2
Protocol  Address          Age (min)  Hardware Addr    Type   Interface
Internet  192.168.0.1              -   0000.0c9f.f1f4   ARPA   GigabitEthernet3
Internet  192.168.0.10            11  0050.56bc.780b    ARPA   GigabitEthernet3
Internet  192.168.0.11           100   0050.56bc.608e   ARPA   GigabitEthernet3
Internet  192.168.0.14            83   0050.56bc.4748   ARPA   GigabitEthernet3
Internet  192.168.0.94             -   0000.0c9f.f1f4   ARPA   GigabitEthernet3
Internet  192.168.0.96             -   0050.56bc.1378   ARPA   GigabitEthernet3
Internet  192.168.0.98            73   0050.56bc.3967   ARPA   GigabitEthernet3
```

上記の出力は、NAT アドレス 192.168.0.1 が仮想 MAC アドレス 0000.0c9f.f1f4 で ARP テーブルに追加されることを示しています。

NAT DIA を使用したアプリケーションレベルのゲートウェイ

次のセクションでは、NAT DIA を使用したアプリケーション レベル ゲートウェイ（ALG）の設定に関して説明します。

NAT DIA を使用した ALG の使用に関する情報

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

アプリケーション レベル ゲートウェイ（ALG）は、アプリケーション レイヤ ゲートウェイとも呼ばれ、アプリケーションパケットのペイロード内の IP アドレスを変換するアプリケーションです。ALG を使用してアプリケーション層プロトコルを解釈し、ファイアウォールと NAT 変換を実行します。

パケットペイロードにアドレス情報を埋め込むプロトコルは、ALG のサポートを必要とします。次のプロトコルでは、アプリケーションペイロードの NAT 変換に ALG が必要です。

- ドメインネームシステム（DNS）
- ファイル転送プロトコル（FTP）
- Session Initiation Protocol（SIP）

  SIP は、SIP に基づく VoIP ソリューションに NAT を展開する機能を追加します。

Cisco vManage リリース 20.11.1 および Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a 以降、次のプロトコルがサポートされます。

- 簡易ファイル転送プロトコル（TFTP）
- ポイントツーポイント トンネリング プロトコル（PPTP）
- Sun リモートプロシージャコール（SUNRPC）
- Skinny Client Control Protocol（SCCP）
- H.323

（注） ゾーンベースのファイアウォール（ZBFW）がNAT DIAに対して有効になっている場合、NAT ALG 機能は ZBFW と相互運用します。

ALG の詳細については、『*IP* アドレッシング：*NAT* コンフィギュレーション ガイド』を参照してください。

NAT DIA を使用して ALG を使用する利点

- クライアントアプリケーションが、ダイナミック TCP または UDP ポートを使用してサーバーアプリケーションと通信できるようにします。
- NAT DIA で設定された NAT ALG とゾーンベースのファイアウォール（ZBFW）間の相互運用性をサポートします。

NAT DIA を使用した ALG の使用に関する制限事項

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

- サービス側 NAT を使用した ALG はサポートされていません。NAT DIA のみがサポートされています。
- **ip nat outside source** コマンドを使用した ALG の設定はサポートされていません。
- ドメインネームシステム（DNS）ALG では、ペイロードを変更するために、NAT 変換テーブルにスタティックエントリが必要です。NAT 変換テーブルにスタティックエントリがない場合、DNS ALG は機能しません。

  次のコマンドを使用して、NAT 変換テーブルにスタティックエントリを作成します。

  ```
  ip nat inside source static local-ip global-ip vrf vrf-id egress-interface
  interface-type-number
  ```

- **clear ip nat translations** コマンドを実行すると、ALG セッションがクリアされます。NAT による変換を再作成するには、新しい NAT コマンドを実行します。これは予期されている動作です。

CLI テンプレートを使用した NAT DIA での ALG の設定

CLI テンプレートの使用の詳細については、CLI テンプレートおよびCLI アドオン機能テンプレートを参照してください。

1. NAT DIA を設定します。

   詳細については、「NAT DIA の設定」を参照してください。

2. NAT ALG グローバルサポートを有効にします。

   ```
   ip nat service all-algs
   ```

3. 次の例に示すように、アプリケーションプロトコルごとに NAT ALG を有効にします。

```
ip nat service dns tcp
ip nat service dns udp
ip nat service ftp
ip nat service sip tcp port port-number
ip nat service sip udp port port-number
```

（注） Cisco vManage リリース 20.11.1 および Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a 以降、次のプロトコルが NAT ALG でサポートされます。

- TFTP
- PPTP
- SUNRPC
- SCCP
- H.323

ALG を設定するための完全な設定例を次に示します。

```
ip nat service all-algs
ip nat service sip tcp port 5060
ip nat service sip udp port 5060
ip nat service dns tcp
ip nat service dns udp
ip nat service ftp
ip nat service H323
ip nat service ras
ip nat service pptp
ip nat service tftp
ip nat service sunrpc tcp
ip nat service sunrpc udp
ip nat service skinny tcp port xxxx(default 2000)
```

ALG 設定の確認

次のセクションでは、NAT ALG 設定の確認に関する情報を提供します。

ALG 変換を表示

```
show ip nat translations tcp
tcp  10.1.15.15:5062       10.20.24.150:57497    10.1.15.150:21        10.1.15.150:21
tcp  10.1.15.15:5063       10.20.24.150:49732    10.1.15.150:20        10.1.15.150:20
```

（注） CLIテンプレートを使用してペイロードの翻訳を表示することはできません。ペイロードの変換を表示するには、Cisco SD-WAN Manager を使用してパケットをキャプチャします。

Cisco SD-WAN Manager を使用したパケットのキャプチャの詳細については、『*Cisco Catalyst SD-WAN Monitor and Maintain Guide*』の「パケットのキャプチャ」を参照してください。

NAT ALG による NAT タイムアウトとプロトコルリッスンの確認

```
Device(config)# show platform hardware qfp active feature nat datapath summary
Nat setting mode: sdwan-default
Number of pools configured: none
Timeouts: 86400(tcp), 300(udp), 60(icmp), 300(dns),
          60(syn), 300(finrst), 86400(pptp), 3600(rmap-entry)
pool watermark: not configured
Nat active mapping inside:1 outside:0 static:0 static network:0
Nat debug: none
Nat synchronization: enabled
Nat bpa: not configured; pap: not configured
Nat gatekeeper: on
Nat limit configured: no
Vpns configured with match-in-vrf: no
Nat packet drop: true
Total active translations: 615 (0 static, 615 dynamic, 615 extended)
Platform specific maximum translations: 131072 configured: none
PAM table non-zero entries:
 0 0xeaa88be0 port=53, proto=6, appl_type=12
 12 0xeaa88c60 port=2000, proto=6, appl_type=8
 25 0xeaa88ba0 port=21, proto=6, appl_type=11
 34 0xeaa88c20 port=5060, proto=6, appl_type=9
 35 0xeaa889e0 port=496, proto=17, appl_type=16
 85 0xeaa88ce0 port=5060, proto=17, appl_type=9
 119 0xeaa88ca0 port=53, proto=17, appl_type=12
```

NAT DIA を使用したポートフォワーディング

次のセクションでは、NAT DIA を使用したポートフォワーディングの設定について説明します。

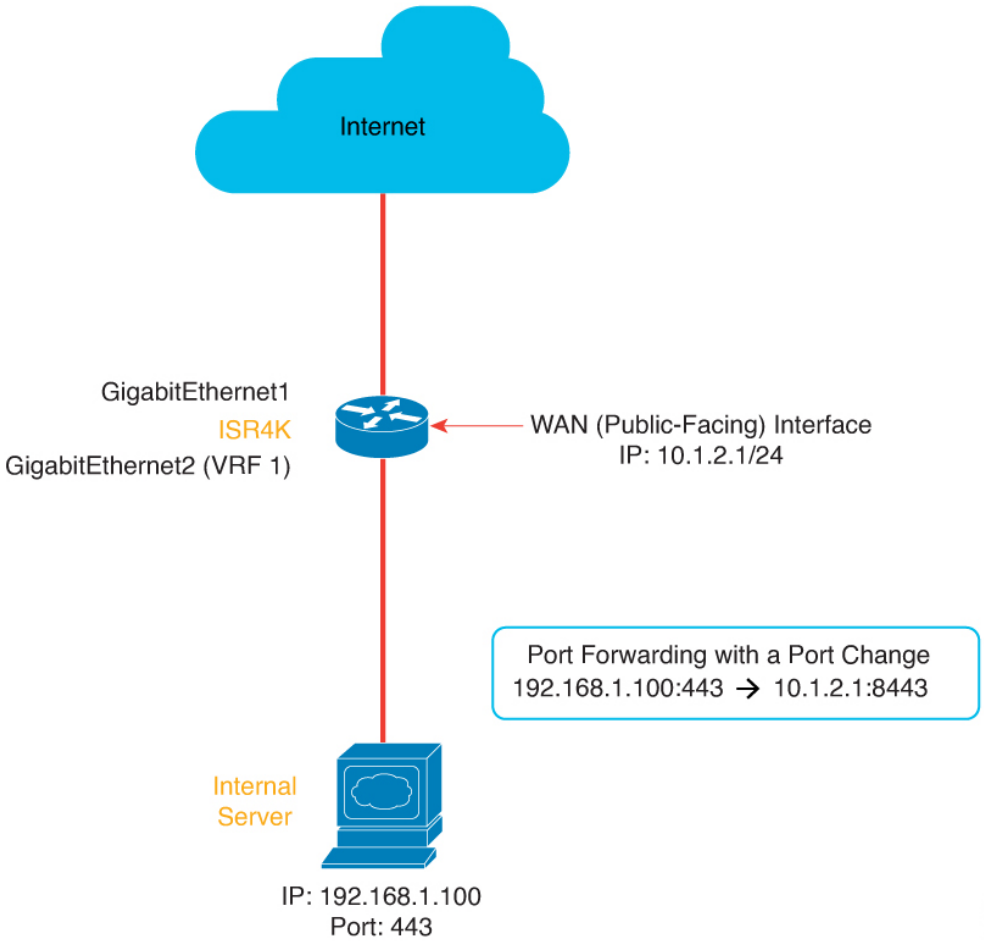
NAT DIA を使用したポートフォワーディングに関する情報

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

NAT DIA を使用したポートフォワーディングは、プライベートネットワーク内でサーバーを実行するユーザーに、パブリック IP アドレスと、内部のローカル IP アドレスとポート番号にマップされるポート番号を共有する機能を提供します。この機能では、各ポートをそれぞれ異なる内部 IP アドレスに転送できるため、同じパブリック IP アドレスから複数のサーバーへのアクセスが可能になります。

Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a および Cisco vManage リリース 20.9.1 以前は、ポートフォワーディングはサービス側の NAT で利用可能でした。

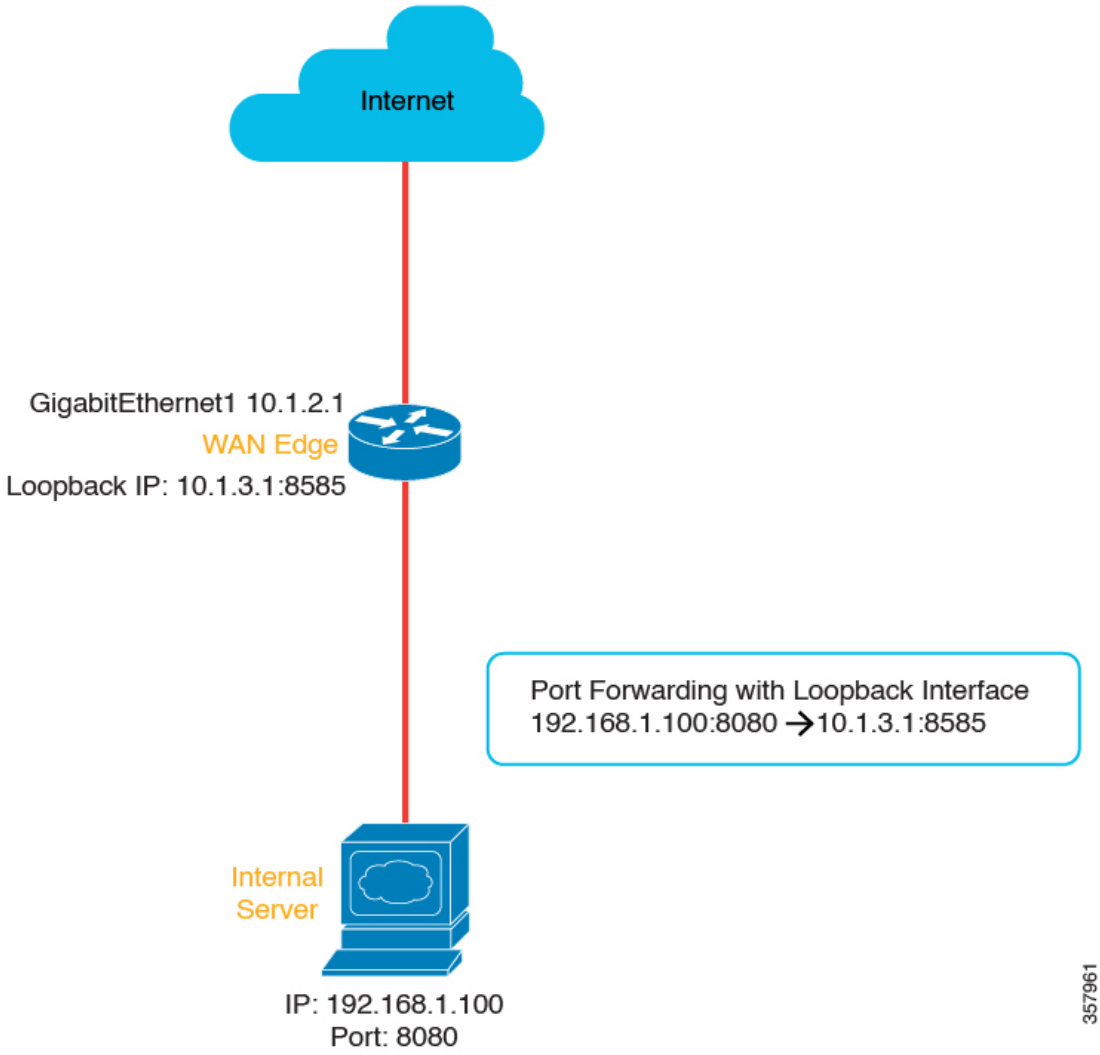
図 *4 :* ポート変更を伴う *NAT DIA* ポートフォワーディング



Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a 以降のリリースでは、NAT DIA を使用したポートフォワーディング用のループバック インターフェイスを設定できます。ループバック インターフェイスは、IP ルーティングプロトコルがループバック インターフェイスに割り当てられたサブネットのアドバタイズを継続する場合、インターフェイスに割り当てられた IP アドレスがいつでも到達可能になるようにします。ループバック インターフェイスとポート番号が設定されると、送信元 IP アドレスと送信元ポート番号がそれぞれループバック IP アドレスとポート番号に変換されます。

Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a から、デバイス CLI テンプレートまたは CLI アドオン機能テンプレートを使用して、ループバック インターフェイスを設定できます。ループバック インターフェイスの設定の詳細については、「*Configure Port Forwarding with NAT DIA Using a CLI Template*」を参照してください。

図 *5* : ループバック インターフェイスを使用した *NAT DIA* ポートフォワーディング



NAT DIA を使用したポートフォワーディングの利点

- パブリックドメインからプライベートネットワーク（LAN）内のサーバーにアクセスできます。
- 異なるポートを異なる内部 IP アドレスに転送できるため、同じパブリック IP アドレスから複数のサーバーにアクセスできます。

NAT DIA を使用したポートフォワーディングの制限事項

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

- NAT DIA を使用したポートフォワーディングでは、TCP ロードバランシングはサポートされていません。
- トラフィックは、パブリックネットワークからのみパブリック IP アドレスとポートに到達できます。
- スタティック NAT を設定している場合、ポートフォワーディングを設定するときに同じスタティック NAT IP アドレスを使用できません。
- NAT DIA でポートフォワーディングを設定するときに、Cisco SD-WAN Manager で予約されたポートは使用できません。
- Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a 以前のリリースでは、ループバック インターフェイスはサポートされていません。

  Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a では、NAT DIA を使用したポートフォワーディングにループバック インターフェイスを設定できます。ループバック インターフェイスの設定の詳細については、「CLI テンプレートを使用した NAT DIA によるポートフォワーディングの設定」を参照してください。
- ダイヤラ仮想インターフェイスはサポートされていません。
- UDP ポート 8000 ～ 48199 は、VoIP トラフィック用に予約されています。Cisco IOS XE Catalyst SD-WAN デバイス で VoIP が有効になっている場合、NAT DIA は、VoIP トラフィック用に予約されているのと同じ UDP ポートを使用できません。
- TLOC 出力インターフェイスの NAT DIA ポートフォワーディングは、ネットワークの外部から送信されたフラグメント化されたパケットをサポートしていません。
- 最大 128 のポート転送ルールを定義して、外部ネットワークからの要求が内部ネットワーク上のデバイスに到達できるようにします。
- IP アドレスとポート番号から IP アドレスとポート番号への変換は、Cisco SD-WAN Manager 機能テンプレートと CLI テンプレートを使用してサポートされています。
- インターフェイス ポート フォワーディングは、CLI テンプレートのみを使用してサポートされます。

  ポート フォワーディング ルールで IP アドレスではなくインターフェイスを使用する場合、これはインターフェイス ポート フォワーディングと呼ばれます。

NAT DIA を使用したポートフォワーディングの設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

パブリック ドメインからプライベートネットワークへのアクセスを許可するポート転送ルールを作成します。

Before You Begin

1. データポリシーを構成して適用します。

2. [Cisco VPN Interface Ethernet] テンプレートを設定するか、既存の [Cisco VPN Interface Ethernet] テンプレートを編集します。
3. インターフェイス オーバーロード モードを設定します。インターフェイス オーバーロード モードはデフォルトで有効になっています。
4. NAT プールを設定します。

NAT DIA を使用したポートフォワーディングの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Cisco VPN Interface Ethernet] テンプレートを編集するには、テンプレート名の横にある [...] をクリックし、[Edit] を選択します。
4. [NAT] をクリックします。
5. [NAT Pool] で、[New NAT Pool] をクリックします。
6. 必須 NAT パラメータを入力します。

   NAT プールパラメータの詳細については、「NAT プールとループバック インターフェイスの設定」を参照してください。
7. [Add] をクリックします。
8. ポート フォワーディング ルールを作成するには、**[Port Forward]** > **[New Port Forwarding Rule]**をクリックし、表の説明に従ってパラメータを設定します。

表 *5 : NAT DIA* のポートフォワーディングのパラメータ

パラメータ名	説明
Protocol	ポート フォワーディング ルールを適用する [TCP] または [UDP] を選択します。TCP トラフィックと UDP トラフィックの両方で同じポートを一致させるには、2 つのルールを構成します。
送信元 IP アドレス	変換される送信元アドレスを入力します。
送信元ポート	ポート番号を入力して、変換する送信元ポートを定義します。 範囲は 0 ～ 65535 です。

パラメータ名	説明
[Translated Source IP Address]	OMP にアドバタイズされる NAT IP アドレスを指定します。ポートフォワーディングは、変換されたポートが一致するオーバーレイから、この IP アドレス宛てのトラフィックに適用されます。
[Translate Port]	ポートフォワーディングを適用するポート番号を入力します。 範囲は 0 ～ 65535 です。 Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a で始まる、スタティックに変換された送信元 IP アドレスは、設定されたダイナミック NAT プールの IP アドレス範囲内にある必要があります。
[Static NAT Direction]	ネットワークアドレス変換を行う方向を選択します。
[Source VPN ID]	トラフィックの送信元のサービス側 VPN を指定します。

9. [更新（Update）] をクリックします。

CLI テンプレートを使用した NAT DIA によるポートフォワーディングの設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

CLI テンプレートの使用の詳細については、CLI テンプレートおよび CLI アドオン機能テンプレートを参照してください。

1. WAN インターフェイスで **ip nat outside** を設定します。

```
interface interface-type-number
 ip address dhcp
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid
end
```

2. WAN インターフェイスでインターフェイス過負荷モードを設定します。

```
ip nat inside source list nat-acl interface interface-type-number overload
```

3. 出力インターフェイスを使用して NAT DIA ポートフォワーディングを設定します。

```
ip nat inside source static tcp ip-address port ip-address port vrf number
egress-interface interface-type-number
ip nat inside source static tcp ip-address port interface interface-type-number port
 vrf number
```

`ip nat inside source static tcp ip-address port interface interface-type-number port vrf number` コマンドは、ポート フォワーディング ルールで IP アドレスではなくインターフェイスを使用するため、インターフェイス ポート フォワーディングの例です。

（注） Cisco SD-WAN Manager 機能テンプレートを使用してインターフェイス ポート フォワーディングを設定できます。

NAT DIA を使用したポートフォワーディングを設定するための完全な設定例を次に示します。

```
interface GigabitEthernet1
 ip address 10.1.2.1 255.255.255.0
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid
end

ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload
ip nat inside source static tcp 192.168.1.100 443 interface GigabitEthernet1 8443 vrf 1
ip nat inside source static tcp 192.168.1.100 80 10.1.2.10 80 vrf 1 egress-interface
GigabitEthernet1
ip nat inside source static tcp 192.168.1.100 22 10.1.2.20 2020 vrf 1 egress-interface
GigabitEthernet1
```

ループバック インターフェイスを使用した NAT DIA によるポートフォワーディング

Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a から、NAT DIA を使用したポートフォワーディングにループバック インターフェイスを設定できます。ループバック インターフェイスを設定するときに、インターネット側インターフェイスである出力インターフェイスを指定します。

ループバック インターフェイスを使用して、NAT DIA によってポートフォワーディングを設定するための設定例を次に示します。

WAN インターフェイスで **ip nat outside** を設定します。

```
interface GigabitEthernet1
 ip address 10.1.2.1 255.255.255.0
 ip nat outside
 negotiation auto
 no mop enabled
 no mop sysid
exit
```

ループバック インターフェイスを定義します。

```
interface Loopback3
 ip address 10.1.3.1 255.255.255.255
exit
```

ループバック インターフェイスを設定します。

```
ip nat inside source static tcp 192.168.1.100 8080 interface Loopback3 8585 vrf 1
egress-interface GigabitEthernet1
ip nat inside source static tcp 192.168.1.100 80 interface Loopback3 5050 egress-interface
 GigabitEthernet1
```

上記の設定例では、送信元 IP アドレスが 192.168.1.100 の着信 TCP パケットが、Loopback3 に割り当てられた IP アドレス 10.1.3.1 に変換されます。送信元ポート 8080 は 8585 に変換されます。

1 ～ 512 の範囲で VRF 番号を指定すると、サービス VPN 内でポートフォワーディングが行われます。VRF 番号の値を指定しない場合、ポートフォワーディングはトランスポート VPN（デフォルトでは VPN 0）で設定されます。

ループバック インターフェイスは、インターフェイス コンフィギュレーション モードで **shutdown** コマンドを実行するまでアクティブなままです。

NAT DIA を使用したポートフォワーディングの設定の確認

NAT DIA を使用したポートフォワーディングの変換の確認

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a、Cisco vManage リリース 20.9.1

次に、**show ip nat translations** コマンドの出力例を示します。

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  10.0.1.7:2022         10.0.100.14:22        ---                   ---
tcp  10.0.1.7:2022         10.0.100.14:22        10.0.1.16:46275       10.0.1.16:46275
Total number of translations: 2
```

上記の出力では、ポート 2022 の内部グローバル IP 10.0.1.7 が、ポート 22 の内部ローカル IP 10.0.100.14 に変換されます。

ループバック インターフェイスを使用したポートフォワーディングの変換の確認

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco vManage リリース 20.11.1

次に、**show ip nat translations** コマンドの出力例を示します。

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  10.1.3.1:5050         192.168.1.100:80        ---                   ---
tcp  10.1.3.1:8585         192.168.1.100:8080      ---                   ---
Total number of translations: 2
```

上記の出力では、ポート 8080 の送信元 IP 192.168.1.100 は、ポート 8585 のループバック IP 10.1.3.1 に変換されます。

NAT 高速ロギング

次のセクションでは、NAT Direct Internet Access（DIA）を使用したネットワークアドレス変換（NAT）および高速ロギング（HSL）の設定に関する情報を提供します。

NAT HSL に関する情報

サポートされる最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.9.1a Cisco IOS XE Release 17.6.4 以降の 17.6.x リリース

NAT HSL を使用すると、Virtual Route Forwarding（VRF）インスタンスの NAT 高速ログを有効または無効にすることができます。HSL が設定されている場合、NAT はルーティング デバ

イス（バージョン 9 の NetFlow に似た記録と同様）を通じて外部コレクタに流れるパケットのログを提供します。外部コレクタにエクスポートされる NAT 変換には、サービス側 VRF からグローバル DIA への変換、およびサービス内 VRF（サービス側 VRF NAT）変換を含めることができます。セッションが作成および削除されると、バインディングごとにレコードが生成されます（バインディングは、ローカルアドレスと、ローカルアドレスが変換されるグローバルアドレスをバインドするアドレスです）。

NAT の HSL 情報を表示するためにコレクタをオンにすることができます。必要な場合にのみ HSL をオンにでき、それに応じて HSL ログレコードが作成され、コレクタに送信されます。これにより、必要のないときに HSL ログレコードを作成および送信しないことで、CPU サイクルと帯域幅が節約されます。

NAT HSL の利点

- 外部コレクタへの NAT 操作のフローモニターレコードの送信をサポートします。
- 必要な場合にのみ HSL レコードの作成と送信を有効にし、CPU サイクルと帯域幅を節約します。
- NAT プールのアドレスが不足すると（プールの枯渇とも呼ばれます）、HSL メッセージを自動的に送信します。

NAT 高速ロギング（HSL）の制限事項

- サービス側 NAT VRF は IPv6 アドレスをサポートしていません。
- サービス側 VRF での IPv6 ターゲットのエクスポートはサポートされていません。
- VRF での IPv6 を使用した変換のエクスポートはサポートされていません。

NAT HSL の前提条件

- NAT 変換がルータで使用できることを確認します。
- ログメッセージが生成されていることを確認します。

NAT HSL のベストプラクティス

- ロギング用に設定された IP アドレスとポートアドレスがコレクタの設定に従っていることを確認します。
- **show interface statistics** コマンドを使用して、出力パケットカウンタを確認し、コレクタに接続しているルータインターフェイスからのパケットの流れを確認します。

CLI テンプレートを使用した NAT HSL の設定

CLI テンプレートの使用の詳細については、CLI アドオン機能テンプレートおよび CLI テンプレートを参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

次に、フローエクスポータを使用して NAT による変換の高速ロギングを有効にする CLI 設定例を示します。

ip nat log translations flow-export v9 udp destination *IPv4address-port* **source** *interface-name interface-number*

次に、特定の宛先および送信元インターフェイスの変換ロギングを有効にする設定例を示します。

```
ip nat log translations flow-export v9 udp destination 10.10.0.1 1020 source
gigabithethernet 0/0/1
```

NAT HSL 設定の確認

次に、**show ip nat translations** コマンドの出力例を示します。エクスポート ターゲット コレクタで変換ログを表示できます。

```
Device# show ip nat translations
Pro  Inside global      Inside local          Outside local         Outside global
---------------------------------------------------------------------------------------
tcp  10.0.0.16:5092     10.0.0.16:56991       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5078     10.0.0.16:55951       172.16.128.7:80       172.16.128.7:80
tcp  10.0.0.16:5070     10.0.0.16:57141       172.16.128.7:80       172.16.128.7:80
tcp  10.0.0.16:5089     10.0.0.16:55823       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5103     10.0.0.16:58717       172.16.128.7:80       172.16.128.7:80
tcp  10.0.0.16:5064     10.0.0.16:55413       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5091     10.0.0.16:59331       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5100     10.0.0.16:59795       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5097     10.0.0.16:57695       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5096     10.0.0.16:55665       209.165.202.129:80    209.165.202.129:80
tcp  10.0.0.16:5066     10.0.0.16:58671       172.16.128.7:80       172.16.128.7:80
```

以下は、設定を確認するために使用される **show platform hardware qfp active feature nat datapath hsl** コマンドからの出力例です。

```
Device# show platform hardware qfp active feature nat datapath hsl
HSL cfg dip 10.10.0.1 dport 1020 sip 10.21.0.16 sport 53738 vrf 0
nat hsl handle 0x3d007d template id 261 pool_exh template id 263
LOG_TRANS_ADD 132148
LOG_TRANS_DEL 132120
LOG_POOL_EXH 0
```

次に、**show vrf detail** コマンドの出力例を示します。

```
Device# show vrf detail
VRF 1 (VRF Id = 1); default RD <not set>; default VPNID <not set>
  New CLI format, supports multiple address-families
  Flags: 0x1808
  Interfaces:
    Gi0/0/1      Gi0/0/2.102      Lo0    Vl103
Address family ipv4 unicast (Table ID = 0x1):
  Flags: 0x0
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
```

```
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
Address family ipv6 unicast (Table ID = 0x1E000001):
  Flags: 0x0
  No Export VPN route-target communities
  No Import VPN route-target communities
  No import route-map
  No global export route-map
  No export route-map
  VRF label distribution protocol: not configured
  VRF label allocation mode: per-prefix
Address family ipv4 multicast not active
Address family ipv6 multicast not active
```

既知の Cisco Catalyst SD-WAN ポートの送信元ポートの保持

次のセクションでは、既知の Cisco Catalyst SD-WAN ポートについて説明します。

既知の Cisco Catalyst SD-WAN ポートの送信元ポート保持に関する情報

Cisco Catalyst SD-WAN 展開では、12346 ～ 12445 の範囲の UDP ポート番号と 23456 ～ 24356 の範囲の TCP ポートを使用して、Cisco IOS XE Catalyst SD-WAN デバイス の接続を制御します。外部 Cisco IOS XE Catalyst SD-WAN デバイス が NAT 時にファイアウォールの背後にある場合、制御トラフィックポートが別のポートに変換される可能性があります。これは通常問題ではありませんが、BFD セッションがダウンすると、NAT は新しい BFD 制御パケットを別のポートに変換します。ファイアウォールは、新しく変換されたポートを受け入れず、古い BFD セッションの変換されたポートを保存しているため、BFD パケットがドロップされます。

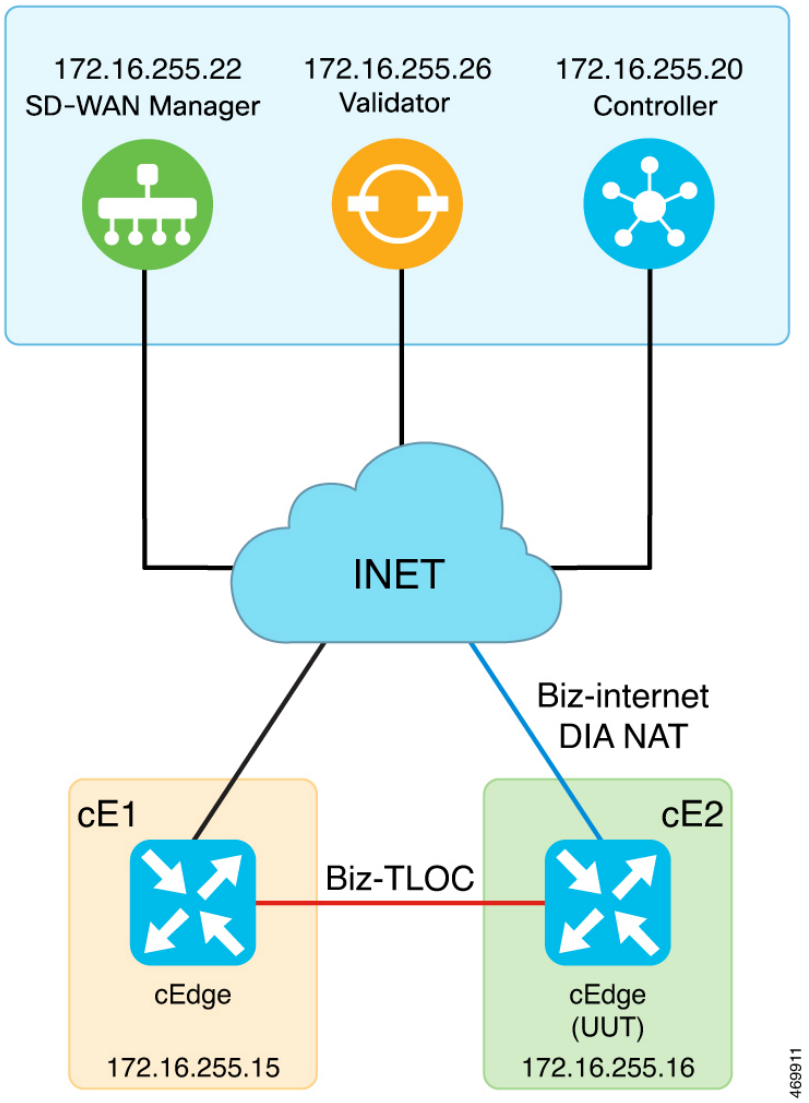
この機能を使用すると、NAT 時に既知の Cisco Catalyst SD-WAN ポートの送信元ポートを保持するように Cisco IOS XE Catalyst SD-WAN デバイス を設定できます。制御トラフィック用に予約されたポートのセットがあり、この範囲内でポートは NAT 時に保持されます。この機能を有効にすると、Cisco IOS XE Catalyst SD-WAN デバイス は既知の SD-WAN ポート範囲の送信元ポートを保持します。そのため、ファイアウォールは NAT の背後にある Cisco Catalyst SD-WAN デバイスを処理できます。

（注） サービス側のトラフィックがこれらのポート範囲を使用していないことを確認してください。そうしないと、制御接続が失敗します。

次の NAT マッピング条件では、この機能を有効にすると、Cisco Catalyst SD-WAN の既知のポートを使用して制御トラフィックの送信元ポート保持が可能になります。

- インターフェイスの過負荷
- ループバックの過負荷

図 *6 : Cisco Catalyst SD-WAN* 展開における送信元ポート保持のトポロジ



トポロジは、デュアルルータサイトを表しています。cE1 には、コントローラに到達するための INET 接続に cE2 を使用するように設定された tloc-extension があります。パケットが cE2 に到達すると、cE1 は既知の Cisco Catalyst SD-WAN ポート 12346 を使用します。cE2 の NAT 機能は、この送信元ポート番号 12346 を保持し、パケットを送信する前に変更しません。

送信元ポート保持の機能

- 予約ポート範囲内の指定されたポートのトラフィックは、**ip nat settings preserve-sdwan-ports** コマンドの設定後に同じポートに変換されます。
- ローカルで生成されたトラフィックは NAT を通過しないため、常に予約されたポート範囲でポートが保持されます。ローカルデバイスと外部デバイスが予約済みポート範囲内の同じポートを使用している場合、ローカルトラフィックが優先されます。

- UDP の予約済みポートの範囲は 12346 ～ 12426 で、TCP の予約済みポートの範囲は 23456 ～ 24356 です。
- TLS（TCP）制御接続では、1024 を超えるポート値を使用できます。送信元ポートの保持は、TCP の予約済みポート範囲 23456 ～ 24356 でのみサポートされるため、他のポート値は変換後に保持されない場合があります。

送信元ポート保持の前提条件

既存の NAT マッピング設定がある場合は、**ip nat settings preserve-sdwan-ports** コマンドを設定した後にデバイスを再起動して、所定の動作を実現します。設定がない場合は、**ip nat settings preserve-sdwan-ports** コマンドを設定した後に NAT マッピング設定を追加します。

送信元ポートの保持に関する制限事項

- サービス側のトラフィックは、予約済みのポート範囲を使用できません。
- Cisco Catalyst SD-WAN の既知のポートがすでにフローに割り当てられ、別のフローが同じポートの変換を要求した場合、新しいフローのパケットはドロップされます。
- 既存の NAT マッピング設定がある場合は、**ip nat settings preserve-sdwan-ports** コマンドを実行した後にデバイスを再起動して、所定の動作を実現します。設定がない場合は、**ip nat settings preserve-sdwan-ports** コマンドを実行した後に NAT マッピング設定を追加します。

CLI テンプレートを使用した DIA インターフェイス オーバーロードの送信元ポート保持の設定

CLI テンプレートの使用の詳細については、CLI アドオン機能テンプレートおよび CLI テンプレートを参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

このセクションでは、NAT 時に既知の Cisco Catalyst SD-WAN ポートの送信元ポート保持を設定するための CLI 設定例を示します。

1. NAT 時に送信元ポート保持を有効にします。

```
ip nat settings preserve-sdwan-ports
```

2. DIA インターフェイス オーバーロードの内部送信元アドレスの NAT を有効にします。

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1
overload
```

3. インターフェイスタイプを設定して、インターフェイス コンフィギュレーション モードを開始します。

```
interface GigabitEthernet1
```

4. インターフェイスを有効化します。

```
no shutdown
```

5. IP アドレスを設定します。

```
ip address 10.1.16.16 255.255.255.0
```

6. 外部ネットワークにインターフェイスを接続します。

```
ip nat outside
```

DIA インターフェイス オーバーロード時のポート保持の完全な設定例を次に示します。

```
ip nat settings preserve-sdwan-ports
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload
!
interface GigabitEthernet1
 no shutdown
 ip address 10.1.16.16 255.255.255.0
 ip nat outside
```

CLI テンプレートを使用した DIA プールオーバーロードの送信元ポート保持の設定

CLI テンプレートの使用の詳細については、CLI アドオン機能テンプレートおよび CLI テンプレートを参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

このセクションでは、NAT 時に既知の Cisco Catalyst SD-WAN ポートの送信元ポート保持を設定するための CLI 設定例を示します。

1. NAT 時に送信元ポート保持を有効にします。

```
ip nat settings preserve-sdwan-ports
```

2. NAT の IP アドレスプールを定義します。

```
ip nat pool natpool-GigabitEthernet1-0 10.1.16.201 10.1.16.250 prefix-length 24
```

3. DIA プールオーバーロードの内部送信元アドレスの NAT を有効にします。

```
ip nat inside source list global-list pool natpool-GigabitEthernet1-0 overload
egress-interface GigabitEthernet1
```

4. インターフェイスタイプを設定して、インターフェイス コンフィギュレーション モードに入ります。

```
interface GigabitEthernet1
```

5. インターフェイスを有効化します。

```
no shutdown
```

6. IP アドレスを設定します。

```
ip address 10.1.16.16 255.255.255.0
```

7. 外部ネットワークにインターフェイスを接続します。

```
ip nat outside
```

DIA プールオーバーロード時のポート保持の完全な設定例を次に示します。

```
ip nat settings preserve-sdwan-ports
ip nat pool natpool-GigabitEthernet1-0 10.1.16.201 10.1.16.250 prefix-length 24
ip nat inside source list global-list pool natpool-GigabitEthernet1-0 overload
egress-interface GigabitEthernet1
!
interface GigabitEthernet1
 no shutdown
 ip address 10.1.16.16 255.255.255.0
 ip nat outside
```

CLI テンプレートを使用した DIA ループバックオーバーロードの送信元ポート保持の設定

CLI テンプレートの使用の詳細については、CLI アドオン機能テンプレートおよび CLI テンプレートを参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

このセクションでは、NAT 時に既知の Cisco Catalyst SD-WAN ポートの送信元ポート保持を設定するための CLI 設定例を示します。

1. NAT 時に送信元ポート保持を有効にします。

```
ip nat settings preserve-sdwan-ports
```

2. DIA ループバックオーバーロードの内部送信元アドレスの NAT を有効にします。

```
ip nat inside source list global-list interface Loopback16 overload egress-interface
 GigabitEthernet1
```

3. ループバック インターフェイスを設定します。

```
interface Loopback16
```

4. ループバック インターフェイスの IP アドレスを設定します。

```
ip address 10.20.16.16 255.255.255.0
```

5. インターフェイスタイプを設定して、インターフェイス コンフィギュレーション モードを開始します。

```
interface GigabitEthernet1
```

6. IP アドレスを設定します。

```
ip address 10.1.16.16 255.255.255.0
```

7. 外部ネットワークにインターフェイスを接続します。

```
ip nat outside
```

DIA ループバックオーバーロード時のポート保持の完全な設定例を次に示します。

```
ip nat settings preserve-sdwan-ports
ip nat inside source list global-list interface Loopback16 overload egress-interface
GigabitEthernet1
!
interface Loopback16
 ip address 10.20.16.16 255.255.255.0
!
interface GigabitEthernet1
 ip address 10.1.16.16 255.255.255.0
 ip nat outside
```

送信元ポートの保存の確認

次に、既知の Cisco Catalyst SD-WAN 送信元ポートでの変換を表示する **show ip nat translations** コマンドの出力例を示します。変換の内部ローカルおよび内部グローバル列を観察し、保持されている送信元ポートを確認します。

```
Device# show ip nat translations
Pro  Inside global          Inside local          Outside local         Outside global
udp  10.1.16.201:12406      10.1.19.15:12406      10.0.5.21:12377       10.0.5.21:12377
udp  10.1.16.201:12406      10.1.19.15:12406      10.0.5.19:12355       10.0.5.19:12355
udp  10.1.16.201:12406      10.1.19.15:12406      10.0.5.11:12367       10.0.5.11:12367
udp  10.1.16.201:12406      10.1.19.15:12406      10.0.12.26:12346      10.0.12.26:12346
udp  10.1.16.201:12406      10.1.19.15:12406      10.1.14.14:12366      10.1.14.14:12366
udp  10.1.16.201:12406      10.1.19.15:12406      10.0.12.20:12356      10.0.12.20:12356
Total number of translations: 6
```

次に、コントロールプレーンのポートを持つトラフィックを表示する **show sdwan bfd sessions table** コマンドの出力例を示します。

```
Device# show sdwan bfd sessions table
                                SRC    DST                    SITE
              DETECT      TX
SRC IP      DST IP      PROTO  PORT   PORT   SYSTEM IP      ID    LOCAL COLOR   COLOR
       STATE  MULTIPLIER  INTERVAL  UPTIME      TRANSITIONS
------------------------------------------------------------------------------------------
10.1.15.15  10.0.5.11   ipsec  12366  12367  172.16.255.11  100   lte           lte
       up     7           1000      0:01:37:43  3
10.1.19.15  10.0.5.11   ipsec  12406  12367  172.16.255.11  100   biz-internet  lte
       up     7           1000      0:00:00:51  0
10.1.15.15  10.1.14.14  ipsec  12366  12366  172.16.255.14  400   lte           lte
       up     7           1000      0:01:37:43  3
10.1.19.15  10.1.14.14  ipsec  12406  12366  172.16.255.14  400   biz-internet  lte
       up     7           1000      0:00:00:51  0
10.1.15.15  10.1.16.16  ipsec  12366  12386  172.16.255.16  600   lte
biz-internet  up     7           1000      0:00:31:41  0
10.1.19.15  10.1.16.16  ipsec  12406  12386  172.16.255.16  600   biz-internet
biz-internet  down   7           1000      NA          0
10.1.15.15  10.0.5.21   ipsec  12366  12377  172.16.255.21  100   lte           lte
       up     7           1000      0:01:37:43  3
10.1.19.15  10.0.5.21   ipsec  12406  12377  172.16.255.21  100   biz-internet  lte
       up     7           1000      0:00:00:51  0
```

宛先 NAT

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco vManage リリース 20.11.1

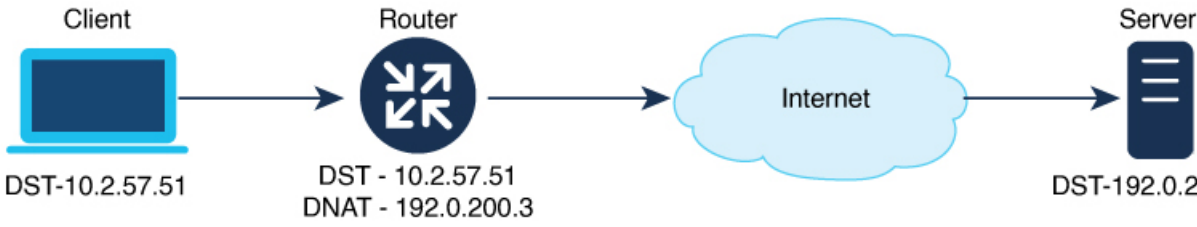
次のセクションでは、NAT ダイレクト インターネット アクセス（DIA）を使用した宛先 NAT の設定について説明します。

宛先 NAT に関する情報

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco vManage リリース 20.11.1

サービス側からインターネットにパケットを送信すると、NAT ダイレクト インターネット アクセス（DIA）は宛先 IP アドレス（プライベート IP アドレスの場合もある）をパブリック IP アドレスに変換します。これは、宛先 NAT と呼ばれます。

2 つのエンドポイント間に配置された WAN エッジデバイスは、宛先 NAT の実行に使用できます。宛先 NAT は、プライベート IP アドレスの宛先を持つ着信パケットをパブリック IP アドレスにリダイレクトするために使用されます。通常、あるホスト上の特定の IP アドレス宛てのパケットを別のホスト上の別のアドレスにリダイレクトするために使用されます。



宛先 NAT の制限事項

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco vManage リリース 20.11.1

- 宛先 NAT では NAT DIA のみがサポートされます。
- 内部から外部方向に発信されるトラフィックのみがサポートされます。
- データポリシーベースの DIA のみがサポートされます。
- ルートベースの DIA 設定はサポートされません。
- NAT DIA でのポートフォワーディングはサポートされません。
- パケットに対する同じ NAT ルールは、別の VRF には適用されません。

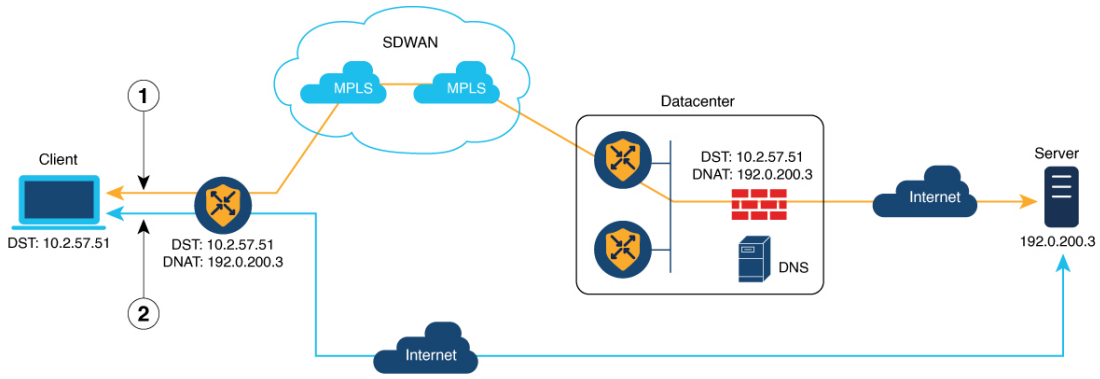
宛先 NAT の使用例

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco vManage リリース 20.11.1

Cisco VPN クライアントを使用するお客様のデバイスは、プライベート IP アドレスが割り当てられている、ファイアウォールサービスを実行しているデバイスへの DNS クエリを開始します。このプライベート IP アドレスは、オーバーレイ IP アドレスです。NAT DIA が設定されていない場合、データポリシーは VPN 0 フォールバックをオーバーレイに使用して、プライベート IP アドレスを持つファイアウォールにトラフィックを送信します。プライベート IP アドレスであるオーバーレイ IP アドレスは、パブリック IP アドレスに変換されます。

トラフィック ルートの優先パスは、送信元と宛先の両方の IP アドレスが変換される NAT DIA が設定されたパスを通過します。

図 7: 宛先 *NAT* の使用例



1	NAT が設定されていないパス	2	NAT が設定されたパス

CLI テンプレートを使用した宛先 NAT の設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco vManage リリース 20.11.1

CLI テンプレートの使用の詳細については、CLI テンプレートおよび CLI アドオン機能テンプレートを参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

外部送信元アドレスの NAT を有効にするには

ip nat outside source static *local-ip-address global-ip-address* **vrf** *vrf-name*

次に、宛先 NAT の完全な設定例を示します。

```
ip nat outside source static 192.0.200.3 10.2.57.51 vrf 1
```

宛先 NAT の確認

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco vManage リリース 20.11.1

次に、**show sdwan policy from-vsmart** コマンドの出力例を示します。

```
Device# show sdwan policy from-vsmart

from-vsmart data-policy _1_vm5-vpn1-dia-policy
 direction all
 vpn-list 1
  sequence 1
   match
    source-ip      10.20.24.0/24
    destination-ip 10.2.57.51/24
   action accept
    nat use-vpn 0
    nat fallback
from-vsmart lists vpn-list 1
 vpn 1
```

この例では、宛先 IP アドレスと、NAT フォールバック機能が設定されているかどうかを確認できます。

次に、**show ip nat translations** コマンドの出力例を示します。

```
Device# show ip nat translations

Pro   Inside global    Inside local    Outside local     Outside global
---   ---              ---             10.2.57.51        192.0.2.1
tcp   203.0.113.1:5062 10.0.0.1:30427  10.2.57.51:1024   192.0.2.1:1024
```

この例では、**outside local** IP アドレスは、**outside global** 内のパブリック IP アドレスに変換されたプライベート IP アドレスを示しています。

宛先 NAT のトラブルシューティング

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco vManage リリース 20.11.1

元の IP アドレスと変換後の IP アドレスを確認するには、**show platform hardware qfp active feature nat datapath bind** コマンドを使用します。

```
Device# show platform hardware qfp active feature nat datapath bind

Bind longest chain 1 avg non-zero bucket len 1 non-zero bkts 2
bind 0xed7739c0 oaddr 8.8.8.8 taddr 4.1.1.5 oport 0 tport 0 vrfid 1 tableid 1 proto 0
domain 1 create time 78840 refcnt 1 mask 0x0 cgn flags 0 timeout 0 ifhandle 0 wlan_info
 0x0 flags 0x2100 mapping 0x0 cp_mapping_id 1 limit_type 0  last_use_ts 82071 mibp 0x0
bind_pool_id: 0 rg 0 nak_retry 0 parent 0x0 egress_ifh 0 in2out_pkts 0 out2in pkts 0
```

トラフィックが DIA インターフェイスを通過しているかどうかを確認するには、**show sdwan policy data-policy-filter** コマンドを使用してパケット数を確認します。

```
Device# show sdwan policy data-policy-filter
                                                    POLICER  OOS      OOS
```

```
NAME  NAME   COUNTER NAME          PACKETS  BYTES  NAME     PACKETS  BYTES
------------------------------------------------------------------------------
u5    vpn-1  DNAT-DIA-COUNTER      5        570
             default_action_count  158      14340
```

DIAインターフェイスがダウンしているときにフォールバックインターフェイスのトラフィックフローを確認するには、**show plat hard qfp active feature sdwan datapath statistics | inc fallback** を使用します。

```
Device# show plat hard qfp active feature sdwan datapath statistics | inc fallback

data-policy-in-sig-fallback-flow-set-fail 0
data-policy-in-nat-fallback 0
data-policy-out-nat-fallback 0
```

NAT DIA トラッカー

表 *6:* 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイス の NAT DIA トラッカー	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能を使用すると、システムトラッカーを設定して、定期的にトランスポートインターフェイスをプローブして、インターネットまたは外部ネットワークが使用できなくなったかどうかを判断できます。 [Cisco System] テンプレートの [Tracker] タブを使用して、DIA トラッカーを設定できます。 [Cisco VPN Interface Ethernet] または [Cisco VPN Interface Cellular] テンプレートを使用して、トラッカーをトランスポート インターフェイスに適用できます。

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイスでのインターフェイスステータスの追跡のデュアル エンドポイント サポート	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能により、Cisco SD-WAN Manager システムテンプレートを使用してデュアルエンドポイントでトラッカーグループを設定し、各トラッカーグループをインターフェイスに関連付けることができます。アクティブなインターネット接続があるにもかかわらず、シングルエンドポイントが非アクティブになる場合があります。この条件は、偽陰性につながります。シングル エンドポイント トラッカーのこの欠点を克服するために、デュアル エンドポイント トラッカー設定を使用できます。
IPv6 インターフェイスの NAT DIA トラッカー	Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a Cisco vManage リリース 20.11.1	NAT DIA トラッカーが IPv6 インターフェイスでサポートされるようになりました。 設定グループのトランスポートプロファイルで [IPv6-Tracker] および [IPv6-Tracker Group] オプションを使用して、IPv6 DIA トラッカーを設定できます。

機能名	リリース情報	説明
IPv4 または IPv6 インターフェイスの NAT DIA 用 ICMP エンドポイントトラッカー	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a Cisco Catalyst SD-WAN Manager リリース 20.13.1	この機能を使用すると、DIA パスを介した ICMP エンドポイントトラッカーを設定できます。IPv4 または IPv6 エンドポイントで NAT DIA の ICMP プローブを設定できます。 設定グループのトランスポートプロファイルで [Tracker] または [IPv6 Tracker] 機能を使用して、ICMP トラッカーを設定できます。 [Basic] 機能プロファイルで [Tracker DIA Stabilize Status] 設定を構成して、インターフェイスフラップの原因となるトラッカーステータスの急速な変化を安定させます。

NAT DIA トラッキングに関する情報

DIA トラッカーは、インターネットまたは外部ネットワークが使用できなくなったかどうかを判断するのに役立ちます。NAT DIA トラッキング機能は、VPN 0 のトランスポート インターフェイスで NAT が有効になっている場合に役立ち、ルーターからのデータトラフィックが直接インターネットに送信されるようにします。

NAT DIA の詳細については、「NAT ダイレクト インターネット アクセス」を参照してください。

インターネットまたは外部ネットワークが使用できなくなった場合、ルータはサービス VPN の NAT ルートに基づいてトラフィックを転送し続けます。インターネットに転送されるトラフィックはドロップされます。インターネット バウンド トラフィックがドロップされないようにするには、エッジルータで DIA トラッカーを設定して、トランスポート インターフェイスのステータスをトラッキングします。トラッカーは定期的にインターフェイスをプローブして、インターネットのステータスを判断し、トラッカーに関連付けられている接続ポイントにデータを返します。

トランスポート インターフェイスでトラッカーが設定されている場合、インターフェイスの IP アドレスは、プローブパケットの送信元 IP アドレスとして使用されます。

IP SLA は、プローブのステータスをモニタリングし、これらのプローブパケットの往復時間を測定し、その値をプローブで設定された遅延と比較します。遅延が設定されたしきい値を超えると、トラッカーはネットワークを使用不可と見なします。

トラッカーがローカルインターネットが利用できないと判断した場合、ルータはサービス VPN から NAT ルートを取り消し、ローカルルーティング設定に基づいてトラフィックをオーバーレイに再ルーティングします。

ローカルルータは、インターフェイスへのパスのステータスを定期的にチェックし続けます。パスが再び機能していることを検出すると、ルータはインターネットへの NAT ルートを再インストールします。

Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a から、2 つのトラッカーを持つトラッカーグループを設定し、このトラッカーグループをインターフェイスに関連付けることができます。2 つのトラッカー（2 つのエンドポイント) を持つトラッカーグループをプローブすると、内部または外部ネットワークが誤って使用不可としてマークされた場合に発生する可能性のある誤検知を回避するのに役立ちます。

Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a から、IPv6 インターフェイスで NAT DIA トラッカーを設定できます。トラッカーおよびトラッカーグループのアドレスタイプは、インターフェイス設定の IPv4 または IPv6 アドレスタイプと一致している必要があります。たとえば、IPv4 アドレスが NAT DIA インターフェイスで設定されている場合、IPv4 トラッカーのみを適用できます。IPv6 アドレスが NAT DIA インターフェイスで設定されている場合は、IPv6 トラッカーのみを適用できます。IPv4 と IPv6 の両方のアドレスが NAT DIA インターフェイスで設定されている場合、設定に応じて IPv4 と IPv6 の両方のトラッカーを適用できます。

NAT DIA 用 ICMP エンドポイントトラッカー

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a から、NAT DIA に使用される NAT 対応の IPV4 または IPv6 トランスポート インターフェイスで ICMP エンドポイントトラッカーを設定できます。ICMP トラッカーは、設定された外部エンドポイントにプローブを送信することで、特定の外部サービスへのインターネットパスに沿って障害を検出し、プローブが失敗するか成功するかをモニターします。プローブの数が設定された乗数値を超えた場合、または ICMP プローブが設定されたしきい値を超えた場合、トラッカーは外部エンドポイントを到達不能と見なし、トランスポート インターフェイスを DIA で使用不可にします。

ICMP プローブは、トランスポートインターフェイスが DIA で使用できなくなった場合のフェールオーバーを短縮します。ICMP エンドポイントトラッカーのエンドポイント IP またはエンドポイント DNS 名を設定できます。複数の IPv4 または IPv6 トラッカーを設定している場合は、トラッカーグループを作成できます。

警告 ICMP トラッカーを設定した DIA インターフェイスを介して出力するようにホストルートを設定していることを確認します。これにより、目的のトラッカーインターフェイスが ICMP プローブを受信するようになります。エンドポイントが ICMP トラッカー用に設定されたインターフェイス以外のインターフェイスを介して到達可能である場合、ICMP プローブがトラッキングされていないインターフェイスに送信され、ICMP プローブが意図しないインターフェイスを介して出力される可能性があります。

NAT DIA 用の次のタイプの ICMP エンドポイントトラッカーを設定できます。

表 *7: ICMP* エンドポイントトラッカーのタイプ

トラッカー	サポートされるトラッカータイプ
単一の NAT DIA ICMP トラッカー	トラッカータイプ： • IPv4 • IPv6 トラッカーエンドポイントのタイプ： • エンドポイント IP • DNS
NAT DIA ICMP トラッカーグループ	トラッカータイプ： • IPv4 • IPv6 トラッカーエンドポイントのタイプ： • エンドポイント IP
NAT DIA 混合トラッカーグループ（HTTP および ICMP）	トラッカータイプ： • IPv4 • IPv6 トラッカーエンドポイントのタイプ： • エンドポイント IP

ICMP トラッカーでサポートされるデバイス

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a、Cisco Catalyst SD-WAN Manager リリース 20.13.1

ICMP トラッカーの制限事項

- 機能テンプレートを使用して ICMP エンドポイント トラッカー タイプを設定することはできません。
- 同じトラッカーグループに IPv4 と IP6 の両方のトラッカータイプを設定することはできません。
- 次のインターフェイスのみに NAT DIA の ICMP エンドポイントトラッカーを設定できます。
  - イーサネット インターフェイス

- イーサネット (PPPoE) インターフェイス
- サブインターフェイス

- 1 つの DIA インターフェイス（デフォルトルート）のみが設定されている場合、ICMP トラッカーがダウンすると、デフォルトルートが取り消されます。

NAT DIA トラッカーでサポートされるインターフェイス

次のインターフェイスに NAT DIA トラッカーを設定できます。

- セルラーインターフェイス
- イーサネット インターフェイス
- イーサネット (PPPoE) インターフェイス
- サブインターフェイス
- DSL ダイヤラインターフェイス（PPPoE および PPPoA）

（注） IPv6 NAT DIA トラッカーは、イーサネット インターフェイスの物理インターフェイスとサブインターフェイスでのみサポートされます。

NAT DIA トラッカーの制限事項

Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a 以前のリリースの制限事項

- Cisco IOS XE Release 17.6.x 以前では、ダイヤラインターフェイスで NAT DIA トラッカーがサポートされていません。Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a から、サブインターフェイスとダイヤラインターフェイスは、シングル エンドポイント トラッカーおよびデュアル エンドポイント トラッカーをサポートします。
- Cisco IOS XE Catalyst SD-WAN デバイス では、DNS URL エンドポイントはサポートされていません。
- 1 つのインターフェイスに適用できるトラッカーまたはトラッカー グループは 1 つだけです。
- NAT フォールバック機能は、Cisco IOS XE Catalyst SD-WAN リリース 17.3.2 からのみサポートされています。
- アドレス 169.254.xx のトンネルの IP アドレスは、手動トンネルで zScaler エンドポイントをトラッキングするためにサポートされていません。
- トラッカーグループを設定するには、少なくとも 2 つのシングル エンドポイント トラッカーを設定する必要があります。

- トラッカーグループには、最大 2 つのシングル エンドポイント トラッカーのみを組み込むことができます。
- Cisco IOS XE リリース 17.10.1 以前のリリースでは、IPv6 インターフェイスに IPv4 トラッカーを設定できません。その逆も同様です。トラッカーはアクティブになりません。

Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a の制約事項

- API URL エンドポイントは、IPv6 DIA トラッカーでのみサポートされ、IPv4 DIA トラッカーではサポートされません。
- IPv4 と IPv6 の両方のトラッカーを同じトラッカーグループで使用することはできません。
- IPv6 トラッカーが TLOC トンネルインターフェイスと連携するようにするには、TLOC トンネルインターフェイスで **allow service all** コマンドを設定する必要があります。
- 複数の NAT66 DIA インターフェイスはサポートされていません。
- 一元管理型データポリシーの NAT フォールバックはサポートされていません。

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a の制約事項

- エンドポイント DNS 要素は、トラッカーグループではサポートされていません。

IPv4 インターフェイスでの NAT DIA トラッカーのワークフロー

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1

1. [Cisco System] テンプレートを使用してインターフェイストラッカーを設定します。Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a から、デュアルトラッカーまたはトラッカーグループを設定できます。トラッカーの設定の詳細については、「トラッカーの設定」を参照してください。
2. トラッカーをトランスポート インターフェイスに適用します。NAT DIA トラッカーの設定の詳細については、「NAT DIA トラッカーの設定」を参照してください。
3. NAT DIA トラッカーの設定を確認します。NAT DIA トラッカーの設定のモニタリングの詳細については、「NAT DIA トラッカーの設定のモニタリング」を参照してください。

Cisco SD-WAN Manager の IPv4 インターフェイスでの NAT DIA トラッカーの設定

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1

[Cisco System] テンプレートを使用して、トランスポート インターフェイスのステータスをトラッキングします。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. 変更する [Cisco System] テンプレートの隣にある […] をクリックし、[Edit] を選択します。
4. [Tracker] をクリックし、 [New Endpoint Tracker] をクリックしてトラッカーパラメータを設定します。

表 *8*：トラッカーパラメータ

パラメータフィールド	説明
名前（**Name**）	トラッカーの名前。名前には 128 文字以内の英数字を使用できます。最大 8 つのトラッカーを設定できます。
しきい値	トランスポート インターフェイスがダウンしていると宣言する前に、プローブが応答を返すのを待機する時間。範囲： 100 ー 1000 ミリ秒デフォルト： 300 ミリ秒
インターバル（**Interval**）	トランスポート インターフェイスのステータスを判別するためにプローブが送信される頻度。範囲：20ー600秒。デフォルト：60 秒（1 秒）
Multiplier（乗数）	トランスポート インターフェイスがダウンしていることを宣言する前にプローブを再送信できる回数。範囲：1 ～ 10。デフォルト：3
[Tracker Type]	[Interface] を選択して、DIA トラッカーを設定します。
[End Point Type: IP Address]	エンドポイントの IP アドレス。これは、ルーターがプローブを送信してトランスポート インターフェイスのステータスを判断するインターネット内の宛先です。IP アドレスが HTTP ポート 80 プローブに応答できるようになっていることを確認します。
[End Point Type: DNS Name]	エンドポイントの DNS 名。これは、ルーターがプローブを送信してトランスポート インターフェイスのステータスを判断するインターネット内の宛先です。

5. [Add] をクリックします。

6. トラッカーグループを作成してパラメータを設定するには、**[Tracker Groups]** > **[New Endpoint Tracker Group]**をクリックします。

表 *9:* トラッカー グループ パラメータ

パラメータ フィールド	説明
[Tracker Type: Tracker Elements]	このフィールドは、[Tracker Group] として [Tracker Type] を選択した場合にのみ表示されます。既存のインターフェイストラッカー名（スペースで区切る）を追加します。このトラッカーをテンプレートに追加すると、トラッカーグループがこれらの個々のトラッカーに関連付けられ、そのトラッカーグループをインターフェイスに関連付けることができます。
[Tracker Type: Tracker Boolean]	このフィールドは、[Tracker Group] として [Tracker Type] を選択した場合にのみ表示されます。[AND] または [OR] を選択します。 [OR] はデフォルトのブール演算です。[OR] は、トラッカーグループの関連付けられたトラッカーのいずれかがインターフェイスがアクティブであると報告した場合に、トランスポート インターフェイス ステータスがアクティブとして報告されることを保証します。 [AND] 操作を選択した場合、トラッカーグループの関連付けられたトラッカーの両方がインターフェイスがアクティブであると報告した場合、トランスポート インターフェイス ステータスはアクティブであると報告されます。

（注） トラッカーグループを設定する前に、2つのシングルエンドポイントトラッカーを設定したことを確認してください。

7. [Add] をクリックします。
8. [Advanced] をクリックして、[Track Interface] 情報を入力します。

   インターネットに接続するトランスポートインターフェイスのステータスをトラッキングするトラッカーの名前を入力します。

（注） インターフェイスステータスのトラッキングは、VPN 0 のトランスポートインターフェイスで NAT を有効にして、最初にデータセンターのルータにアクセスするのではなく、ルータからのデータトラフィックが直接インターネットに出られるようにする場合に役立ちます。この状況では、トランスポート インターフェイスで NAT を有効にすると、ローカルルータとデータセンター間の TLOC が 2 つに分割され、1 つはリモートルータに、もう 1 つはインターネットに送られます。トランスポート トンネル トラッキングを有効にすると、ソフトウェアはインターネットへのパスを定期的に調べて、インターネットが稼働しているかどうかを判断します。このパスがダウンしていることをソフトウェアが検出すると、インターネットの宛先へのルートが撤回され、インターネットに向かうトラフィックはデータセンターのルータを介してルーティングされます。インターネットへのパスが再び機能していることをソフトウェアが検出すると、インターネットへのルートが再インストールされます。

（注） テンプレートを更新する前に、すべての必須フィールドへの入力が完了していることを確認してください。

9. [更新（Update）] をクリックします。

NAT DIA トラッカーの設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco Catalyst SD-WAN 制御コンポーネントリリース 20.7.1。

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a から、NAT DIA に ICMP トラッカーを設定できます。

Cisco SD-WAN Manager の設定グループを使用した IPv4 インターフェイスでの NAT DIA トラッカーの設定

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a および Cisco vManage リリース 20.11.1

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]** を選択します。

   Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a 以前では、**[Configuration]** > **[Templates]** > **[Configuration Groups]** の順に選択します。

   設定グループの作成の詳細については、「設定グループワークフロー」を参照してください。

2. 設定グループに機能を追加します。

   機能の追加の詳細については、「Feature Management」を参照してください。

3. [Transport and Management Profile] で、[Tracker] と [Tracker Group] を設定します。

   IPv4 インターフェイスでのトラッカーの設定の詳細については、「Tracker and tracker group on an IPv4 interface」を参照してください。また、「Tracker Group」を参照してください。

4. [Transport and Management Profile] で、VPN 0 機能のインターフェイスの横にある [...] をクリックします。

   - [Associate Sub Feature] を選択した場合は、必要に応じて事前設定された [Tracker] および [Tracker Group] のチェックボックスをオンにします。
   - [Add Sub Feature] を選択した場合は、ドロップダウンリストから [Tracker] および [Tracker Group] を選択し、ステップ 3 の設定手順に従います。

   VPN 0 設定の詳細については、「Ethernet Interface」を参照してください。

5. 設定グループを作成したら、グループにデバイスを追加します。詳細については、「Add Devices to a Configuration Group」を参照してください。これで、設定グループに関連付けられているデバイスを展開できます。詳細については、「デバイス設定の展開」を参照してください。

CLI を使用した IPv4 インターフェイスでの NAT DIA トラッカーの設定

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1

CLI を使用した NAT DIA トラッカーの設定（シングルエンドポイント）

CLI アドオン機能テンプレートまたは CLI デバイステンプレートを使用して、NAT DIA トラッキングを設定できます。CLI テンプレートを使用した構成の詳細については、「CLI テンプレート」を参照してください。

```
Device# config-transaction
Device(config)# endpoint-tracker tracker1
Device(config-endpoint-tracker)# endpoint-ip ip-address
Device(config-endpoint-tracker)# threshold value
Device(config-endpoint-tracker)# multiplier value
Device(config-endpoint-tracker)# interval value
Device(config-endpoint-tracker)# tracker-type interface
```

トラッカーグループの設定

Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a から NAT DIA トラッカーをプローブするトラッカーグループを作成できます。

```
Device# config-transaction
Device(config)# endpoint-tracker tracker-name1
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-ip ip-address
Device(config-endpoint-tracker)# threshold value
Device(config-endpoint-tracker)# multiplier value
Device(config-endpoint-tracker)# interval value

Device# config-transaction
Device(config)# endpoint-tracker tracker-name2
```

```
Device(config-endpoint-tracker)# tracker-type interface
Device(config-endpoint-tracker)# endpoint-dns-name <dns-name>
Device(config-endpoint-tracker)# threshold value
Device(config-endpoint-tracker)# multiplier value
Device(config-endpoint-tracker)# interval value

Device(config)# endpoint-tracker tracker-group-name
Device(config-endpoint-tracker)# tracker-type tracker-group
Device(config-endpoint-tracker)# boolean or
Device(config-endpoint-tracker)# tracker-elements tracker-name1 tracker-name2
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# endpoint-tracker tracker-group-name
```

（注） トラッカーグループには、エンドポイントトラッカーを混在させることができます。IP アドレストラッカーと DNS トラッカーを組み合わせて、トラッカーグループを作成できます。

CLI を使用した NAT DIA の ICMP トラッカーの設定

CLI を使用した NAT DIA の ICMP トラッカーの設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a および Cisco Catalyst SD-WAN Manager リリース 20.13.1。

CLI アドオンプロファイルまたは設定グループのトランスポートプロファイルを使用して、NAT DIA の ICMP トラッキングを設定できます。詳細については、「Configuration Groups and Feature Profiles」を参照してください。

単一のエンドポイントを設定するには

```
Device# config-transaction
Device(config)# endpoint-tracker t1
Device(config-endpoint-tracker)# tracker-type interface-icmp
Device(config-endpoint-tracker)# endpoint-ip ip-address
Device(config-endpoint-tracker)# threshold value
Device(config-endpoint-tracker)# multiplier value
Device(config-endpoint-tracker)# icmp-interval value
```

トラッカーグループを設定するには

```
Device# config-transaction
Device(config)# endpoint-tracker tracker-name1
Device(config-endpoint-tracker)# tracker-type interface-icmp
Device(config-endpoint-tracker)# endpoint-ip <ip-address>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# icmp-interval <value>

Device# config-transaction
Device(config)# endpoint-tracker <tracker-name2>
Device(config-endpoint-tracker)# tracker-type interface-icmp
Device(config-endpoint-tracker)# endpoint-dns-name <dns-name>
Device(config-endpoint-tracker)# threshold <value>
Device(config-endpoint-tracker)# multiplier <value>
Device(config-endpoint-tracker)# icmp-interval <value>

Device(config)# endpoint-tracker tracker-group-name
Device(config-endpoint-tracker)# tracker-type tracker-group
Device(config-endpoint-tracker)# boolean or
Device(config-endpoint-tracker)# tracker-elements tracker-name1 tracker-name2
```

```
Device(config)# interface GigabitEthernet0/0/1
Device(config-if)# endpoint-tracker tracker-group-name
```

次の例は、エンドポイントIPアドレスを使用してトラッカーを設定する方法を示しています。

```
Device(config)# endpoint-tracker tracker1
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# interval 2
Device(config-endpoint-tracker)# tracker-type interface
```

次の例は、エンドポイントを DNS としてトラッカーを設定する方法を示しています。

```
Device(config)# endpoint-tracker tracker2
Device(config-endpoint-tracker)# endpoint-dns-name www.example.com
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# interval 2
```

次の例は、エンドポイント IP アドレスを使用して ICMP トラッカーを設定する方法を示しています。

```
Device(config)# endpoint-tracker tracker3
Device(config-endpoint-tracker)# tracker-type interface-icmp
Device(config-endpoint-tracker)# endpoint-ip 10.1.1.1
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# icmp-interval 2
```

次の例は、エンドポイントを DNS として使用して ICMP トラッカーを設定する方法を示しています。

```
Device(config)# endpoint-tracker tracker4
Device(config-endpoint-tracker)# tracker-type interface-icmp
Device(config-endpoint-tracker)# endpoint-dns-name www.example.com
Device(config-endpoint-tracker)# threshold 100
Device(config-endpoint-tracker)# multiplier 5
Device(config-endpoint-tracker)# icmp-interval 2
```

CLI を使用した IPv4 インターフェイスでの NAT DIA トラッキングの設定例

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1

次のセクションでは、CLI を使用して NAT DIA トラッカーを設定する例を示します。

設定例：CLI を使用したシングルエンドポイント NAT DIA トラッカー

次の例は、シングルエンドポイント NAT DIA トラッカーを設定する方法を示しています。

```
config-transaction
    endpoint-tracker tracker1
    tracker-type interface
    endpoint-ip 10.1.1.1
    threshold 100
    multiplier 5
    interval 20
exit
```

設定例：トラッカーグループ

この例は、2 つのトラッカー（2 つのエンドポイント）を持つトラッカーグループを設定する方法を示しています。Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a からインターフェイスをプローブするトラッカーグループを作成できます。

```
config-transaction
    endpoint-tracker tracker1
    endpoint-ip 10.1.1.1
    interval 20
    threshold 100
    multiplier 1
    tracker-type interface
exit

endpoint-tracker tracker2
    endpoint-dns-name www.cisco.com
    interval 600
    threshold 1000
    multiplier 10
    tracker-type interface
exit

endpoint-tracker group1
    tracker-type tracker-group
    boolean or
    tracker-elements tracker1 tracker2
exit
```

次の例は、トラッカーグループをインターフェイスに適用し、サポートされているインターフェイスで設定する方法を示しています。

```
interface GigabitEthernet0/0/1
    endpoint-tracker group1
```

NAT DIA トラッカーステータスの安定化

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a から、[Tracker DIA Stabilize Status] というグローバル構成設定を、Cisco SD-WAN Manager の [Basic] 機能プロファイルを使用して行います。または、CLI を使用して **dia-stabilize-status** コマンドを使用できます。この設定は、HTTP と ICMP の両方の DIA インターフェイス全体でのすべてのエンドポイントトラッカーの状態変化に適用され、トラッカーの状態を安定させ、急速なステータス変更によるインターフェイスの急速なフラップを回避します。

インターフェイスにエンドポイントトラッカーを設定すると、トラッカーは HTTP または ICMP プローブを送信してそのエンドポイントのトラッキングを開始します。エンドポイントが到達可能である場合、またはプローブが成功した場合、トラッカーは UP とマークされます。エンドポイントに到達できない場合、またはプローブが失敗した場合、トラッカーは DOWN とマークされます。トラッカーステータスの継続的な変更を回避するために、一定数のプローブを送信後にのみトラッカーステータスが変更されるように、乗数が適用されます。

この乗数では、エンドポイントがダウンしていることを宣言する前にプローブを送信できる回数を指定します。指定できる範囲は 1 ～ 10 です。デフォルトは 3 です。乗数は、設定された値に基づいてトラッカーを繰り返しプローブするために使用され、乗数の設定に達した後でもプローブが成功する場合は、トラッカーを UP とマークします。たとえば、乗数が 3 に設定さ

れている場合、プローブが 3 回連続して成功すると、トラッカーのステータスが UP に変わります。

設定された乗数または再試行値は、プローブがトラッカーオブジェクトを正常に起動し、NAT に通知するために適用されます。トラッカーの状態が UP の場合、NAT はルートをインストールします。これにより、再試行によってトラッカーオブジェクトがアップ状態であることが担保されるため、インターフェイスのフラップが回避されます。Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a より前だと、HTTP プローブの場合、トラッカーは乗数によって設定された回数のプローブの後に DOWN とマークされます。トラッカーは、最初のプローブが成功した後に UP とマークされます。このメカニズムにより、ネットワークフラップが発生します。**dia-stabilize-status** コマンドは、値「乗数 + 1」を使用してトラッカーのステータスを変更することで、この動作を安定させます。たとえば、乗数の値が 3 の場合、ステータスが DOWN のトラッカーは 3+1 回（ICMP 間隔に基づいて 2 秒間隔で）ping されます。4 番目のプローブが成功すると、トラッカーは UP とマークされます。

Cisco IOS XE Catalyst SD-WAN リリース 17.12.x 以前では、乗数は SIG トラッカー（UP から DOWN および DOWN から UP）および HTTP トラッカー（UP から DOWN）に使用されていました。Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a 以降では、**dia-stabilize-status** 設定が ICMP および HTTP トラッカーに適用され、DOWN から UP へのステータス遷移がトラッキングされます。

CLI を使用した設定

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a および Cisco Catalyst SD-WAN Manager リリース 20.13.1

次の例は、CLI を使用して、この機能を設定する方法を示しています。

```
device(config)# endpoint-tracker-settings dia-stabilize-status
```

Cisco Catalyst SD-WAN Manager を使用した設定

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a および Cisco Catalyst SD-WAN Manager リリース 20.13.1

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]** を選択します。

   設定グループの作成の詳細については、「設定グループワークフロー」を参照してください。

2. 設定グループに機能を追加します。

   機能の追加の詳細については、「Feature Management」を参照してください。

3. [System Profile] で、[Basic] 機能を設定します。

   [Basic] 機能の設定の詳細については、「Basic」を参照してください。

4. [Track Settings] をクリックします。

5. [Tracker DIA Stabilize Status] で、ドロップダウンリストから [Global] を選択し、設定を有効にします。

6. [Save] をクリックします。

IPv4 インターフェイスでの NAT DIA トラッカー設定のモニタリング

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1

インターフェイス DIA トラッカーの表示

トランスポート インターフェイスで DIA トラッカーに関する情報を表示するには、次の手順を実行します。

1. Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Devices]**の順に選択します。

   Cisco vManage リリース 20.6.x 以前：Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Network]**の順に選択します。

2. デバイスのリストからデバイスを選択します。
3. [Real Time] をクリックします。
4. シングルエンドポイント トラッカーの場合、[Device Options] ドロップダウンリストから、[Endpoint Tracker Info] を選択します。
5. デュアルエンドポイント トラッカーの場合、[Device Options] ドロップダウンリストから、[Endpoint Tracker Group Info] を選択します。

IPv4 インターフェイスでの NAT DIA トラッカーの設定の確認

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a および Cisco vManage リリース 20.7.1

テンプレートをデバイスに接続した後、コマンド構文を確認できます。次の設定例は、NAT DIA トラッカーのトラッカー定義と、トラッカーをトランスポート インターフェイスに適用する方法を示しています。

```
endpoint-tracker tracker-t1
  threshold 1000
  multiplier 3
  interval 20
  endpoint-ip 10.1.16.13
  tracker-type interface

interface GigabitEthernet1
 no shutdown
 endpoint-tracker tracker-t1
 ip nat outside
```

次の設定例は、設定がコミットされているかどうかを確認する方法を示しています。

```
Device# show endpoint-tracker interface GigabitEthernet1

Interface          Record Name          Status        RTT in msecs    Probe ID
Next Hop
```

```
GigabitEthernet1   tracker-t1              UP              2               1
10.1.16.13
```

次の設定例は、トラッカーに関するタイマー関連の情報を示しており、トラッカー関連の問題があった場合デバッグするのに役立ちます。

```
Device# show endpoint-tracker records
Record Name            Endpoint       EndPoint Type   Threshold    Multiplier   Interval
     Tracker-Type
p1                      10.1.16.13          IP              300          3          60
       interface
```

ICMP トラッカーの設定の確認

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a から、ICMP トラッカーの設定後にコマンド構文を確認できます。次の設定例は、NAT DIA トラッカーの ICMP トラッカー定義と、トラッカーをトランスポート インターフェイスに適用する方法を示しています。

```
endpoint-tracker tracker-t2
  tracker-type interface-icmp
  endpoint-ip 10.1.16.13
  threshold 1000
  multiplier 3
  icmp-interval 2


interface GigabitEthernet1
 no shutdown
 endpoint-tracker tracker-t2
```

次の設定例は、設定がコミットされているかどうかを確認する方法を示しています。

```
Device# show endpoint-tracker interface GigabitEthernet1

Interface          Record Name          Status        RTT in msecs    Probe ID
Next Hop
GigabitEthernet1   tracker-t2              UP              2               1
10.1.16.13
```

デュアルトラッカーの Show コマンド

次に、**show endpoint-tracker tracker-group** コマンドの出力例を示します。

```
Device# show endpoint-tracker tracker-group
Tracker Name               Element trackers name       Status      RTT in msec    Probe
 ID
interface-tracker-group     tracker1, tracker2      UP(UP OR UP)      1,1          53,
54
```

```
Device# show ip sla summary

IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds

ID           Type        Destination       Stats       Return Code     Last Run

*9           dns         10.1.1.1           RTT=3       OK          12 seconds ago
*10          http        10.1.1.10 .        RTT=89      OK          23 seconds ago
```

```
Device# show endpoint-tracker records
Record Name            Endpoint       EndPoint Type   Threshold    Multiplier   Interval
```

```
     Tracker-Type
group1          tracker1 OR tracker2       N/A            N/A          N/A          N/A
      tracker-group
group3          tracker3 OR tracker4       N/A            N/A          N/A          N/A
      tracker-group
tracker1             198.168.20.2          IP             300          3             60
        interface
tracker2             198.168.20.3          IP             300          3             60
        interface
tracker3         www.cisco.com.com      DNS_NAME         300          3             60
        interface
tracker4         www.cisco.com.com      DNS_NAME         300          3             60
        interface
```

次に、**show ip sla summary** コマンドの出力例を示します。

```
Device# show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds
ID            Type       Destination      Stats   Return Code       Last Run
*53           http         10.1.1.1       RTT=2        OK        35 seconds ago
*54           http         10.1.1.10      RTT=2        OK        1 minute, 35 seconds
ago
```

次に、ICMP エンドポイントトラッカーに対する **show endpoint-tracker tracker-group** コマンドの出力例を示します。

```
Device# show endpoint-tracker tracker-group
Tracker Name     Element trackers name     Address Family    Status            RTT in
msec      Probe ID
trackergroup1    tracker1, tracker2        IPv4              UP(UP OR UP)      1, 2
         5, 4
```

次に、ICMP エンドポイントトラッカーに対する **show ip sla summary** コマンドの出力例を示します。

```
Device# show ip sla summary
IPSLAs Latest Operation Summary
Codes: * active, ^ inactive, ~ pending
All Stats are in milliseconds. Stats with u are in microseconds
ID            Type       Destination      Stats   Return Code       Last Run
*4           icmp-echo    10.1.29.99      RTT=1        OK        1 seconds ago
```

IPv6 インターフェイスでの NAT DIA トラッカーのワークフロー

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a および Cisco vManage リリース 20.11.1

Cisco SD-WAN Manager の設定グループを使用した IPv6 インターフェイスでの NAT DIA トラッカーの設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco vManage リリース 20.11.1

（注） 設定グループ、デバイス CLI テンプレート、または CLI アドオン機能テンプレートを使用して、IPv6 DIA トラッカー機能を設定できます。この機能は、機能テンプレートを使用して設定することはできません。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]** を選択します。

   Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a 以前では、**[Configuration]** > **[Templates]** > **[Configuration Groups]** の順に選択します。

   設定グループの作成の詳細については、「設定グループワークフロー」を参照してください。

2. 設定グループに機能を追加します。

   機能の追加の詳細については、「Feature Management」を参照してください。

3. [Transport and Management Profile] で、[IPv6-Tracker] と [IPv6-Tracker Group] を設定します。

   IPv6 トラッカーの設定の詳細については、「IPv6 Tracker and IPv6 tracker group」を参照してください。また、「IPv6 Tracker Group」を参照してください。

4. [Transport and Management Profile] で、VPN 0 機能の横にある [...] をクリックし、[Associate Sub Feature] を選択します。

   - [Associate Sub Feature] を選択した場合は、必要に応じて、事前設定された [IPv6-Tracker] および [IPv6-Tracker Group] のチェックボックスをオンにします。
   - [Add Sub Feature] を選択した場合は、ドロップダウンリストから [IPv6-Tracker] および [IPv6-Tracker Group] を選択し、ステップ 3 の設定手順に従います。

   VPN 0 設定の詳細については、「Ethernet Interface」を参照してください。

5. 設定グループを作成したら、グループにデバイスを追加します。詳細については、「Add Devices to a Configuration Group」を参照してください。これで、設定グループに関連付けられているデバイスを展開できます。詳細については、「デバイス設定の展開」を参照してください。

CLI テンプレートを使用した IPv6 インターフェイスでの NAT DIA トラッカーの設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco vManage リリース 20.11.1

CLI テンプレートの使用の詳細については、CLI アドオン機能テンプレートおよび CLI テンプレートを参照してください。

（注） CLI テンプレートを使用して ICMP トラッカーを設定することはできません。

IPv6 エンドポイントトラッカーの設定

1. エンドポイントのステータスをトラッキングするためのエンドポイントトラッカーを設定します。

   endpoint-tracker *tracker-name*

2. トラッカーのトラッカータイプを設定します。

   tracker-type *ipv6-interface*

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a から、*ipv6-interface-icmp* を使用して NAT DIA の ICMP トラッキングを設定できます。

3. エンドポイントの IPv6 アドレスを設定します。

   ipv6-endpoint *ipv6-address*

（注） IPv4 トラッカーと IPv6 トラッカーを同じトラッカーグループに設定することはできません。

IPv6 エンドポイントトラッカーを設定するための完全な設定例を次に示します。

```
endpoint-tracker t1
   tracker-type ipv6-interface
   ipv6-endpoint 2001:DB8:1::1
```

IPv6 エンドポイント ICMP トラッカーを設定するための完全な設定例を次に示します。

```
endpoint-tracker t1
   tracker-type ipv6-interface-icmp
   ipv6-endpoint 2001:DB8:1::1
```

DNS トラッカーの設定

1. エンドポイントのステータスをトラッキングするためのエンドポイントトラッカーを設定します。

   endpoint-tracker *tracker-name*

2. トラッカーのトラッカータイプを設定します。

   tracker-type *ipv6-interface*

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a から、*ipv6-interface-icmp* を使用して NAT DIA の ICMP トラッキングを設定できます。

3. エンドポイントのドメイン名を設定します。

endpoint-dns-name *dns-name*

DNS トラッカーを設定するための完全な設定例を次に示します。

```
endpoint-tracker dns_t1
   tracker-type ipv6-interface
   endpoint-dns-name cisco.com
```

次に、DNS ICMP トラッカーを設定するための完全な設定例を示します。

```
endpoint-tracker dns_t1
   tracker-type ipv6-interface-icmp
   endpoint-dns-name cisco.com
```

IPv6 トラッカーグループの設定

1. HTTP または ICMP IPv6 エンドポイントトラッカーを設定します。
2. IPv6 インターフェイスで HTTP または ICMP DNS トラッカーを設定します。
3. エンドポイントのステータスをトラッキングするためのエンドポイントトラッカーを設定します。

   endpoint-tracker *tracker-group-name*
4. トラッカーのトラッカータイプを設定します。

   tracker-type *tracker-group*

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a から、*ipv6-interface-icmp* を使用して NAT DIA の ICMP トラッキングを設定できます。

5. トラッカーグループの設定時に Boolen ロジックを有効にします

   boolean{**and** | **or**}
6. トラッカー名を追加して、デュアル エンドポイント トラッカー グループを作成します。

   tracker-elements *tracker1 tracker2*

IPv6 トラッカーグループを設定するための完全な設定例を次に示します。

```
endpoint-tracker t1
   tracker-type ipv6-interface
   ipv6-endpoint 2001:DB8:1::1
!
endpoint-tracker t2
   tracker-type ipv6-interface
   endpoint-dns-name cisco.com
!
endpoint-tracker groupv6
   tracker-type tracker-group
   boolean or
   tracker-elements t1 t2
```

次に、IPv6 ICMP トラッカーグループを設定するための完全な設定例を示します。

```
endpoint-tracker t3
   tracker-type ipv6-interface-icmp
   ipv6-endpoint 2001:DB8:1::1
!
endpoint-tracker t4
   tracker-type ipv6-interface-icmp
   endpoint-dns-name cisco.com
!
endpoint-tracker groupv7
   tracker-type tracker-group
   boolean or
   tracker-elements t3 t4
```

同じインターフェイスでの IPv4 と IPv6 の両方のトラッカーの設定

1. IPv4 エンドポイントトラッカーを設定します。

```
endpoint-tracker t1
   tracker-type interface-ip
   endpoint-ip 10.1.1.1
```

2. IPv4 インターフェイスで DNS トラッカーを設定します。

```
endpoint-tracker t2
   tracker-type interface-ip
   endpoint-dns-name example.com
```

3. IPv6 エンドポイントトラッカーを設定します。

```
endpoint-tracker t3
   tracker-type ipv6-interface
   ipv6-endpoint 2001:DB8:1::1
```

4. IPv6 インターフェイスで DNS トラッカーを設定します。

```
endpoint-tracker t4
   tracker-type ipv6-interface
   endpoint-dns-name cisco.com
```

5. IPv4 トラッカーをトラッカーグループに追加します。

```
endpoint-tracker groupv4
   tracker-type tracker-group
   boolean and
   tracker-elements t1 t2
```

6. IPv6 トラッカーをトラッカーグループに追加します。

```
endpoint-tracker groupv6
   tracker-type tracker-group
   boolean or
   tracker-elements t3 t4
```

7. インターフェイスにトラッカーグループを適用します。

```
interface GigabitEthernet1
 endpoint-tracker groupv4
 ipv6-endpoint-tracker groupv4
```

次に、同じインターフェイスで IPv4 と IPv6 の両方のトラッカーを設定する完全な設定例を示します。

```
endpoint-tracker t1
   tracker-type interface-ip
   endpoint-ip 10.1.1.1
!
endpoint-tracker t2
   tracker-type interface-ip
   endpoint-dns-name example.com
!
endpoint-tracker t3
   tracker-type ipv6-interface
   ipv6-endpoint 2001:DB8:1::1
!
endpoint-tracker t4
   tracker-type ipv6-interface
   endpoint-dns-name cisco.com
!
endpoint-tracker groupv4
   tracker-type tracker-group
   boolean and
   tracker-elements t1 t2
!
endpoint-tracker groupv6
   tracker-type tracker-group
   boolean or
   tracker-elements t3 t4
```

トラッカーグループの HTTP および ICMP トラッカーの設定

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a から、Cisco Catalyst SD-WAN デバイスで HTTP IPv4 トラッカーと ICMP IPv6 トラッカー（またはその逆）を設定します。

1. HTTP IPv4 エンドポイントトラッカーを設定します。

```
endpoint-tracker t1
   tracker-type interface
   endpoint-ip 10.1.1.1
```

2. ICMP IPv4 エンドポイントトラッカーを設定します。

```
endpoint-tracker t2
   tracker-type ipv6-interface-icmp
   endpoint-ip 10.1.1.2
```

3. HTTP および ICMP エンドポイントトラッカーを使用してトラッカーグループを設定します。

```
endpoint-tracker t3
   tracker-type tracker-group
   tracker-elements t1 t2
```

4. インターフェイスにトラッカーグループを適用します。

```
interface GigabitEthernet1
    endpoint-tracker t3
```

サポートされている IPv6 インターフェイスへの定義済み IPv6 トラッカーまたはトラッカー グループの適用

1. インターフェイスタイプを設定して、インターフェイス コンフィギュレーション モードを開始します。

```
interface GigabitEthernet1
```

2. 事前定義された IPv6 エンドポイントトラッカー名を適用します。

   ipv6-endpoint-tracker *tracker-name*

次に、トラッカーをインターフェイスに適用し、サポートされているインターフェイスで設定する完全な設定例を示します。

```
interface GigabitEthernet1
    ipv6-endpoint-tracker t1
```

IPv6 インターフェイスでの NAT DIA トラッカーの設定の確認

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.11.1a、Cisco vManage リリース 20.11.1

次に、単一の IPv6 エンドポイントトラッカー設定の **show endpoint-tracker** コマンドの出力例を示します。

```
Device# show endpoint-tracker

endpoint-tracker t1
ipv6-endpoint 2001:DB8:1::1
tracker-type ipv6-interface
```

次に、1 つのインターフェイスに適用された単一の IPv6 エンドポイントトラッカーの **show endpoint-tracker** コマンドの出力例を示します。

```
Device# show endpoint-tracker

Interface                    Record Name            Status          Address Family   RTT
 in msecs    Probe ID        Next Hop
GigabitEthernet1                  t1                  Up              IPv6
1               6               2001:DB8:1::1
```

次に、DNS トラッカー設定の **show endpoint-tracker** コマンドの出力例を示します。

```
Device# show endpoint-tracker

Interface                    Record Name            Status          Address Family   RTT
 in msecs    Probe ID        Next Hop
GigabitEthernet1                dns_t1               Up              IPv6             1
              9               2001:DB8:1::1
```

次に、IPv6 トラッカーグループ設定の **show endpoint-tracker tracker-group** コマンドの出力例を示します。

```
Device# show endpoint-tracker tracker-group

Tracker Name                    Element trackers name              Address Family
Status                       RTT in msec      Probe ID
groupv6                             t1, t2                           IPv6
UP(UP OR UP)                 1, 0             10, 11
```

次に、IPv4 と IPv6 の両方のトラッカーが同じインターフェイスに設定されている場合の **show endpoint-tracker** コマンドの出力例を示します。

```
Device# show endpoint-tracker

Interface                    Record Name            Status          Address Family   RTT
 in msecs    Probe ID        Next Hop
GigabitEthernet1                 t1                  Up              IPv4             1
               7               10.0.29.99
GigabitEthernet1                 t2                  Up              IPv6             1
               8               2001:DB8:1::1
```

ICMP トラッカーの設定の確認

テンプレートをデバイスにアタッチした後、Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a からコマンド構文を確認できます。

次に、1 つのインターフェイスに適用された単一の IPv6 ICMP エンドポイントトラッカーの **show endpoint-tracker** コマンドの出力例を示します。

```
Device# show endpoint-tracker

Interface                    Record Name            Status          Address Family   RTT
 in msecs    Probe ID        Next Hop
GigabitEthernet1                 t2                  Up              IPv6
1               6              2001:DB8:1::1
```

サービス側 NAT

表 *10 :* 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイス のサービス側 NAT	Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a Cisco vManage リリース 20.3.1	この機能を使用すると、ネットワークオーバーレイのサービス側ホストとの間で送受信されるデータトラフィックに、内部および外部 NAT を設定できます。 サービス側 NAT 設定を使用すると、サービス側のホストからオーバーレイへのデータトラフィック、およびオーバーレイからサービス側のホストへのトラフィックの送信元 IP アドレスを変換できます。
VPN 内サービス側 NAT に対応	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	VPN 内 NAT により、サービス側 LAN インターフェイスが同じ VPN 内の他のサービス側 LAN インターフェイスと通信できます。送信元 IP アドレスを外部ローカルアドレスに変換する必要がある LAN インターフェイスで **ip nat outside** コマンドを設定します。パケットが他の LAN インターフェイスから外部インターフェイスとして設定されたインターフェイスにルーティングされるように、スタティックまたはダイナミック NAT ルールを適用できます。 デバイス CLI テンプレートまたは CLI アドオンテンプレートを使用して、VPN 内サービス側 NAT を設定できます。

機能名	リリース情報	説明
サービス側条件付きスタティック NAT サポート	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a	この機能を使用すると、宛先 IP アドレスに基づいて、同じ送信元 IP アドレスを別の IP アドレスに変換できます。 デバイス CLI を使用して、サービス側条件付きスタティック NAT を設定できます。
サービス側スタティックネットワーク NAT のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1	この機能は、サブネットのサービス側スタティック NAT の設定をサポートします。複数のスタティック NAT プールを設定する代わりに、サブネット全体に対して単一のスタティック NAT プールを設定できます。 Cisco SD-WAN Manager またはデバイス CLI テンプレートを使用して、サービス側スタティックネットワーク NAT を構成できます。

サービス側 NAT に関する情報

Cisco IOS XE Catalyst SD-WAN デバイス では、デバイスのサービス側で NAT を設定して、データトラフィックがトランスポート VPN にあるオーバーレイトンネルに入る前に NAT 処理されるようにすることができます。サービス側 NAT は、受信するデータトラフィックの IP アドレスをマスクします。

デバイスのサービス側でダイナミック NAT と 1:1 スタティック NAT の両方を設定できます。これを行うには、デバイス上のサービス VPN 内に NAT プールインターフェイスを構成してから、Cisco Catalyst SD-WAN コントローラ で一元化されたデータポリシーを構成します。このポリシーは、必要なプレフィックスを持つデータトラフィックをサービス側 NAT に転送します。目的の NAT プールインターフェイスでダイナミック NAT またはスタティック NAT を設定します。

サービス側 NAT が有効になっている場合、VPN 1 で一致するすべてのプレフィックスは NAT プールインターフェイスに送信されます。このトラフィックは NAT 処理され、NAT はサービス側の IP アドレスを交換し、NAT プールの IP アドレスに置き換えます。その後、パケットは宛先に転送されます。

ネットワークのサービス側に出入りするデータの NAT を設定できます。サービス側 NAT は、構成された一元化されたデータポリシーと一致する、内部および外部ホストアドレスのデータトラフィックを変換します。

内部送信元アドレス変換

サービス側または LAN 側のホストがリモートブランチにトラフィックを送信する場合、内部アドレス変換サービスは送信元 IP アドレス（内部ホスト）変換を許可します。この変換は、データトラフィックがオーバーレイトンネルに送信される前に行われます。NAT 内部プールと内部スタティック NAT アドレスがオーバーレイに再配布されます。これらのアドレスは、オーバーレイ管理プロトコル（OMP）を使用してすべてのリモートブランチにアドバタイズされます。したがって、リモートホストは、内部ホストに到達するためのパスを認識しています。

内部アドレス変換の場合、サービス側データトラフィックは、ダイナミック NAT の一元化されたデータポリシーの一致条件と一致します。送信元 IP アドレスが一致条件を満たしている場合、データはサービス VPN で設定された NAT を通過してから、オーバーレイを介してリモートエッジルータに入ります。アドレス変換は、トンネルの出力インターフェイスで発生します。Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a および Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a よりも前のリリースでは、スタティック内部 NAT は一元化されたデータポリシーでの一致条件を必要としません。スタティック変換は、送信元 IP アドレスがスタティック NAT 用に設定された IP アドレスと一致する場合に発生します。

Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降、スタティック NAT をプールにマッピングでき、データポリシーの一致がある場合はスタティック NAT がトラフィックに適用されます。

外部送信元アドレス変換

リモートサイトからのトラフィックがオーバーレイトンネルを通過するとき、外部アドレス変換サービスはリモートホストの送信元 IP アドレス（外部ホスト）を変換します。変換は、トラフィックがネットワークの LAN（VPN）側に送信される前に行われます。ルート再配布が設定されている場合、NAT 外部プールアドレスまたはルートは、Open Shortest Path First（OSPF）または他のプロトコルを介してネットワークの LAN 側に再配布されます。したがって、内部ホストは、リモートホストに到達するためのパスを認識しています。

Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a より前のリリースと Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a までのリリースでは、サービス側 NAT の内側と外側の両方がダイナミック NAT 設定である必要があります。内部アドレス変換と外部アドレス変換の両方に 1:1 スタティック NAT マッピングを設定することもできます。

Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降、一元化されたデータポリシーを使用して、スタティック NAT の NAT プールアクションも設定できます。

（注） スタティック NAT を設定する前に、ダイナミック NAT を設定します。

サービス側 NAT のデータポリシー

Cisco IOS XE Catalyst SD-WAN デバイス で NAT を有効にするには、スタティックおよびダイナミック NAT の一元化されたデータポリシーを構成します。データポリシーは、ダイナミック NAT の一致基準と NAT プールアクションを提供します。

Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降、スタティック NAT の一致基準と NAT プールアクションを設定するデータポリシーを作成できます。

サービス側 NAT の利点

- 送信元 IPv4 アドレスから宛先 IPv4 アドレスへの変換を提供する
- パブリック IPv4 アドレスをプライベート送信元 IPv4 アドレスにマッピングする
- サービスプロバイダーが IPv6 へのシームレスな移行を実装する方法を提供する

サービス側 NAT のトラフィックフロー

サービス側 NAT の 2 つのデータトラフィックフローを次に示します。

- ネットワークのサービス側からオーバーレイネットワーク経由でリモートエッジに向かうトラフィックの送信元の変換
- オーバーレイネットワークを介してリモートエッジからネットワークのサービス側に向かうトラフィックの送信元の変換

サービス側からの NAT Feature Invocation Array（FIA）：トラフィックがトンネル経由でリモートエッジに向かうサービス VPN からのものである場合、NAT FIA はトンネルインターフェイスである出力インターフェイスで有効になります。データポリシーの方向は from-service として設定されています。

NAT FIA from-tunnel：トラフィックがリモートエッジからトンネルを通過してサービス VPN に到達する場合、サービス VPN LAN インターフェイスである出力インターフェイスで NAT FIA が有効になります。データポリシーの方向は from-tunnel として設定されています。

データポリシーの方向が all（全方向）に設定されている場合、サービス VPN インターフェイスおよびトンネルインターフェイスで NAT FIA が有効になります。

（注） 一元化されたデータポリシーの IP アドレスとスタティック NAT 送信元 IP アドレスは、Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a および Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a までの以前のリリースでは重複することはできません。トラフィックの一致条件が重複しないように、一元化されたデータポリシーを明確に定義する必要があります。

サービス側 NAT の制限事項

- NAT プールの変換のみがサポートされています。

- 異なる VRF 間の変換はサポートされていません。
- Cisco SD-WAN Manager では、最大 31 のプールを設定できます。
- NAT プール名を **natpool** *natpool-number* として指定します。*natpool-number* は、データポリシーで指定された NAT プール値と一致する必要があります。

  例：`natpool10`
- Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a、Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a、Cisco IOS XE Catalyst SD-WAN リリース 17.3.2 ではスタティック NAT アドレスは、プールアドレスで共有してはなりません。
- Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a から始まるスタティック NAT アドレスは、データポリシーと一緒に使用されている場合、設定された NAT プールアドレスリストに属している可能性があります。
- VRF のスタティック NAT には、データポリシーとダイナミック NAT プールを定義する必要があります。
- NAT64 の IPv4 変換はサポートされていません。
- 各サービス VPN には、一意の NAT プール番号が必要です。
- NAT エントリは、最初に作成した後は編集できません。

サービス側 NAT の設定

サービス側 NAT を設定するためのワークフロー

1. Cisco Catalyst SD-WAN コントローラの一元化されたデータポリシーを構成して、NAT プール番号とアクションを含めます。NAT 内部の一元化されたデータポリシーの方向は、[from-service] である必要があります。NAT 外部のポリシーの方向は [from-tunnel] である必要があります。
2. サービス側 VPN である [Cisco VPN] テンプレートを使用して、動的 NAT プール番号を設定します。
3. [Cisco VPN] テンプレートを使用して動的 NAT マッピングを設定します。
4. （オプション）[Cisco VPN] テンプレートを使用してスタティック NAT マッピングを設定します。

   Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降、スタティック NAT の NAT プールを設定し、スタティッ NAT の一致基準と NAT プールアクションを提供するデータポリシーを作成できます。

   サービス側のスタティック NAT の設定の詳細については、「サービス側スタティック NAT の設定」を参照してください。

5. NAT 内部の場合、NAT プールサブネットと IP アドレスのスタティック NAT 変換が OMP に自動的にアドバタイズされます。NAT 外部の場合、NAT プールサブネットの再配布と、IPv4 アドレスのサービス側プロトコルへのスタティック NAT 変換を手動で設定できます。

（注） データポリシーアクションが VPN 0 に対して設定されている場合、アクションは DIA トラフィックに対して設定されます。NAT プール設定を含むいずれかのサービス VPN（例：VPN 1）に対してデータポリシーアクションが設定されている場合、アクションはサービス側 NAT 用です。

サービス側 NAT の一元化されたデータポリシーの作成および適用

一元管理型データポリシーは、Cisco Catalyst SD-WAN コントローラ で設定され、Cisco Catalyst SD-WAN オーバーレイネットワーク上のルータ間で送信されるデータトラフィックに影響を与えるポリシーです。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policies]** を選択します。
2. [Centralized Policy] をクリックします。
3. [Add Policy] をクリックします。

   ポリシー構成ウィザードが開きます。一元管理型データポリシーの作成の詳細については、「Configure Centralized Policies Using Cisco SD-WAN Manager」を参照してください。
4. ポリシーリストを作成します。

   対象グループの構成の詳細については、「一元化されたポリシーの対象グループの構成」を参照してください。
5. トラフィック規則を設定します。

   トラフィックルールの構成に関する詳細については、「トラフィックルールの構成」を参照してください。
6. サイトと VPN にポリシーを適用します。

   サイトと VPN にポリシーを適用する方法の詳細については、「サイトと VPN にポリシーを適用する」を参照してください。

   ポリシーを適用する方向を [All]、[From Tunnel]、または [From Service] から選択します。

表 *11* : ダイナミックおよびスタティック *NAT* アプリケーション

NAT の設定	データポリシーの方向
ダイナミック NAT 内部のみ（NAT プール）	From-service
ダイナミック NAT 外部のみ（NAT プール）	From-tunnel

NAT の設定	データポリシーの方向
ダイナミック NAT 内部（NAT プール）+ スタティック NAT 内部のみ	From-service
ダイナミック NAT 内部（NAT プール）+スタティック ポート フォワーディングのみ	From-service
ダイナミック NAT 外部（NAT プール）+ スタティック NAT 外部のみ	From-tunnel
上記の 2 つ以上の組み合わせ	all

7. ポリシーをアクティブにします。

   ポリシーのアクティブ化の詳細については、「一元化データポリシーのアクティブ化」を参照してください。

サービス側ダイナミック NAT の設定

はじめる前に

1. Cisco Catalyst SD-WAN コントローラ の一元化されたデータポリシーを構成して、NAT プール番号とアクションを含めます。
2. 新しい [Cisco VPN] テンプレートを作成するか、既存の [Cisco VPN] テンプレートを編集します。[Cisco VPN] テンプレートは、NAT を設定するサービス側 VPN に対応します。

ダイナミック NAT プールの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Cisco VPN] テンプレートを編集するには、テンプレート名の横にある [...] をクリックし、[Edit] を選択します。
4. [NAT] をクリックします。
5. [NAT Pool] で、[New NAT Pool] をクリックします。
6. 必須パラメータを入力し、[Update] をクリックします。

表 *12 : NAT* プールパラメータ

パラメータ名	説明
[NAT Pool Name]	一元化されたデータポリシーで構成されている NAT プール番号を入力します。NAT プール名は、VPN および VRF 全体で一意である必要があります。ルータごとに最大 31（1 ～ 31）の NAT プールを設定できます。
[NAT Pool Prefix Length]	NAT プールのプレフィックス長を入力します。
[NAT Pool Range Start]	NAT プールの開始 IP アドレスを入力します。 **1.** フィールドを有効にするには、スコープを [Default] から [Global] に変更します。 **2.** NAT プールの最後の IP アドレスを入力します。
[NAT Pool Range End]	NAT プールの終了 IP アドレスを入力します。 **1.** フィールドを有効にするには、スコープを [Default] から [Global] に変更します。 **2.** NAT プールの最後の IP アドレスを入力します。
[NAT Overload]	[On] をクリックして、ポートごとの変換を有効にします。デフォルトは [オン（On）] です。 [NAT Overload] が [Off] に設定されている場合、ダイナミック NAT のみがエンドデバイスで設定されます。ポートごとの NAT は設定されていません。
[NAT Direction]	NAT 方向を選択します。

サービス側スタティック NAT の設定

Before You Begin

1. データポリシーを構成して適用します。
2. [Cisco VPN] テンプレートを設定するか、既存の [Cisco VPN] テンプレートを編集します。

3. ダイナミック NAT を設定します。

サービス側スタティック NAT の設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Cisco VPN] テンプレートを編集するには、テンプレート名の横にある [...] をクリックし、[Edit] を選択します。
4. [NAT] をクリックします。
5. [Static NAT] をクリックします。
6. [Static NAT] で、[New Static NAT] をクリックします。
7. 必須パラメータを入力し、[Update] をクリックします。

表 *13 :* スタティック *NAT* パラメータ

パラメータ名	説明
[NAT Pool Name]	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降、スタティック NAT にも NAT プールを使用できます。[Global] 設定オプションを使用して NAT プール番号を選択します。
送信元 IP アドレス	送信元 IP アドレスとして内部ローカルアドレスを入力します。
[Translated Source IP Address]	変換された送信元 IP アドレスとして内部グローバルアドレスを入力します。パブリック IP アドレスをプライベート送信元アドレスにマップします。 Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a では、スタティック NAT に NAT プールを使用している場合、スタティックに変換された送信元 IP アドレスは、設定されたダイナミック NAT プールの IP アドレス範囲内にある必要があります。
[Static NAT Direction]	ネットワークアドレス変換を行う方向を選択します。
内部	デバイスのサービス側から送信され、ルータのトランスポート側に向かうパケットの IP アドレスを変換するには、[Inside] を選択します。

パラメータ名	説明
外部	トランスポート側デバイスからデバイスに到着し、サービス側デバイス宛てのパケットの IP アドレスを変換するには、[Outside] を選択します。

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.4.1a および Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a までの以前のリリース（サービス側の NAT 機能が導入されたとき）では、スタティック NAT IP アドレスが NAT プール IP アドレスと重複してはなりません。

Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a では、スタティックに変換された送信元 IP アドレスは、設定されたダイナミック NAT プールの IP アドレス範囲内にある場合があります。

NAT のサービス側ポートフォワーディングの設定

ポート フォワーディング ルールを設定して、外部ネットワークからの要求が内部ネットワーク上のデバイスに到達できるようにすることができます。

Before You Begin

1. データポリシーを構成して適用します。
2. [Cisco VPN] テンプレートを設定するか、既存の [Cisco VPN] テンプレートを編集します。
3. NAT プールを設定します。

NAT のサービス側ポートフォワーディングの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Cisco VPN] テンプレートを編集するには、テンプレート名の横にある [...] をクリックし、[Edit] を選択します。
4. [NAT] をクリックします。
5. [NAT Pool] で、[New NAT Pool] をクリックします。
6. 必須 NAT パラメータを入力します。

   NAT プールパラメータの詳細については、「NAT プールとループバック インターフェイスの設定」を参照してください。

7. [Add] をクリックします。
8. ポートフォワーディングルールを作成するには、**[Port Forward]** > **[Add New Port Forwarding Rule]**をクリックし、必要なパラメータを設定します。

   最大 128 のポート転送ルールを定義して、外部ネットワークからの要求が内部ネットワーク上のデバイスに到達できるようにすることができます。

   表 *14*：ポート フォワーディング パラメータ

パラメータ名	説明
[NAT Pool Name]	Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a 以降、スタティック NAT に NAT プールを使用できます。[Global] 設定オプションを使用して NAT プール番号を選択します。
送信元ポート	ポート番号を入力して、変換する送信元ポートを定義します。範囲：0 ～ 65535
送信元 IP アドレス	変換される送信元アドレスを入力します。
[Translate Port]	ポートフォワーディングを適用するポート番号を入力します。 範囲：0 ～ 65535 Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a では、スタティックに変換された送信元 IP アドレスは、設定されたダイナミック NAT プールの IP アドレス範囲内にある必要があります。
Protocol	ポート フォワーディング ルールを適用する [TCP] または [UDP] を選択します。TCP トラフィックと UDP トラフィックの両方で同じポートを一致させるには、2 つのルールを構成します。
[Translated Source IP Address]	OMP にアドバタイズされる NAT IP アドレスを指定します。ポートフォワーディングは、変換されたポートが一致するオーバーレイから、この IP アドレス宛てのトラフィックに適用されます。

9. [更新（Update）] をクリックします。

CLI を使用したサービス側 NAT の設定

一元化されたデータポリシーの構成：送信元の条件を任意の宛先に一致させる

送信元 IP から任意の宛先 IP への一致条件を含む一元化されたデータポリシーを設定します。

```
policy
 data-policy edge1
  vpn-list vpn_1
   sequence 101
    match
     source-ip 192.168.11.0/24
```

```
    !
    action accept
     count nat_vrf_1
     nat pool 1
    !
   !
   default-action accept
  !
  vpn-list vpn_2
   sequence 102
    match
     source-ip 192.168.22.0/24
    !
    action accept
     count nat_vrf_2
     nat pool 2
    !
   !
   default-action accept
  !
  vpn-list vpn_3
   sequence 103
    match
     source-ip 192.168.13.0/24
    !
    action accept
     count nat_vrf_3
     nat pool 3
    !
   !
   default-action accept
  !
 !
 lists
  vpn-list vpn_1
   vpn 1
  !
  vpn-list vpn_2
   vpn 2
  !
  vpn-list vpn_3
   vpn 3
  !
  site-list edge1
   site-id 500
  !
 !
!
```

内部ダイナミックおよびスタティック NAT の設定

NAT プールの内部ダイナミックおよびスタティック NAT を設定します。

```
ip nat pool natpool1 10.11.11.1 10.11.11.2 prefix-length 24
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload
!
ip nat pool natpool2 10.22.22.1 10.22.22.2 prefix-length 24
ip nat outside source list global-list pool natpool2 vrf 2 overload match-in-vrf
ip nat outside source static 192.168.22.10 10.22.22.10 vrf 2 match-in-vrf
!
ip nat pool natpool3 10.13.13.1 10.13.13.2 prefix-length 24
ip nat inside source list global-list pool natpool3 vrf 3 match-in-vrf overload
```

```
ip nat inside source static tcp 192.168.13.10 80 10.13.13.10 8080 vrf 3 extendable
match-in-vrf
```

内部スタティック NAT の NAT プールを使用したスタティック NAT の設定（Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a から開始）

NAT プールの内部でスタティック NAT を設定します。

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
```

NAT プールに内部スタティック NAT および外部スタティック NAT を設定します。

```
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat pool natpool2 10.11.11.5 10.11.11.6 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
ip nat outside source static 192.168.21.10 10.22.22.10 vrf 1 match-in-vrf pool natpool1
```

使用例 1：内部 NAT プールを使用した内部スタティック NAT

この例では、内部スタティック NAT のみが NAT プールにマッピングされている場合、シーケンス 101 は、オーバーレイネットワークを介してリモートエッジからネットワークのサービス側に向かうスタティック NAT トラフィック（インからアウトへ）に対して、データポリシー構成を指定します。シーケンス 102 は、ネットワークのサービス側から、宛先グローバル IP アドレス 10.11.11.10 のリモートエッジデバイス宛てのトラフィック（アウトからイン）に対してデータポリシー構成を指定します。

```
policy
 data-policy edge1
  vpn-list vpn_1
   sequence 101
    match
     source-ip 192.168.11.0/24
     destination-ip 192.168.21.0/24
    !
    action accept
     count nat_vrf_1
     nat pool 1
    !
   !
   default-action accept
  !
 sequence 102
    match
     source-ip 192.168.21.0/24
     destination-ip 10.11.11.0/27
    !
    action accept
     count nat_vrf_2
     nat pool 2
    !
   !
   default-action accept
  !
   default-action accept
```

```
  !
 !
```

使用例 2：内部 NAT アドレスプールにマッピングされた内部スタティック NAT および外部スタティック NAT

この例では、内部スタティック NAT と外部スタティック NAT が NAT プールにマッピングされている場合、シーケンス 101 は、オーバーレイネットワークを介してリモートエッジデバイスからネットワークのサービス側に向かうスタティック NAT トラフィック（インからアウトへ）に対して、データポリシー構成を指定します。シーケンス 102 は、ネットワークのサービス側から、宛先グローバル IP アドレス 10.11.11.10 のリモートエッジデバイス宛てのトラフィック（アウトからイン）に対してデータポリシー構成を指定します。

```
policy
data-policy vedge1
  vpn-list vpn_1
   sequence 101
    match
     source-ip 192.168.11.0/24
     destination-ip 10.22.22.10/27
    !
    action accept
     count nat_vrf_1
     nat pool 1
    !
   !
   sequence 102
    match
     source-ip 192.168.21.0/24
     destination-ip 10.11.11.0/27
    action accept
     nat pool 1
   default-action accept
  !
```

（注） Cisco IOS XE Catalyst SD-WAN リリース 17.3.1a 以降、**ip nat settings central-policy** コマンドは、Cisco IOS XE Catalyst SD-WAN デバイス の NAT が Cisco Catalyst SD-WAN モードで機能するために必要です。Cisco SD-WAN Manager 機能テンプレートを使用してデバイスで NAT を有効にする場合、Cisco SD-WAN Manager はこのコマンドをデバイスに自動的にプッシュします。ただし、デバイスで NAT を設定するためだけにデバイス CLI テンプレートを使用している場合は、デバイス CLI テンプレート設定に **ip nat settings central-policy** コマンドを追加する必要があります。

サービス側 NAT の設定の確認

VRF 1 の例

192.168.11.10 からのトラフィックは、スタティック NAT ルールに基づいて変換されます。192.168.11.0/24 の他の送信元からのトラフィックは、プール IP に変換されます。

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
tcp  10.13.13.10:8080      192.168.13.10:80      ---                   ---
```

```
---  ---                  ---                  10.22.22.10          192.168.22.10

---  10.11.11.10          192.168.11.10        ---                  ---
icmp 10.11.11.1:18193     192.168.11.2:18193   192.168.21.2:18193   192.168.21.2:18193
tcp  10.11.11.10:59888    192.168.11.10:59888  192.168.21.10:21     192.168.21.10:21
tcp  10.11.11.10:50069    192.168.11.10:50069  192.168.21.10:35890  192.168.21.10:35890
tcp  10.11.11.10:39164    192.168.11.10:39164  192.168.21.10:80     192.168.21.10:80
Total number of translations: 7
```

VRF 2 の例

192.168.22.10 からのトラフィックは、スタティック NAT ルールに基づいて 10.22.22.10 に変換されます。他の送信元 192.168.22.0/24 からのトラフィックは、プール IP に変換されます。

```
Device# show ip nat translations
Pro  Inside global        Inside local          Outside local         Outside global
tcp  10.13.13.10:8080     192.168.13.10:80      ---                   ---
---  ---                  ---                   10.22.22.10           192.168.22.10

---  10.11.11.10          192.168.11.10         ---                   ---
tcp  192.168.12.10:21     192.168.12.10:21      10.22.22.10:56602     192.168.22.10:56602
tcp  192.168.12.10:46238  192.168.12.10:46238   10.22.22.10:49532     192.168.22.10:49532
icmp 10.22.22.1:18328     192.168.22.2:18328    192.168.12.2:18328    192.168.12.2:18328
tcp  192.168.12.10:80     192.168.12.10:80      10.22.22.10:46340     192.168.22.10:46340
Total number of translations: 7
```

VRF 3 の例

10.13.13.10:8080 へのトラフィックはすべて 192.168.13.10:80 に変換されます。192.168.11.0/24 からのその他のトラフィックはすべて、プール IP に変換されます。

```
Device# show ip nat translations
Pro  Inside global        Inside local          Outside local         Outside global
tcp  10.13.13.10:8080     192.168.13.10:80      ---                   ---
---  ---                  ---                   10.22.22.10           192.168.22.10

---  10.11.11.10          192.168.11.10         ---                   ---
tcp  10.13.13.1:43162     192.168.13.10:43162   192.168.23.10:21      192.168.23.10:21
tcp  10.13.13.1:41753     192.168.13.10:41753   192.168.23.10:34754   192.168.23.10:34754
icmp 10.13.13.1:19217     192.168.13.2:19217    192.168.23.2:19217    192.168.23.2:19217
tcp  10.13.13.10:8080     192.168.13.10:80      192.168.23.10:40298   192.168.23.10:40298
tcp  10.13.13.1:43857     192.168.13.10:43857   192.168.23.10:80      192.168.23.10:80
Total number of translations: 8
```

NAT プールがスタティック NAT に使用されている場合のサービス側 NAT の確認（Cisco IOS XE Catalyst SD-WAN リリース 17.5.1a から）

次の出力例は、クライアント 1（192.168.11.10）からサーバー 2（192.168.21.11）への UDP トラフィックを示しています。

```
Device# show ip nat translations
Pro  Inside global        Inside local          Outside local         Outside global
---  10.11.11.2           192.168.11.10         ---                   ---
---  10.11.11.5           192.168.11.10         ---                   ---
udp  10.11.11.5:5001      192.168.11.10:5001    192.168.21.11:5001    192.168.21.11:5001
 ----> NAT IP from Pool 2
Total number of translations: 3
```

次の出力例は、クライアント 1（192.168.11.10）からサーバー 1（192.168.21.10）への UDP トラフィックを示しています。

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  10.11.11.2            192.168.11.10         ---                   ---
---  10.11.11.5            192.168.11.10         ---                   ---
udp  10.11.11.5:5001       192.168.11.10:5001    192.168.21.11:5001    192.168.21.11:5001
 ----> NAT IP from Pool 2
udp  10.11.11.2:5001       192.168.11.10:5001    192.168.21.10:5001    192.168.21.10:5001
 ----> NAT IP as per static NAT rule mapped to Pool 1
Total number of translations: 4
```

次の出力例は、クライアント 2（192.168.11.11）からサーバー 2（192.168.21.11）への UDP トラフィックを示しています。

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  10.11.11.2            192.168.11.10         ---                   ---
---  10.11.11.6            192.168.11.11         ---                   ---
---  10.11.11.5            192.168.11.10         ---                   ---
udp  10.11.11.5:5001       192.168.11.10:5001    192.168.21.11:5001    192.168.21.11:5001
 ----> NAT IP from pool 2
udp  10.11.11.6:5001       192.168.11.11:5001    192.168.21.11:5001    192.168.21.11:5001
 ----> NAT IP from pool 2
udp  10.11.11.2:5001       192.168.11.10:5001    192.168.21.10:5001    192.168.21.10:5001
 ----> NAT IP as per static NAT rule mapped to Pool 1
Total number of translations: 6
```

サービス側 NAT の設定例

例：Cisco VPN インターフェイス イーサネット テンプレートでの NAT 設定

```
ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1 overload

  ip nat translation tcp-timeout 3600
  ip nat translation udp-timeout 60
  ip nat route vrf 1 10.0.0.1 10.0.0.1 global

interface GigabitEthernet1
   no shutdown
   arp timeout 1200
   ip address 10.1.15.15 255.255.255.0
   ip redirects
   ip mtu    1500
   ip nat outside
```

例：ダイナミック NAT の設定

```
ip nat pool natpool-gigabitethernet1-0 198.51.100.1 198.51.100.2 prefix-length 24
ip nat inside source list global-list pool natpool-gigabitethernet1-0 egress-interface
GigabitEthernet1
```

例：インターフェイス過負荷の設定

```
ip nat pool natpool-gigabitethernet1-0 209.165.201.1 209.165.201.2 prefix-length 24
ip nat inside source list global-list pool natpool-gigabitethernet1-0 overload
egress-interface GigabitEthernet1
```

例：ループバック インターフェイスによるインターフェイス過負荷の設定

```
ip nat inside source list global-list interface loopback1 overload egress-interface
GigabitEthernet1
```

VPN 内サービス側 NAT

次のセクションでは、VPN 内サービス側 NAT の設定に関する情報を提供します。

VPN 内サービス側 NAT に関する情報

VPN 内サービス側 NAT はサービス側 NAT の拡張機能であり、サービス側 LAN インターフェイスが、同じ VPN 内の別のサービス側 LAN インターフェイスと通信できるようにします。VPN 内サービス側 NAT は、スタティックまたはダイナミック NAT を使用して、データトラフィックをどちらの方向にも開始できるようにします。**ip nat outside** コマンドを使用して、パケットが他の LAN インターフェイスから外部インターフェイスとして設定されたインターフェイスにルーティングされるように、スタティックまたはダイナミック NAT ルールを適用できます。

デバイス CLI テンプレートまたは CLI アドオンテンプレートを使用して、VPN 内サービス側 NAT を設定できます

VPN 内サービス側 NAT のポートフォワーディングを設定できます。

VPN 内サービス側 NAT のポートフォワーディングの設定の詳細については、「NAT のサービス側ポートフォワーディングの設定」を参照してください。

VPN 内サービス側 NAT の利点

- 同じ VPN で LAN-to-LAN トラフィックをサポート可能
- 実際の IP アドレスとマッピングされた IP アドレス間をマッピングする際にスタティックまたはダイナミック NAT をサポート可能
- 同じ VPN 内の 2 つの LAN インターフェイス間の双方向トラフィックをサポート可能

VPN 内サービス側 NAT の制限事項

- リモートブランチへのサービス側 LAN インターフェイスの NAT はサポートされていません。
- サービス側 LAN インターフェイスからのパケットでは、ダイレクトインターネットアクセス（DIA）はサポートされていません。
- サービス間 LAN インターフェイスは、同じ VPN 内にある必要があります。

  NAT は、異なる VPN 間ではサポートされていません。
- ファイアウォール、AppNav-XE、およびマルチキャストはサポートされていません。
- デバイス CLI テンプレートまたは CLI アドオンテンプレートを使用して、VPN 内サービス側 NAT を設定します。Cisco SD-WAN Manager 機能テンプレートのサポートは Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a では利用できません。

（注） 他の NAT 関連機能に Cisco SD-WAN Manager 機能テンプレートを使用すると、**ip nat outside** 設定がインターフェイスから削除されます。したがって、VPN 内サービス側 NAT 機能は使用できません。

- データポリシーの方向を [Al] として設定します。
- LAN 側の物理インターフェイスとイーサネット サブ インターフェイスのみがサポートされます。ループバックおよびブリッジ ドメイン インターフェイス（BDI）インターフェイスはサポートされていません。
- ポート転送を使用した NAT DIA はサポートされていません。

VPN 内サービス側 NAT の設定

VPN 内サービス側 NAT を設定するためのワークフロー

1. スタティックまたはダイナミック NAT マッピングの Cisco Catalyst SD-WAN コントローラの一元化されたデータポリシーを設定します。

   一元化されたデータポリシーの設定の詳細については、「NAT の一元化されたデータポリシーの作成と適用」を参照してください。

2. [Cisco VPN] テンプレートを使用して、スタティックまたはダイナミック NAT を設定します。
3. （オプション）スタティックまたはダイナック NAT マッピングのプール名を設定します。

   スタティックまたはダイナミック NAT マッピングのプール名の設定の詳細については、「サービス側のスタティック NAT の設定」を参照してください。

4. デバイスの CLI テンプレートまたは CLI アドオンテンプレートを使用して、NAT 変換用の外部インターフェイスを設定し、その設定をデバイスに適用します。
5. デバイス CLI テンプレートまたは CLI アドオンテンプレートをデバイスに接続します。

CLI アドオンテンプレートを使用した VPN 内サービス側 NAT の設定

はじめる前に

新しい CLI アドオンテンプレートを作成するか、既存の CLI アドオンテンプレートを編集します。

CLI Add-on Feature Templates の詳細については、「CLI Add-on Feature Templates」を参照してください。

CLI アドオンテンプレートを使用した VPN 内サービス側 NAT の設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Add template] をクリックします。
4. デバイスリストからデバイスを選択します。
5. [OTHER TEMPLATES] の [CLI Add-On Template] をクリックします。
6. [CLI Add-On Template] エリアで、設定を入力します。
7. **ip nat outside** コマンドを使用して、外部インターフェイスを設定します。
8. **[Save（保存）]** をクリックします。

   作成した CLI アドオンテンプレートが [CLI Configuration] に表示されます。
9. CLI アドオンテンプレートをデバイスにアタッチします。

VPN 内サービス側 NAT の設定例

例：ポリシーの構成

次に、NAT プールを含む Cisco Catalyst SD-WAN コントローラ の一元化されたデータポリシーの構成例を示します。

```
Device# show running policy
policy
data-policy cedge1
vpn-list vpn_1
sequence 101
match
source-ip 192.168.11.0/24
!
action accept
count nat_vrf_1
nat pool 1
!
!
default-action accept
!
!
lists
vpn-list vpn_1
vpn 1
!
site-list cedge1
site-id 500
.
```

.
.

例：IP NAT 外部で設定された LAN インターフェイス 1

次の例は、**ip nat outside** インターフェイスが GigabitEthernet 5.102 インターフェイスに設定されていることを示しています。

```
Device# interface GigabitEthernet5.102
encapsulation dot1Q 102
vrf forwarding 1
ip address 192.168.12.1 255.255.255.0
ip mtu 1496
ip nat outside
ip ospf dead-interval 40
ip ospf 1 area 0
pool configuration:
ip nat pool natpool1 10.11.11.1 10.11.11.2 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload

static nat inside config:
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vr
end
```

例：LAN インターフェイス 2

次の例は、GigabitEthernet 5.101 インターフェイスが同じ VPN および VRF で設定されていることを示しています。

```
Device# interface GigabitEthernet5.101
encapsulation dot1Q 101
vrf forwarding 1
ip address 192.168.11.1 255.255.255.0
ip mtu 1496
ip ospf dead-interval 40
ip ospf 1 area 0
pool configuration:
ip nat pool natpool1 10.11.11.1 10.11.11.2 prefix-length 24
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload

static nat inside config:
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vr
end
```

サービス側条件付きスタティック NAT

次のセクションでは、サービス側条件付きスタティック NAT の設定について説明します。

サービス側条件付きスタティック NAT に関する情報

サービス側条件付きスタティック NAT を設定して、宛先 IP アドレスに基づいて、同じ送信元 IP アドレスを別のグローバル IP アドレスに変換します。

サービス側条件付き NAT を使用すると、設定済みの別のスタティック NAT プール IP アドレス範囲内で同じ送信元 IP アドレスを設定できます。Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a 以前は、この機能はサポートされていませんでした。

デバイス CLI を使用して、サービス側条件付きスタティック NAT を設定します。

サービス側条件付きスタティック NAT の利点

- データポリシーの宛先 IP アドレスに基づいて、同じ送信元 IP アドレスを別の IP アドレスに変換します。
- 別の構成済みスタティック NAT プール IP アドレス範囲内で同じ送信元 IP アドレスを使用できるようにします。

サービス側条件付きスタティック NAT の制限事項

- サービス側の条件付きスタティック NAT は、内部スタティック NAT およびサービス側トラフィック専用です。
- 外部スタティック NAT はサポートされていません。
- DIA トラフィックはサポートされていません。

サービス側条件付きスタティック NAT を設定するためのワークフロー

1. 一元化されたデータポリシーを構成し、異なる宛先 IP アドレスでシーケンスを構成します。

   詳細については、「サービス側 NAT の一元化されたデータポリシーの作成と適用」を参照してください。

2. 同じローカル IP アドレスを持つ少なくとも 2 つの NAT プールを設定します。

   CLI を使用したサービス側条件付きスタティック NAT の設定の詳細については、「CLI を使用したサービス側条件付きスタティック NAT の設定」を参照してください。

3. 宛先 IP アドレスの変換を確認します。

   宛先 IP アドレスの変換の確認に関する詳細については、「CLI を使用した条件付き静的 NAT の確認」を参照してください。

CLI を使用したサービス側条件付きスタティック NAT の設定

1. 一元化されたデータポリシーを構成し、シーケンスを構成します。

```
data-policy EDGE1
vpn-list vpn_1
sequence 101
match
source-ip 192.168.11.10/32
destination-ip 192.168.21.10/32
!
action accept
count vrf1_In2Out1
nat pool 1
!
!
sequence 102
```

```
match
source-ip 192.168.11.10/32
destination-ip 192.168.21.2/32
!
action accept
count vrf1_In2Out2
nat pool 2
!
!
default-action accept
!
!
lists
vpn-list vpn_1
vpn 1
!
site-list EDGE1
site-id 500
!
!
!
```

2. 少なくとも 2 つの NAT プールを設定します。

```
Device(config)# ip nat pool natpool1 10.11.11.1 10.11.11.10 prefix-length 24
Device(config)# ip nat pool natpool2 10.22.22.1 10.22.22.10 prefix-length 24
```

3. 対応する NAT プールに同じ送信元 IP アドレスを使用して、内部スタティック NAT を設定します。

```
Device(config)# ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1
match-in-vrf pool natpool1
Device(config)# ip nat inside source static 192.168.11.10 10.22.22.10 vrf 1
match-in-vrf pool natpool2
Device(config)# ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf
 overload
Device(config)# ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
 overload
```

サービス側条件付きスタティック NAT の設定の確認

NAT Pool 1 および NAT Pool 2 の送信元 IP 変換例

natpool1 の場合、Cisco IOS XE Catalyst SD-WAN デバイス は送信元 IP アドレス `192.168.11.10` を `10.11.11.10` に変換し、宛先は `192.168.21.10` です。

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  10.11.11.10           192.168.11.10         ---                   ---
---  10.22.22.10           192.168.11.10         ---                   ---
icmp 10.22.22.10:8371      192.168.11.10:8371    192.168.21.2:8371     192.168.21.2:8371
icmp 10.11.11.10:8368     192.168.11.10:8368    192.168.21.10:8368    192.168.21.10:8368
Total number of translations: 4
```

natpool2 の場合、Cisco IOS XE Catalyst SD-WAN デバイス は送信元 IP アドレス `192.168.11.10` を `10.22.22.10` に変換し、宛先は `192.168.21.2` です。

サービス側スタティックネットワーク NAT

次のセクションでは、サービス側スタティックネットワーク NAT の設定について説明します。

サービス側スタティックネットワーク NATの情報

1 つの設定を使用して、ネットワーク全体にサービス側スタティック NAT を設定できます。

Cisco SD-WAN Manager またはデバイス CLI テンプレートを使用して、サービス側スタティックネットワーク NAT を構成できます。

サービス側スタティックネットワーク NATの利点

- サブネット全体を設定するための単一のスタティック NAT プールの設定をサポートします。
- LAN プレフィックスおよび LAN インターフェイスのオブジェクトトラッカー機能をサポートします。

サービス側スタティックネットワーク NATの制限事項

- 一元化されたデータポリシーを使用した構成はサポートされていません。
- NAT プールアドレスの重複はサポートされていません。
- サービス側内部ネットワーク NAT のみがサポートされます。
- 外部スタティックネットワーク NAT はサポートされていません。
- DIA 設定はサポートされていません。

サービス側スタティックネットワーク NAT の構成

Before You Begin

- データポリシーを構成して適用します。

  サービス側 NAT の一元化されたデータポリシーの作成と適用の詳細については、「サービス側 NAT の一元化されたデータポリシーの作成と適用」を参照してください。

- [Cisco VPN] テンプレートを設定するか、既存の [Cisco VPN] テンプレートを編集します。
- サービス側スタティック NAT を設定します。

（注） サービス側スタティックネットワーク NAT を構成する前に、NAT プールを構成する必要があります。

サービス側スタティック NAT と NAT プールの設定の詳細については、「サービス側スタティック NAT の設定」を参照してください。

サービス側スタティックネットワーク NAT の構成

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. [Cisco VPN] テンプレートを編集するには、テンプレート名の横にある [...] をクリックし、[Edit] を選択します。
4. [NAT] をクリックします。
5. [Static NAT] をクリックします。
6. [Static NAT] で、[New Static NAT Subnet] をクリックします。
7. 必須パラメータを入力します。

表 *15*：新しいスタティック *NAT* サブネットパラメータ

パラメータ名	説明
[Source IP Subnet]	送信元 IP サブネットアドレスとして内部ローカルアドレスを入力します。
[Translated Source IP Subnet]	変換された送信元 IP サブネットアドレスとして、外部グローバル サブネット アドレスを入力します。パブリック IP アドレスをプライベート送信元アドレスにマップします。
[Network Prefix Length]	ネットワークのプレフィックス長を入力します。
[Static NAT Direction]	ネットワークアドレス変換の方向を選択します。 ネットワーク アドレス変換を実行する方向として [内部] を選択します。
[Add Object /Group Tracker]	（オプション）オブジェクトをトラッキングする場合は、オブジェクト ID 番号を入力します。 オブジェクトトラッカー機能は、サービス側スタティックネットワーク NAT でサポートされています。

8. [更新（Update）] をクリックします。

CLI を使用したサービス側スタティックネットワーク NAT の構成

1. 次のコマンドを使用して、サービス側スタティックネットワーク NAT を構成します。

```
Device(config)# ip nat inside source static network 192.168.11.0 192.168.70.0 /24
vrf 1
match-in-vrf
```

2. （オプション）サービス側 NAT オブジェクトトラッカーを設定します。

詳細については、「サービス側 NAT オブジェクトトラッカーの設定」を参照してください。

サービス側スタティックネットワーク NAT 設定の確認

次のセクションでは、サービス側スタティックネットワーク NAT 設定を確認する方法について説明します。

サービス側スタティックネットワーク NAT の変換の確認

次に、**show ip nat translations** コマンドの出力例を示します。

```
Device# show ip nat translations
Pro  Inside global         Inside local          Outside local         Outside global
---  192.168.70.0          192.168.11.0          ---                   ---
---  192.168.70.11         192.168.11.11         ---                   ---
---  192.168.70.10         192.168.11.10         ---                   ---
icmp 192.168.70.11:16528   192.168.11.11:16528   192.168.21.11:16528   192.168.21.11:16528
icmp 192.168.70.10:16525   192.168.11.10:16525   192.168.21.10:16525   192.168.21.10:16525
icmp 192.168.70.10:16526   192.168.11.10:16526   192.168.21.10:16526   192.168.21.10:16526
icmp 192.168.70.10:16527   192.168.11.10:16527   192.168.21.10:16527   192.168.21.10:16527
```

サービス側スタティックネットワーク NAT ルートの作成の確認

次に、**show ip route vrf** コマンドの出力例を示します。

```
Device# show ip route vrf 1
Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected

Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 5 subnets, 2 masks
n Nd     10.0.1.0/24 [6/0], 2d00h, Null0
C        10.0.100.0/24 is directly connected, GigabitEthernet8
L        10.0.100.15/32 is directly connected, GigabitEthernet8
C        10.20.24.0/24 is directly connected, GigabitEthernet5
L        10.20.24.15/32 is directly connected, GigabitEthernet5
n Ni  192.168.70.0/24 [7/0], 00:00:12, Null0
```

サービス側 NAT オブジェクトトラッカー

表 *16 :* 機能の履歴

機能名	リリース情報	説明
サービス側 NAT オブジェクトトラッカーのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.8.1a Cisco vManage リリース 20.8.1	この機能により、サービス側スタティック NAT 内部の LAN プレフィックスと LAN インターフェイスのトラッキングのサポートが追加されます。 NAT ルートに関連付けられているオブジェクトトラッカーの状態 (アップまたはダウン) が変化すると、NAT OMP ルートがルーティングテーブルに追加または削除されます。追加または削除された NAT ルートとインターフェイスをモニタリングするための Cisco SD-WAN Manager の通知を表示できます。 サービス側 NAT オブジェクトトラッカーは、Cisco SD-WAN Manager、デバイス CLI テンプレート、または CLI アドオンテンプレートを使用して設定できます。

サービス側 NAT オブジェクトトラッカーに関する情報

サービス側 NAT オブジェクトトラッカーは、次のトラッキングのサポートを提供します。

- LAN プレフィックス：ルーティングテーブルのルート情報ベース（RIB）のプレフィックスを追跡します。

（注） ルーティングテーブルにプレフィックスがない場合、サービス側 NAT オブジェクトトラッカーは NAT プレフィックスの OMP ルートを削除します。

- LAN インターフェイス：LAN インターフェイスが稼働しているかどうかを追跡します。

トラッキング対象の各オブジェクトは、Cisco SD-WAN Manager、デバイス CLI、または CLI アドオンテンプレートで指定された一意の番号によって識別されます。クライアントプロセスは、この番号を使用して特定のオブジェクトを追跡します。

トラッキングプロセスは、トラッキング対象のオブジェクトを定期的にポーリングし、値の変更があれば記録します。トラッキング対象オブジェクトの変更は、すぐに、または指定された遅延後に、対象のクライアントプロセスに通知されます。オブジェクトの値は、アップまたはダウンとして報告されます。

LAN プレフィックスまたは LAN インターフェイスの状態に応じて、OMP を介した NAT ルートアドバタイズメントが追加または削除されます。Cisco SD-WAN Manager でイベントログを表示して、どの NAT ルートアドバタイズメントが追加または削除されたかを監視できます。

Cisco SD-WAN Manager でのオブジェクトトラッカーイベントログの監視の詳細については、「サービス側 NAT オブジェクトトラッカーの監視」を参照してください。

サービス側の NAT オブジェクトトラッカーは、Cisco SD-WAN Manager、デバイス CLI、または CLI アドオンテンプレートを使用して設定できます。

track キーワードが **ip nat inside source** コマンドに追加します。

track キーワードの詳細については、*Cisco Catalyst SD-WAN Qualified Command Reference* の ip nat inside source コマンドを参照してください。

サービス側 NAT オブジェクトトラッカーの利点

- オブジェクトトラッカーの状態に基づいて、OMP を介して NAT ルートアドバタイズメントを追加または削除します。
- 追加または削除された NAT ルート広告を監視するための Cisco SD-WAN Manager イベントログ通知を提供します。
- LAN プレフィックスと LAN インターフェイスのオブジェクト トラッカー サポートを提供します。

サービス側 NAT オブジェクトトラッカーの制限事項

- サービス側スタティック NAT オブジェクトトラッカーは、スタティック NAT 内およびダイナミック NAT 内でのみサポートされます。
- 外部スタティック NAT または NAT DIA はサポートされていません。
- 外部変換とポートフォワーディングはサポートされていません。
- Cisco SD-WAN Manager は、IP ルートの追跡をサポートしていません。デバイス CLI テンプレートまたは CLI アドオンテンプレートを使用して、IP ルートをトラッキングできます。Cisco SD-WAN Manager を使用して、インターフェイスをオブジェクトとしてトラッキングできます。

サービス側 NAT オブジェクトトラッカーの使用例

LAN インターフェイスまたは LAN プレフィックスがダウンすると、サービス側 NAT オブジェクトトラッカーが自動的にダウンします。Cisco SD-WAN Manager でイベントログを表示して、どの NAT ルートアドバタイズメントが追加または削除されたかを監視できます。

サービス側 NAT オブジェクトトラッカーを設定するためのワークフロー

1. Cisco Catalyst SD-WAN コントローラの一元化されたデータポリシーを構成して、NAT プール番号とアクションを含めます。

   サービス側 NAT オブジェクトトラッカーの一元化されたデータポリシーの構成と適用の詳細については、「サービス側 NAT の一元化されたデータポリシーの作成と適用」を参照してください。

2. Cisco System テンプレートを使用して、サービス側 NAT オブジェクトトラッカーまたはトラッカーグループを設定します。

   サービス側 NAT オブジェクトトラッカーの設定の詳細については、「サービス側 NAT オブジェクトトラッカーの設定」を参照してください。

3. （オプション）サービス側ダイナミック NAT を設定します。

   サービス側ダイナミック NAT の設定の詳細については、「サービス側ダイナミック NAT の設定」を参照してください。

4. サービス側スタティック NAT の NAT プールを設定します。

   サービス側スタティック NAT の NAT プールの設定の詳細については、「サービス側スタティック NAT の設定」を参照してください。

5. Cisco VPN テンプレートを使用して、サービス側 NAT オブジェクトトラッカーをスタティック内部 NAT プールに関連付けます。

   Cisco VPN テンプレートを使用してサービス側 NAT オブジェクトトラッカーをスタティック内部 NAT プールに関連付ける方法の詳細については、「Cisco VPN テンプレートを使用したサービス側 NAT オブジェクトトラッカーと NAT プールの関連付け」を参照してください。

サービス側 NAT オブジェクトトラッカーの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. [Cisco System] テンプレートを編集するには、テンプレート名の横にある [...] をクリックし、[Edit] を選択します。

4. [Tracker] をクリックし、[New Object Tracker] を選択して、サービス側の NAT オブジェクト トラッカー パラメータを設定します。

表 *17*：サービス側 *NAT* オブジェクト トラッカー パラメータ

フィールド	説明
[Tracker Type]	[Interface] または [Route] を選択して、LAN インターフェイスまたは LAN プレフィックスのオブジェクトトラッキングを設定します。
オブジェクト ID	オブジェクト ID 番号を入力します。 オブジェクト番号はトラッキング対象のオブジェクトを識別し、1 ～ 1000 の範囲で指定できます。
インターフェイス（Interface）	グローバルインターフェイスまたはデバイス固有のインターフェイスを選択します。

5. [Add] をクリックします。
6. [更新（Update）] をクリックします。
7. （オプション）トラッカーグループを作成するには、[Tracker] を選択し、**[Tracker Groups]**>**[New Object Tracker Groups]**をクリックして、サービス側 NAT オブジェクトトラッカーを設定します。

（注） トラッカーグループを作成するために 2 つのトラッカーを作成したことを確認してください。

表 *18*：サービス側 *NAT* オブジェクト トラッカー グループ パラメータ

フィールド	説明
[Group Tracker ID]	トラッカーグループの名前を入力します。
[Tracker ID]	グループ化するオブジェクトトラッカーの名前を入力します。

フィールド	説明
基準	[AND] または [OR] を選択します。 [AND] 操作を選択した場合、トラッカーグループの関連付けられた両方のトラッカーがルートがアクティブであると報告した場合、トランスポート インターフェイスのステータスはアクティブであると報告されます。 [OR] は、トラッカーグループの関連付けられたトラッカーのいずれかがルートがアクティブであると報告した場合に、トランスポート インターフェイスのステータスがアクティブとして報告されることを保証します。

8. [Add] をクリックします。
9. [更新（Update）] をクリックします。

Cisco VPN テンプレートを使用して、サービス側 NAT オブジェクトトラッカーを NAT プールに関連付ける

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. [Cisco VPN] テンプレートを編集するには、テンプレート名の横にある [...] をクリックし、[Edit] を選択します。
4. ダイナミックまたはスタティック NAT の NAT プールを設定します。

   ダイナミックまたはスタティック NAT の NAT プールの設定に関する詳細については、「サービス側スタティック NAT の設定」を参照してください。
5. [NAT Direction] フィールドで、スコープを [Default] から [Global] に変更し、ドロップダウンリストから [Inside] を選択します。
6. [Add Object/Object Group Tracker] フィールドに、トラッキングするインターフェイスまたはルートのオブジェクト ID 番号を入力します。
7. [Add] をクリックします。
8. [更新（Update）] をクリックします。

CLI を使用したサービス側 NAT オブジェクトトラッカーの設定

1. 次の例に示すように、NAT プール番号とアクションを含む Cisco Catalyst SD-WAN コントローラ の一元化されたデータポリシーを構成します。

```
policy
 data-policy ssn_policy
  vpn-list ssn_vpn_list
   sequence 10
    match
     destination-ip 192.168.21.0/24
!
    action accept
     count counter_dst_192
     nat pool 1
    !
   !
   sequence 20
    match
     destination-ip 10.11.11.0/27
  !
    action accept
     count counter_dst_10
     nat pool 2
    !
   !
   sequence 101
    match
     source-ip 192.168.11.0/24
     protocol  1
    !
    action accept
     nat pool 1
    !
   !
   default-action accept
  !
 !
 lists
  vpn-list ssn_vpn_list
   vpn 1
  !
  site-list ssn_site_list
   site-id 500
  !
 !
!
apply-policy
 site-list ssn_site_list
  data-policy ssn_policy all
 !
!
```

2. トラッカー名とトラッカー ID を使用して内部スタティック NAT を設定します。

```
Device(config)# ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1
match-in-vrf track 1
```

3. プレフィックス長を使用して内部スタティック NAT プールを設定します。

```
Device(config)# ip nat pool natpool2 10.11.11.0 10.11.11.25 prefix-length 27
```

4. オーバーロードモード、トラッカー名、およびトラッカーIDを使用して、内部スタティック NAT グローバルプールを設定します。

```
Device(config)# ip nat inside source list global-list pool natpool2 vrf 1 match-in-vrf
 overload track 1
```

5. IP ルートの到達可能性をトラッキングします。

```
Device(config)# track 1 ip route 192.168.11.0 255.255.255.0 reachability
Device(config-track)# ip vrf 1
```

（注） ルーティング テーブル エントリがルートに存在し、そのルートがアクセス可能である場合、トラッキング対象オブジェクトはアップ状態にあると見なされます

6. インターフェイスのラインプロトコルの状態を追跡します。

```
Device(confige)# track 1 interface GigabitEthernet5.101 line-protocol
```

CLI アドオンテンプレートを使用したサービス側 NAT オブジェクトトラッカーの設定

はじめる前に

新しいCLIアドオンテンプレートを作成するか、既存のCLIアドオンテンプレートを編集します。

CLI Add-on Feature Templates の詳細については、「CLI Add-on Feature Templates」を参照してください。

CLI アドオンテンプレートを使用したサービス側 NAT オブジェクトトラッカーの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. [Add template] をクリックします。
4. デバイスリストからデバイスを選択します。
5. [OTHER TEMPLATES] の [CLI Add-On Template] をクリックします。
6. [CLI Add-On Template] エリアで、次の例に示すように設定を入力します。

```
track 1 ip route 192.168.11.0 255.255.255.0 reachability
ip vrf 1
ip nat pool natpool1 10.11.11.1 10.11.11.30 prefix-length 24
ip nat inside source static 192.168.11.10 10.11.11.10 vrf 1 match-in-vrf pool natpool1
 track 1
ip nat inside source list global-list pool natpool1 vrf 1 match-in-vrf overload track
 1
```

7. **[Save（保存）]** をクリックします。

   作成した CLI アドオンテンプレートが [CLI Configuration] に表示されます。

8. CLI アドオンテンプレートをデバイスにアタッチします。

サービス側 NAT オブジェクトトラッカーの設定の確認

次のセクションでは、サービス側 NAT オブジェクトトラッカーの設定を確認する方法について説明します。

サービス側 NAT オブジェクトトラッカーの状態の確認

次に、**show track object-id** コマンドの出力例を示します。

```
Device# show track 1
 Track 1
  Interface GigabitEthernet5.101 line-protocol
  Line protocol is Up
    1 change, last change 01:38:57
  Tracked by:
    NAT 0
```

この出力では、`Line protocol is Up (OMP)` は、サービス側オブジェクトトラッカーが稼働していることを示しています。

OMP を介した NAT ルートがルーティングテーブルに追加されていることを確認します。

次に、**show ip route vrf** コマンドの出力例を示します。

```
Device# show ip route vrf 1
Routing Table: 1
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
Gateway of last resort is not set
      10.0.0.0/24 is subnetted, 3 subnets
m        10.11.11.1 [251/0] via 192.168.11.10, 04:03:35, Sdwan-system-intf
m        10.11.11.6 [251/0] via 192.168.13.10, 04:03:35, Sdwan-system-intf
m        10.11.11.30 [251/0] via 192.168.11.21, 04:03:35, Sdwan-system-intf
```

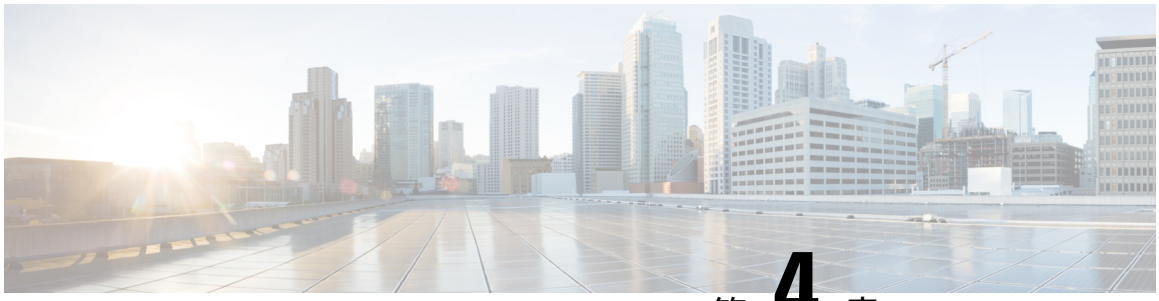
この出力では、`Ni - NAT 内部`が設定されています。

この出力では、`m` で始まる行は、NAT ルートがルーティングテーブルに追加されたことを示しています。

サービス側 NAT オブジェクトトラッカーのモニタリング

Cisco SD-WAN Manager 内で追加または削除された NAT ルートとインターフェイスを監視できます。

1. Cisco SD-WAN Manager のメニューから**[Monitor]** > **[Logs]**の順に選択します。
2. [イベント（Events）] をクリックします。



第 4 章

NAT64 の設定

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

NAT64 の設定

NAT64 設定では、IPv6 および IPv4 ネットワークを接続するために、IPv6 アドレスを IPv4 アドレスに変換できます。

トラフィックの発信は常に、オーバーレイネットワークのトランスポート側（WAN）からサービス側（LAN）に行われます。

NAT64 ダイレクト インターネット アクセス

表 *19 :* 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイス の NAT64 DIA	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b Cisco vManage リリース 19.2.1	NAT64 ダイレクト インターネット アクセス（DIA）機能は、インターネットトラフィックを中央サイトまたはインターネットアクセス用のデータセンターにトンネリングする代わりに、ブランチサイトからインターネットに直接トラフィックのルーティングをサポートします。 NAT64 DIA を使用すると、ブランチサイトの IPv6 クライアントは、データセンターまたはブランチのローカルにある IPv4 エンタープライズアプリケーション サーバーにアクセスできます。IPv6 クライアントは、インターネットを使用してブランチから IPv4 サーバーに直接アクセスすることもできます。

NAT64 DIA に関する情報

NAT64 DIA を使用すると、IPv4 サーバーはリモートブランチまたはデータセンターから IPv6 サーバーにアクセスできます。

NAT64 DIA のトラフィックフローは、LAN から DIA です。

NAT64 DIA の仕組み

1. [Cisco VPN Interface Ethernet] テンプレートを使用して、IPv4 および IPv6 を有効にします。
2. サービス側 VPN である [Cisco VPN] テンプレートに IPv6 ルートを設定します。

   送信元と宛先の IPv6 アドレスが変換されます。
3. NAT IPv4 DIA が設定されているため、インターフェイスが過負荷になり、送信元 IPv4 アドレスが変換されます。宛先 IPv4 アドレスは同じままです。

NAT64 DIA の利点

- 優れたアプリケーション パフォーマンスを実現
- 帯域幅の消費と遅延の削減に貢献

- 帯域幅コストの削減に貢献
- リモートサイトに DIA を提供することで、ブランチオフィスのユーザーエクスペリエンスを向上させます。

NAT64 DIA の制限事項

- NAT64 DIA は、インターフェイス オーバーロードのみを使用します。
- NAT DIA プールまたはループバックは、NAT64 ではサポートされていません。
- OMP への NAT ルートのアドバタイズメントはサポートされていません。

NAT64 DIA ルートの制限事項

- ルーティングテーブルにルートをインストールするには、次の NAT64 DIA ルートを使用できます。

  /128 プレフィックスの NAT64 DIA ルートの例：

  ```
  nat64 route vrf 4 64:FF9B::1E00:102/128 global
  ```

  /96 プレフィックスの NAT64 DIA ルートの例：

  ```
  nat64 route vrf 4 64:FF9B::/96 global
  ```

- ルーティングテーブルにルートをインストールするために、次の NAT64 DIA ルート設定を使用することはできません。

  ```
  nat64 route vrf 4 64:ff9b::/64 global
  nat64 route vrf 4 ::0/0 global
  ```

NAT64 DIA と DIA ルートの設定

NAT64 DIA を有効にするためのワークフロー

1. IPv4 と IPv6 の両方で、[Cisco VPN Interface Ethernet] テンプレートを使用して NAT64 を有効にします。

   （注） NAT64 IPv4 DIA は、デフォルトでインターフェイスの過負荷を使用します。

   IPv6 DIA の NAT64 を構成する場合、インターフェイスの過負荷は既に設定されています。

   [Cisco VPN Interface Ethernet] テンプレートは、トランスポート インターフェイスです。

2. サービス VPN である [Cisco VPN] テンプレートを使用して、NAT64 DIA IPv6 ルートを設定します。

NAT64 DIA の設定

インターフェイスの過負荷での NAT64 DIA の設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Cisco VPN Interface Ethernet] テンプレートを編集するには、**...** をクリックし、[Edit] をクリックします。
4. [Interface Name] フィールドで、インターフェイスを選択します。
5. [NAT] をクリックし、[IPv4] を選択します。
   1. スコープを [Default] から [Global] に変更します。
   2. [オン] をクリックして、IPv4 の NAT を有効にします。
   1. [NAT Type] フィールドで、インターフェイス過負荷の [Interface] をクリックします。

      [Interface] オプションが IPv4 に対して [On] に設定されていることを確認します。

表 *20 : NAT IPv4* パラメータ

パラメータ名	説明
NAT	NAT 変換を使用するかどうかを指定します。 デフォルトは [オフ（Off）] です。
NAT Type	IPv4 の NAT 変換タイプを指定します。 使用可能なオプションには、[Interface]、[Pool]、および [Loopback] が含まれます。 デフォルトは [Interface] オプションです。[Interface] オプションは、NAT64 でサポートされています。

パラメータ名	説明
[UDP Timeout]	UDP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 範囲：1 ～ 536870 秒 デフォルト：300 秒（5 分） （注） Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a および Cisco vManage リリース 20.6.1 以降、NAT64 のデフォルトの [UDP Timeout] 値は 300 秒（5 分）に変更されました。
[TCP Timeout]	TCP セッションを介した NAT 変換がいつタイムアウトするかを指定します。 タイムアウト値を入力します デフォルト：3600 秒（1 時間） （注） Cisco IOS XE Catalyst SD-WAN リリース 17.6.1a および Cisco vManage リリース 20.6.1 以降、NAT64 のデフォルトの [TCP Timeout] 値は 3600 秒（1 時間）に変更されました。

6. ステップ 5 を繰り返しますが、[IPv6] を選択して IPv6 の NAT を有効にします。

（注） NAT64 DIA に IPv4 と IPv6 の両方を設定します。

7. [NAT Selection] フィールドで、[NAT64] をクリックして NAT64 を有効にします。

（注） IPv6 の場合、インターフェイスの過負荷はすでに設定されています。

表 *21 : NAT IPv6* パラメータ

パラメータ名	説明
NAT	NAT変換を使用するかどうかを指定します。 デフォルトは [オフ（Off）] です。

パラメータ名	説明
[NAT Selection]	NAT64 を指定します。 デフォルトは [NAT66] オプションです。

8. [更新（Update）] をクリックします。

NAT64 DIA ルートの設定

Cisco VPN テンプレートを使用した NAT64 DIA ルートの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Cisco VPN] 機能テンプレートを編集するには、**...** をクリックし、[Edit] をクリックします。

（注） サービス側 VPN である [Cisco VPN] 機能テンプレートで IPv6 DIA ルートを設定します。

4. [IPv6 Route] をクリックします。
5. [New IPv6 Route] をクリックします。
6. [Prefix] フィールドに、よく知られたプレフィックス [64:FF9B::/96] を入力します。
7. [Gateway] フィールドで、[VPN] をクリックします。
8. [Enable VPN] フィールドで、スコープを [Default] から [Global] に変更し、[On] をクリックして VPN を有効にします。
9. [NAT] フィールドで、[NAT64] をクリックします。
10. [更新（Update）] をクリックします。

CLI を使用した NAT64 DIA ルートの設定

例：NAT64 DIA ルートの設定

```
Device(config)# nat64 route vrf 4 64:FF9B::1E00:102/128 global
```

NAT64 DIA ルート設定の確認

例 1

以下は、サービス VPN 用の **show ipv6 route vrf** コマンドからの出力例です。

```
Device# show ipv6 route vrf 4
IPv6 Routing Table - 4 - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP
m   64:FF9B::/96 [251/0]
     via 172.16.255.15%default, Sdwan-system-intf%default
```

この例では、`64:FF9B::/96` は、IPv6 を IPv4 アドレスに変換するための NAT64 の既知のプレフィックスです。

例 2

NAT64 DIA がトランスポート VPN で設定されているため、トランスポート VPN のルーティングテーブルは次のように表示されます。

```
Device# show ipv6 route
IPv6 Routing Table - default - 2 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP, Nd - Nat-Route DIA
S   64:FF9B::/96 [1/0]
```

NAT64 DIA の設定例

この例は、NAT64 DIA の設定を示しています。

```
interface GigabitEthernet1
          no shutdown
          arp timeout 1200
          ip address 10.1.15.15 10.255.255.255
          no ip redirects
          ip mtu    1500
          ip nat outside
          load-interval 30
          mtu           1500
          negotiation auto
          nat64 enable
          !
          nat64 v6v4 list nat64-global-list interface GigabitEthernet1 overload
          !
```

```
        ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet1
overload
```

（注） GigabitEthernet1 は、トランスポート VPN インターフェイスです。

サービス側 NAT64

表 *22 :* 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE Catalyst SD-WAN デバイス のサービス側 NAT64	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b Cisco vManage リリース 19.2.1	サービス側ネットワークアドレス変換（NAT）64 機能は、送信元 IPv6 アドレスを NAT プール内の使用可能な IPv4 アドレスに変換します。宛先 IPv6 アドレスは、IPv4 組み込み IPv6 アドレスであるため、宛先 IPv6 アドレスはサーバーの実際の IPv4 アドレスに変換されます。 サービス側 NAT64 により、IPv4 サーバーは IPv6 クライアントと通信できます。

サービス側 NAT64 に関する情報

IPv4 パブリックアドレス空間が減少し、よりルーティング可能なアドレスに対する必要性が高まる中、サービスプロバイダーと企業は IPv6 ネットワークの構築と展開を続けています。IPv4 インターネットはしばらく存続するため、IPv4 ネットワークと IPv6 ネットワーク間の通信は、シームレスなエンドユーザー エクスペリエンスにとって重要な要件です。

NAT IPv6 to IPv4（NAT64）テクノロジーは、IPv6 と IPv4 ネットワーク間の通信を容易にします。

サービス側 NAT64 機能は、送信側 IPv6 アドレスを NAT プール内の使用可能な IPv4 アドレスに変換します。宛先 IPv6 アドレスは、IPv4 組み込み IPv6 アドレスであるため、宛先 IPv6 アドレスはサーバーの実際の IPv4 アドレスに変換されます。

Cisco IOS XE Catalyst SD-WAN デバイス は、IPv6 アドレスを IPv4 アドレスに、IPv4 アドレスを IPv6 アドレスに変換するためにステートフル NAT64 を使用します。NAT オーバーロードを使用したステートフル NAT64 は、IPv4 アドレスと IPv6 アドレス間の 1:*n* マッピングを提供します。

サービス側 NAT64 の仕組み

1. IPv6 クライアントが IPv4 サーバーへの接続を試みます。

2. IPv6 クライアントは、IPv6 AAAA レコード DNS クエリを作成します。これは、IPv4 アドレスに対する IPv6 クエリです。

   DNS64 サーバーは、IPv4 に埋め込まれた IPv6 アドレスで応答します。

   例：

   ```
   64:ff9b::c000:0201
   ```

   これは、NAT64 の既知のプレフィックス（WKP）である `64:FF9B::/96` を使用します。WKP は、アドレスファミリ間のアルゴリズムマッピングに使用されます。

   IPv4 埋め込み IPv6 アドレスは、可変長プレフィックス、埋め込み IPv4 アドレス、および可変長サフィックスで設定されます。最後の 32 ビットは、元の IPv4 アドレスの 16 進表現で、この例では 192.0.2.1 です。

3. IPv6 クライアントは、IPv4 サーバーへの接続を試みます。

4. IPv6 から IPv4 への変換が実行されます。

   送信元 IPv6 アドレスは、プール内の使用可能な IPv4 アドレスの 1 つに変換されます。

   宛先 IPv6 アドレスは、IPv4 組み込み IPv6 アドレスであるため、宛先 IPv6 アドレスはサーバーの実際の IPv4 アドレスに変換されます。

サービス側 NAT64 の利点

- インターネット上の IPv4 サーバーを使用したサービス VPN 内の IPv6 クライアント間の通信をサポート
- IPv6 および IPv4 ネットワークへのデュアルアクセスを維持するために、IPv6 アドレスから IPv4 アドレスへの変換を提供します。
- ステートフル NAT64 を使用する場合、既存の IPv4 ネットワーク インフラストラクチャをほとんどまたはまったく変更する必要がない
- IPv4 インターネットサービスにアクセスする IPv6 ユーザーにシームレスなインターネット エクスペリエンスを提供し、IPv4 のビジネス継続性を維持します。
- データポリシーを設定することなく、NAT64 の設定をサポート

サービス側 NAT64 の使用例

サポートされているトラフィックフローは、リモートサイト、データセンター、または別のブランチサイトにある IPv6 クライアントから、ローカル LAN 上の IPv4 クライアントまたはサーバーまでです。

（注） トラフィックの発信は常に、オーバーレイネットワークのトランスポート側（WAN）からサービス側（LAN）に行われます。

サービス側 NAT64 の前提条件

- ドメイン ネーム システム（DNS）トラフィックを機能させるには、別の DNS64 をインストールして稼働させる必要があります。

サービス側 NAT64 の制限事項

- トラフィックは常にリモートブランチサイトから発信され、ローカル LAN 上の IPv4 サーバーにアクセスする必要があります。
- トラフィックは、IPv4 サーバーからデータセンター内の IPv6 クライアントまたはリモートブランチサイトに発信できません。

サービス側 NAT64 の IPv4 アドレス制限事項

- 使用可能な IPv4 宛先 IP アドレスの詳細については、導入ガイドライン、RFC 6052、セクション 3.1 を参照してください。
- RFC 5735 のセクション 3 の展開ガイドラインに記載されているような、非グローバル IPv4 アドレスを表すために、既知のプレフィックス（WKP）を使用することはできません。

  たとえば、次の IPv4 プレフィックスは許可されていません。

  - 0.0.0.0/8
  - 10.0.0.0/8
  - 127.0.0.0/8
  - 169.254.0.0/16

- サービス側（LAN）でプライベート IPv4 アドレス範囲を使用することはできません。

サービス側 NAT64 の設定

次のセクションでは、サービス側 NAT64 の設定に関する情報を提供します。

機能テンプレートを使用したサービス側 NAT64 の有効化

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Cisco VPN Interface Ethernet] テンプレートを編集するには、**...** をクリックし、[Edit] をクリックします。

（注） [Cisco VPN Interface Ethernet] テンプレートは、サービス側のインターフェイスです。

4. [NAT] をクリックし、NAT64 に [IPv6] を選択します。
5. スコープを [Default] から [Global] に変更します。
6. [NAT64] フィールドで、[On] をクリックして NAT64 を有効にします。
7. [更新（Update）] をクリックします。

サービス側 NAT64 プールの設定

はじめる前に

1. NAT64 IPv4 プールを設定する前に、[Cisco VPN Interface Ethernet] テンプレートを使用してサービス側の NAT64 を有効にしておく必要があります。
2. 新しい [Cisco VPN] 機能を作成するか、既存の [Cisco VPN] 機能を編集します。[Cisco VPN] 機能テンプレートは、NAT64 を設定するサービス側 VPN に対応します。

サービス側 NAT64 プールの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Cisco VPN] テンプレートを編集するには、テンプレートの横にある **...** をクリックし、[Edit] をクリックします。
4. [NAT] をクリックします。
5. [NAT64 v4 Pool] をクリックします。
6. [New NAT64 v4 Pool] をクリックします。
7. [NAT64 Pool name] フィールドで、プール名を指定します。

（注） プール名には番号を指定する必要があります。

8. [NAT 64 v4 Pool Range Start] フィールドで、プール範囲の開始の IPv4 アドレスを指定します。
9. [NAT 64 v4 Pool End Start]フィールドで、プール範囲の終了の IPv4 アドレスを指定します。
10. ドロップダウンリストから [Global] を選択します。
11. [On] をクリックして、[NAT 64 Overload] を有効にします。

（注） [NAT 64 Overload] はデフォルトで [Off] に設定されています。

12. [Add] をクリックします。
13. [Update] をクリックして、設定をデバイスにプッシュします。

CLI を使用したサービス側 NAT64 の設定

表 *23 :* 機能の履歴

機能名	リリース情報	説明
NAT64 デバイスの IPv6 サポート	Cisco IOS XE Catalyst SD-WAN リリース 16.12.1b	この機能は、Cisco IOS XE Catalyst SD-WAN デバイス での IPv4 と IPv6 間の通信を容易にする NAT64 をサポートします。

CLI を使用したサービス側 NAT64 の有効化

このセクションでは、サービス側の NAT64 を有効にするための CLI 設定の例を示します。

LAN インターフェイスでサービス側の NAT64 を有効にします。これは、Cisco SD-WAN Manager 上の [Service VPN] テンプレートに相当します。

IPv4 アプリケーション サーバーはローカル LAN サイトにあり、IPv6 クライアントはデータセンターまたは LAN のリモートサイトにあります。

```
Device# interface GigabitEthernet 5.104
nat64 enable
```

CLI を使用したサービス側 NAT64 プールの設定

このセクションでは、サービス側 NAT64 プールを設定するための CLI 設定の例を示します。

```
Device# nat64 v4 pool pool10 192.0.2.0 192.0.2.254
nat64 v6v4 list global-list_nat64 pool pool10 vrf 4 overload
```

サービス側 NAT64 の設定の確認

例：指定されたデバイスのルーティングテーブルに表示される内容

次に、**show ipv6 route vrf** コマンドの出力例を示します。

```
Device# show ipv6 route vrf 4
IPv6 Routing Table - 4 - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP, Nd - Nat-Route DIA
Nd  64:FF9B::/96 [6/0]
     via Null0%default, directly connected
m   2001:DB8:AA:A::/64 [251/0]
     via 172.16.255.16%default, Sdwan-system-intf%default
C   2001:DB8:BB:A::/64 [0/0]
     via GigabitEthernet5.104, directly connected
L   2001:DB8:BB:A::1/128 [0/0]
     via GigabitEthernet5.104, receive
L   FF00::/8 [0/0]
     via Null0, receive
```

この例では、NAT64 の既知のプレフィックス、`64:FF9B::/96` がサービス VPN の IPv6 ルーティングテーブルに表示されます。

次に、**show ip route vrf 4** コマンドの出力例を示します。

```
Device# show ip route vrf 4
Routing Table: 4
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
       n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       H - NHRP, G - NHRP registered, g - NHRP registration summary
       o - ODR, P - periodic downloaded static route, l - LISP
       a - application route
       + - replicated route, % - next hop override, p - overrides from PfR
       & - replicated local route overrides by connected
```

NAT64 IPv4 プールアドレスは、サービス VPN の IPv4 ルーティングテーブルの `nat inside` ルートとしてルーティングテーブルにインストールされます。

例：OMP のルーティングテーブルに表示される内容

次に、**show ipv6 route vrf** コマンドの出力例を示します。

```
Device# show ipv6 route vrf 4
IPv6 Routing Table - 4 - 5 entries
Codes: C - Connected, L - Local, S - Static, U - Per-user Static route
       B - BGP, R - RIP, H - NHRP, I1 - ISIS L1
       I2 - ISIS L2, IA - ISIS interarea, IS - ISIS summary, D - EIGRP
```

```
       EX - EIGRP external, ND - ND Default, NDp - ND Prefix, DCE - Destination
       NDr - Redirect, RL - RPL, O - OSPF Intra, OI - OSPF Inter
       OE1 - OSPF ext 1, OE2 - OSPF ext 2, ON1 - OSPF NSSA ext 1
       ON2 - OSPF NSSA ext 2, la - LISP alt, lr - LISP site-registrations
       ld - LISP dyn-eid, lA - LISP away, le - LISP extranet-policy
       lp - LISP publications, a - Application, m - OMP
m   64:FF9B::/96 [251/0]
     via 172.16.255.15%default, Sdwan-system-intf%default
C   2001:DB8:AA:A::/64 [0/0]
     via GigabitEthernet5.104, directly connected
L   2001:DB8:AA:A::1/128 [0/0]
     via GigabitEthernet5.104, receive
m   2001:DB8:BB:A::/64 [251/0]
     via 172.16.255.15%default, Sdwan-system-intf%default
L   FF00::/8 [0/0]
     via Null0, receive
```

この例では、NAT64 の既知のプレフィックスである `64:FF9B::/96` がオーバーレイ管理プロトコル（OMP）ルートとして受信されます。

NAT64 IPv4 プールアドレスは、OMP ルートとして受信されます。

サービス側 NAT64 の設定例

この例は、サービス側 NAT64 の設定を示しています。

```
nat64 v4 pool 1-4 192.0.2.0 192.0.2.254
nat64 v6v4 list nat64-list pool 1-4 vrf 4 overload
!
interface GigabitEthernet5.104
 encapsulation dot1Q 104
 vrf forwarding 4
 ip address 10.1.19.15 10.255.255.255
 ip mtu 1496
 ip ospf network broadcast
 ip ospf 4 area 0
 nat64 enable
end
```

この例は、NAT64 プールの設定を示しています。

```
nat64 v4 pool 1-4 192.0.2.0 192.0.2.254
nat64 v6v4 list nat64-list pool 1-4 vrf 4 overload
!
interface GigabitEthernet5.104
 encapsulation dot1Q 104
 vrf forwarding 4
 ip address 10.1.19.15 10.255.255.255
 ip mtu 1496
 ip ospf network broadcast
 ip ospf 4 area 0
 nat64 enable
end
```

NAT64 によるカプセル化を使用したアドレスとポートのマッピング

表 *24 :* 機能の履歴

機能名	リリース情報	説明
NAT64 によるカプセル化（MAP-E）を使用したアドレスとポートのマッピング	Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a	この機能は、IPv6 のみのネットワークを使用しているときに、IPv4 クライアントが IPv4 サーバーにアクセスするためのサポートを提供します。IPv4 トラフィックは、IPv6 トンネルを介してインターネットにルーティングされます。 この機能を使用すると、IP カプセル化を使用して IPv6 ネットワーク上で IPv4 パケットを転送するための MAP-E ドメインおよび MAP-E パラメータを設定できます。MAP-E カスタマーエッジ（CE）デバイスの起動時、または IPv4 アドレスが変更されるときに、このデバイスは HTTP を使用して MAP-E ルールサーバーから MAP-E パラメータを自動的に取得します。 この機能を使用すると、IP カプセル化を使用して IPv6 ネットワーク上で IPv4 パケットを転送するための MAP-E ドメインおよび MAP-E パラメータを設定できます。MAP-E カスタマーエッジ（CE）デバイスの起動時、または IPv4 アドレスが変更されるときに、このデバイスは HTTP を使用して MAP-E ルールサーバーから MAP-E パラメータを自動的に取得します。

NAT64 を使用した MAP-E に関する情報

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a

Mapping of Address and Port with Encapsulation（MAP-E）は Internet Engineering Task Force（IETF）のドラフトであり、カプセル化を使用して IPv6 専用ネットワーク上で IPV4 パケットを転送するメカニズムについて説明しています。

MAP-E ドメイン内では、IPv6 専用ネットワークを介してカプセル化して転送することで、IPv4 パケットは MAP-E CE デバイスとパブリック IPv4 インターネットとの間で交換されます。

NAT64 機能を備えた MAP-E は、次の設定をサポートします。

- 共有 IPv4 の設定

  MAP-E は、MAP-E ドメイン内の複数の MAP-E CE デバイスが単一の IPv4 アドレスを共有できるようにします。同じ IPv4 アドレスを持つ各 MAP-E CE デバイスは、異なる TCP または UDP ポートを使用する必要があります。MAP-E は、IPv6 専用ネットワークで共有 IPv4 アドレスを使用して IPv4 接続を提供します。

- 固定 IPv4 の設定

  固定 IPv4 設定では、1 つの MAP-E CE デバイスが固定 IPv4 アドレスを使用します。

NAT64 を使用した MAP-E 設定のコンポーネント

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a

MAP-E ドメインを使用したアドレスとポートの各マッピングでは、異なるマッピングルールが使用されます。MAP-E 設定には、次のものが含まれます。

- Basic mapping rule（BMR）

  BMR は MAP-E IPv6 アドレス またはプレフィックスを設定します。IPv6 プレフィックスごとに設定できる BMR は 1 つだけです。MAP-E CE デバイスは、BMR を使用して、IPv4 アドレス、IPv4 プレフィックス、または IPv6 プレフィックスからの共有 IPv4 アドレスで自身を設定します。IPv4 送信元アドレスと送信元ポートが IPv6 アドレスまたはプレフィックスにマップされている使用例では、パケットの転送に BMR を使用することもできます。すべての MAP-E CE は、BMR でプロビジョニングする必要があります。

  ポートパラメータとともに BMR IPv6 プレフィックスがトンネルの送信元アドレスとして使用されます。

- 単一のデフォルト マッピング ルール（DMR）

  インターフェイスアドレスと一致する DMR プレフィックスはホストとして認識され、プレフィックス長が 128 の DMR プレフィックスはトンネルの送信元アドレスとして認識されます。ボーダールータの IPv6 アドレスは、トンネルの宛先アドレスです。

- ポートセットID（PSID）

  PSID は、使用が許可されているポートを識別します。

  ボーダールータは、PSID とポートセットが一致するかどうかを確認します。ポートセット ID とポート セットが一致する場合、DMR は IPv6 パケットのパケット宛先に一致します。BMR に基づき、ボーダールータは IPv4 送信元アドレスを作成し、IPv6 宛先アドレスから IPv4 宛先アドレスを抽出します。IPv6 パケットは、NAT64 の IPv6 から IPv4 変換エンジンを使用して、IPv6 パケットから IPv4 パケットを作成します。

MAP-E CE デバイスの起動時または IPv6 アドレスが変更されるたびに、HTTP を使用して MAP-E ルールサーバーから MAP-E パラメータを自動的に設定します。

MAP-E ドメインおよびMAP-Eパラメータを設定するには、**nat64 provisioning** コマンドを使用します。MAP-E ドメインおよび MAP-E パラメータの設定の詳細については、『Cisco IOS XE SD-WAN Qualified Command Reference Guide』を参照してください。

MAP-E ルールの REST API 仕様については、『IP Addressing: NAT Configuration Guide』を参照してください。

NAT64 を使用した MAP-E の利点

- IPv6 のみのネットワーク上で IPv4 トラフィックフローをサポートします。
- ボーダールータに追加のハードウェアを必要とせずに、低遅延で効率的なトラフィック配信をサポートします。
- IPv6 に移行するための使いやすくスケーラブルなソリューションをサポートします。

NAT64 を使用した MAP-E の制限事項

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a

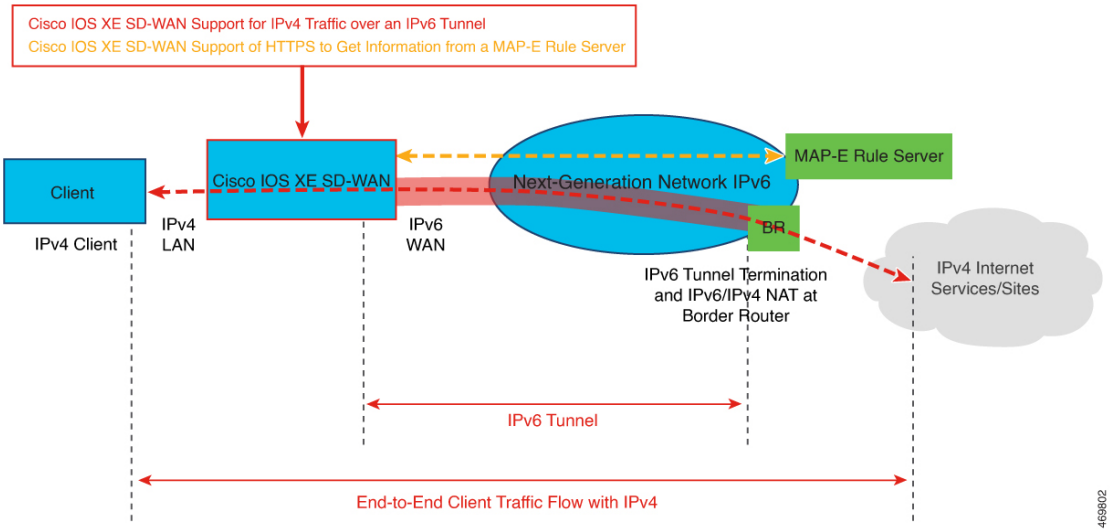
- MAP-E CE デバイスごとに 1 つの BMR をサポートします。アドレスとポートの変換ごとに異なるマッピングルールを設定します。
- 64 の BMR プレフィックス長、フラグメンテーション、およびローカルパケット生成はサポートされていません。

NAT64 を使用した MAP-E のワークフロー

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a

次の図は、MAP-E で IPv6 のみのネットワークを使用する場合に、IPv4 クライアントが IPv4 サーバーに到達するためのエンドツーエンドのクライアント トラフィック フローを示しています。

図 *8 : NAT64* を使用した *MAP-E* のワークフロー

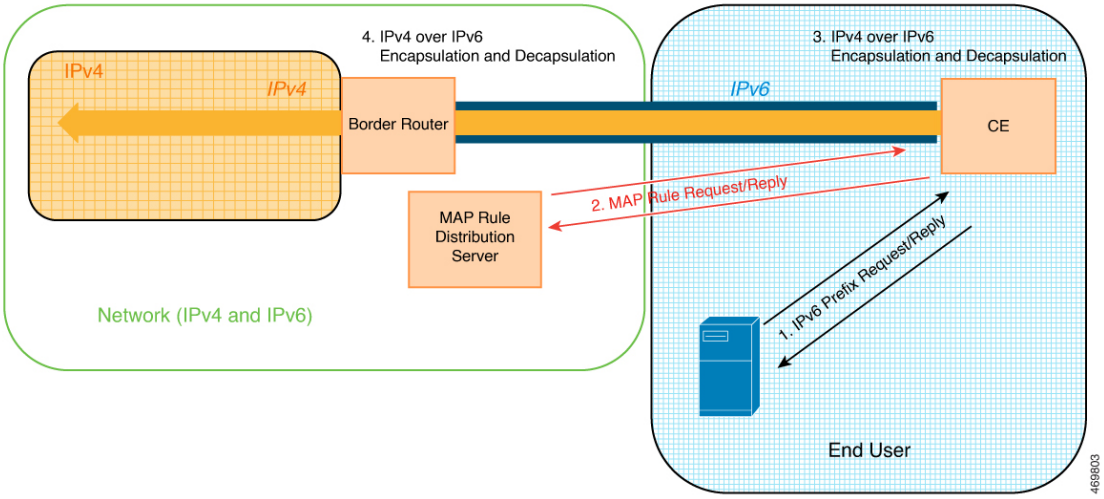


MAP-E CE デバイスと MAP-E ルールサーバー間の MAP-E 相互作用

1. MAP-E ルールサーバーは、IPv6 のみのネットワークから IPv6 プレフィックスを取得します。
2. MAP-E CE デバイスは、HTTP 要求を MAP-E ルールサーバーに送信し、応答を受信します。

   MAP-E は、Cisco IOS XE Catalyst SD-WAN デバイス が MAP-E CE デバイスとして機能できるようにします。
3. MAP-E ルールに従って、MAP-E CE デバイスは着信 IPv4 パケットの変換を実行します。
4. MAP-E CE デバイスは IPv4 パケットを IPv6 パケットにカプセル化し、IPv6 パケットをボーダールータに送信します。
5. エンコードされた IPv6 パケットを受信すると、IPv6 パケットは MAP-E ルールに従ってボーダールータによってカプセル化が解除され、IPv6 トラフィックは IPv4 パブリックインターネットにルーティングされます。

図 *9 : MAP-E* ワークフロー



CLI テンプレートを使用した NAT64 での MAP-E の設定

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a

CLI テンプレートの使用の詳細については、CLI アドオン機能テンプレートおよび CLI テンプレートを参照してください。

（注） デフォルトでは、CLI テンプレートはグローバル コンフィギュレーション モードでコマンドを実行します。

このセクションでは、MAP-E ドメインと MAP-E パラメータを設定するための CLI 設定の例を示します。

1. NAT64 フラグメンテトヘッダーを無効にします。

```
nat64 settings fragmentation header disable
```

2. NAT64 DIA ルートを設定します。

```
nat64 route ip-address interface-type-number
```

詳細については、「NAT64 DIA ルートの設定」を参照してください。

3. NAT64 MAP-E ドメインを指定し、MAP-E コンフィギュレーション モードを開始します。

```
nat64 provisioning mode jp01
```

4. ユーザー名とパスワードを使用してアドレス解決サーバーを設定します。

```
address-resolution-server http://ipv6-prefix/directory-path
address-resolution-server 6 username encypted-user-name
address-resolution-server 6 password encypted-password
```

アドレス解決サーバーのユーザー名とパスワードを暗号化するための暗号化タイプ（2 または 6）を指定することもできます。

5. MAP-E ルールサーバーを設定します。

```
rule-server http://admin:admin@ipv6-prefix//directory-path
```

ルールサーバーの URL を暗号化するための暗号化タイプ（2 または 6）を指定することもできます。

6. （オプション） HTTP サーバーからの応答の待機時間を秒単位で設定します。

```
rule-server request wait-time value-seconds
```

7. ホスト名を設定します。

```
hostname hostname
```

ホスト名は MAP-E ルールサーバーのものです。ホスト名を上書きする場合は、新しいホスト名を指定できます。

8. トンネルインターフェイスを設定します。

```
tunnel interface Tunnelnumber
tunnel source interface-type-interface-number
```

（注） 固定 IPv4 設定専用のトンネルインターフェイスとトンネル送信元を設定します。

9. サービスプレフィックスを設定します。

```
service-prefix ipv6-prefix
```

（注） MAP-E ルールサーバーから返される MAP-E ルールの IPv6 プレフィックスは、MAP-E CE デバイスで設定された IPv6 サービスプレフィックスと一致する必要があります。

（注） 固定 IPv4 設定または共有 IPv4 設定のいずれかのサービスプレフィックスを設定します。

MAP-E ドメインとパラメータを設定するための完全な設定例を次に示します。

```
nat64 settings fragmentation header disable
nat64 settings v4 tos ignore
interface GigabitEthernet1
!
nat64 settings mtu minimum 1500
nat64 provisioning mode jp01
 address-resolution-server http://2001:db8:b000:0:fe7f:6ee7:33db:5013/nic/update
 address-resolution-server password encypted-password
 address-resolution-server username encypted-username
 rule-server http://admin:admin@2001:DB8:A000::1//mape-rule.json
 rule-server request wait-time 180
 hostname hostname
```

```
 tunnel interface Tunnel1
 tunnel source GigabitEthernet2
 service-prefix 2001:DB8:b800::/48
!
nat64 route 0.0.0.0/0 GigabitEthernet1
```

NAT64 設定による MAP-E の確認

サポート対象の最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.10.1a

次に、**show nat64 map-e** コマンドの出力例を示します。

```
Device# show nat64 map-e
MAP-E Domain 9126
   Mode MAP
   Border-relay-address
      Ip-v6-address 2001:DB8::9
   Basic-mapping-rule
      Ip-v6-prefix 2001:DB8:B001:80::/60
      Ip-v4-prefix 10.1.1.0/24
      Port-parameters
         Share-ratio 4   Contiguous-ports 256   Start-port 1024
         Share-ratio-bits 2   Contiguous-ports-bits 8   Port-offset-bits 6
      Port-set-id 0
```

上記の出力は、ポートが MAP-E CE デバイス全体で共有されるため、共有 IPv4 アドレス設定の例です。出力には、MAP-E ルールサーバーから返された MAP-E パラメータが表示されます。

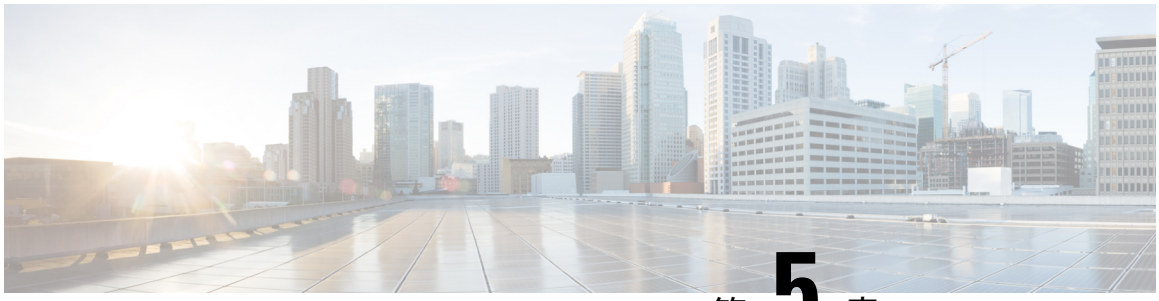
次に、**show nat64 statistics** コマンドの出力例を示します。

```
Device# show nat64 statistics
NAT64 Statistics

Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Sessions found: 0
Sessions created: 0
Expired translations: 0
Global Stats:
   Packets translated (IPv4 -> IPv6)
      Stateless: 0
      Stateful: 0
      nat46: 0
      MAP-T: 0
      MAP-E: 5
   Packets translated (IPv6 -> IPv4)
      Stateless: 0
      Stateful: 0
      nat46: 0
      MAP-T: 0
      MAP-E: 4

Interface Statistics
   GigabitEthernet0/0/0 (IPv4 not configured, IPv6 configured):
      Packets translated (IPv4 -> IPv6)
         Stateless: 0
         Stateful: 0
         nat46: 0
         MAP-T: 0
         MAP-E: 0
      Packets translated (IPv6 -> IPv4)
         Stateless: 0
```

```
         Stateful: 0
         nat46: 0
         MAP-T: 0
         MAP-E: 4
      Packets dropped: 0
   GigabitEthernet0/0/1 (IPv4 configured, IPv6 not configured):
      Packets translated (IPv4 -> IPv6)
         Stateless: 0
         Stateful: 0
         nat46: 0
         MAP-T: 0
         MAP-E: 5
      Packets translated (IPv6 -> IPv4)
         Stateless: 0
         Stateful: 0
         nat46: 0
         MAP-T: 0
         MAP-E: 0
      Packets dropped: 0
Dynamic Mapping Statistics
   v6v4
Limit Statistics
```



第 5 章

NAT66 の設定

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

NAT66 の設定

NAT66 の設定

表 *25 :* 機能の履歴

機能名	リリース情報	説明
NAT66 DIA のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a Cisco vManage リリース 20.7.1	IPv6 から IPv6 へのネットワークアドレス変換（NAT66）ダイレクトインターネットアクセス（DIA）機能により、IPv6 デバイスは、IPv6 パケットヘッダー内の内部送信元アドレスプレフィックスを外部送信元アドレスプレフィックスに変換できます。 NAT66 DIA を使用すると、ローカル IPv6 インターネットトラフィックを、トランスポート VPN（VPN 0）を介してサービス側 VPN（VPN 1）からインターネットに直接送信することができます。 NAT66 DIA は、Cisco SD-WAN Manager、CLI、またはデバイス CLI テンプレートを使用して設定できます。 この機能では、新しい CLI コマンドが導入されています。新しい NAT コマンドに関する詳細については、『Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide』を参照してください。
NAT66 DIA の複数の WAN リンクのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a Cisco Catalyst SD-WAN Manager リリース 20.12.1	複数の WAN リンクを使用してローカル IPv6 トラフィックをインターネットに直接出力するように NAT66 を設定できます。
SLAAC を使用した WAN インターフェイスでの IPv6 アドレスの自動設定	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a Cisco Catalyst SD-WAN Manager リリース 20.13.1	ルータアドバタイズメント（RA）プレフィックスを使用して、NAT66 プレフィックス変換用の IPv6 アドレスを自動的に割り当てることで、ステートレスアドレス自動設定（SLAAC）を設定できます。

機能名	リリース情報	説明
フロースティッキネスのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a Cisco Catalyst SD-WAN Manager リリース 20.13.1	フロースティッキネスは、NAT パスのフローレベルの状態を記録し、NAT パスの変更によってアプリケーションフローがリセットされないようにします。ディープパケットインスペクション（DPI）で最初のパケット一致が失敗すると、エッジルータは、この不明なアプリケーションの最初のフローが元のパスに固定されるようにし、いくつかのパケットの後に DPI エンジンによってパケット一致が認識されると、ポリシーをバイパスしてパスを変更します。
NAT66 DIA での一元管理型データポリシーのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a Cisco Catalyst SD-WAN Manager リリース 20.13.1	**nat use-vpn 0** コマンドを使用して一元管理型データポリシーを設定できます。これにより、ポリシー一致基準に基づいて、送信元 IP が変換された後に、一致するトラフィックが VPN 0 に送信されます。 この機能は、サービスおよびトンネルからサポートされます。フォールバックオプションは、DIA ルートが使用できない場合に、トラフィックがルーティングにフォールバックし、オーバーレイパスを使用するようにします。
NAT66 DIA ルートの再配布のサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a Cisco Catalyst SD-WAN Manager リリース 20.14.1	BGP または OSPFv3 プロトコルへの NAT66 DIA ルートの再配布を設定できます。
NAT66 DIA ステータスイベントのサポート。	Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a Cisco Catalyst SD-WAN Manager リリース 20.14.1	Cisco SD-WAN Manager ログで NAT DIA ステータスをモニターできます。**nat-update** と呼ばれる新しいイベントによって、[Events] ページに NAT DIA のステータスが表示されます。
NAT66 DIA による Point-to-Point Protocol（PPP）ダイヤラインターフェイスのサポート	Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a Cisco Catalyst SD-WAN Manager リリース 20.14.1	この機能により、PPP over Ethernet（PPPoE）と PPP over Asynchronous Transfer Mode（PPPoA）の 2 種類の PPP ダイヤラインターフェイスのサポートが追加されます。 この機能を使用すると、IPv6 サービスおよびサイトにアクセスするための PPP ダイヤラインターフェイスを設定できます。

NAT66 DIA に関する情報

IPv6 から IPv6 へのネットワークプレフィックス変換（NPTv6）は、IPv6 アドレスプレフィックスを別の IPv6 アドレスプレフィックスに変換するメカニズムです。使用されるアドレス変換方式は、IPv6 から IPv6 へのネットワークアドレス変換（NAT66）です。NAT66 機能をサポートするデバイスは、NAT66 トランスレータと呼ばれます。NAT66 トランスレータは、送信元と宛先のアドレス変換機能を提供します。

（注） NPTv6 機能は、Cisco IOS XE Catalyst SD-WAN リリース 17.7.1a の Cisco Catalyst SD-WAN に導入される前に、Cisco IOS XE プラットフォームですでに利用可能でした。詳細については、『*IP Addressing: NAT Configuration Guide*』を参照してください。

NAT66 DIA を使用すると、IPv6 環境であるネットワークから別のネットワークにパケットをリダイレクトまたは転送できます。NAT66 DIA は、内部ネットワークと外部ネットワーク内のアドレス間に 1:1 の関係を持つアルゴリズム変換機能を提供します。異なるネットワークを相互接続し、マルチホーミング、負荷分散、およびピアツーピアネットワークをサポートできます。

NAT66 DIA は、64 ビットを超えるプレフィックスとスタティック IPv6 ホスト間の変換をサポートします。IPv6 アドレスのプレフィックス部分のみが変換されます。

（注） IPv6アドレスで Cisco SD-WAN Manager にアクセスする場合は、URL にポート番号 8443 を指定してください。

例：

```
https://[cisco-vmanage IPv6-address]:8443/
```

NAT66 DIA フローのスティッキネス

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a。

NAT66 DIA がアプリケーション一致の一元管理型データポリシーで設定されている場合、パスの変更により、NAT66 DIA ポリシーの対象となるアプリケーションフローがリセットされる可能性があります。たとえば、アプリケーションリストに一致するデータポリシーがあり、アクションが NAT66 DIA である場合、最初のいくつかのパケットはディープ パケット インスペクション（DPI）によって識別されない可能性があります。したがって、NAT66 DIA アプリケーションポリシーに一致しないパケットは、Cisco Catalyst SD-WAN オーバーレイパスへのルーティングに従います。フローが識別されると、フローのその後のパケットは、データポリシーで定義されている NAT66 DIA パスを使用します。このパス変更により、フローがリセットされます。これは、パスが異なると、サーバーへのクライアント送信元またはポートの組み合わせが異なることを意味し、サーバーは不明な TCP フローをリセットします。

NAT66 DIA フローのスティッキネス機能は、NAT66 パスのフローレベル状態を記録します。フローの最初のパケットが非 NAT66 の場合、このフローの残りのパケットも非 NAT66 パスを

使用します。最初のパケットフローが NAT66 DIA パスを経由する場合、このフローの残りのパケットも NAT66 DIA パスを使用します。これは、NAT66 DIA データポリシーではデフォルトで有効になっています。

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a から、NAT66 DIA フローのスティッキネス機能はデフォルトで有効になっています。フロースティッキネスを無効にするには、CLI アドオンテンプレートを使用してローカライズされたポリシーで **flow-stickiness-disable** コマンドを使用します。

NAT66 DIA の仕組み

1. ブランチサイトの IPv6 クライアントは、ネットワークのトランスポート側（VPN 0）にある Cisco SD-WAN Manager データセンターにアクセスしようとします。
2. Cisco IOS XE Catalyst SD-WAN デバイス は、IPv6 アドレスをサービス VPN（VPN 1）から、ネットワークの WAN 側であるネクストホップ トランスポート VPN（VPN 0）にルーティングします。
3. NAT66 トランスレータは、IPv6 から IPv6 へのプレフィックス変換を実行します。Dynamic Host Configuration Protocol バージョン 6（DHCPv6）では、プレフィックス委任のために IPv6 プレフィックス範囲にソース IPv6 プレフィックスが必要です。

   NAT66 変換は、トランスポート VPN インターフェイスで発生します。

   DHCPv6 プレフィックス委任により、ISP は顧客のネットワーク内で使用する顧客にプレフィックスを割り当てるプロセスを自動化できます。プレフィックス委任は、DHCPv6 プレフィックス委任オプションを使用して、プロバイダーエッジ（PE）デバイスと宅内装置（CPE）の間で行われます。ISP が顧客にプレフィックスを委任した後、顧客はネットワークをさらに分割し、顧客のネットワーク内のリンクにプレフィックスを割り当てることができます。
4. Cisco SD-WAN Manager からトラフィックが返されると、Cisco IOS XE Catalyst SD-WAN デバイス は DIA ルートテーブルで NAT66 エントリを検索し、パケットをクライアントの IPv6 アドレスに転送します。

ステートレス DHCP を使用した NAT66 DIA の設定

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a から、ルータアドバタイズメント（RA）プレフィックスでステートレスアドレス自動設定（SLAAC）を使用して、WAN インターフェイスで IPv6 アドレスを自動設定できます。ステートレス DHCPv6 は、SLAAC と DHCPv6 の組み合わせです。デバイスは O ビットが設定された RA を送信しますが、M ビットは設定しません。DHCPv6 サーバーがクライアント アドレス バインディングを追跡する必要がないため、これはステートレス DHCPv6 と呼ばれます。RA プレフィックスは、サービス側トラフィックの IPv6 DIA の NAT66 で使用できます。設定すると、同じ送信元プレフィックスを異なる外部インターフェイスと照合できます。

開始する前に、DHCPv6 と SLAAC が設定されていることを確認します。詳細については、「*Information About DHCPv6*」を参照してください。

（注） SLAAC インターフェイスで使用される RA プレフィックスが、スタティック NAT66 マッピングルールで使用される外部プレフィックスと異なることを確認します。

マッピングルールが設定され、フローが一致すると、トラフィックは内部から外部に流れます。NAT66 は、サービス側ホストと RA プレフィックスを共有するためのバインドテーブルを維持します。サービス側インターフェイスからの IPv6 パケットが DIA パスを通過する場合、RA プレフィックスを使用して元の送信元アドレスと変換された送信元アドレスに対してバインドが作成されます。パケットを元に戻す場合は、同じバインドが使用されます。NAT66 は、指定された時間、バインドエントリを維持します。デフォルトのタイムアウト値は 5 分です。

インターフェイスのプレフィックス変換ルールは、パケットがそのインターフェイスを通過する場合にのみ有効であり、RA でプレフィックス変換ルールを設定した場合は出力インターフェイスを指定する必要はありません。

[Translated Source Prefix] をシステムのデフォルトとして設定すると、SLAAC 機能によって自動的に RA プレフィックス（外部）が提供されます。それ以外の場合は、変換ルールで外部プレフィックスを設定する必要があります。

Cisco Catalyst SD-WAN Manager または CLI を使用して、ステートレス DHCP を使用した NAT66 DIA を設定できます。

- Cisco Catalyst SD-WAN Manager によるステートレス DHCP を使用した NAT66 DIA の設定
- CLI でステートレス DHCP を使用した DIA の設定

一元管理型データポリシーを使用した NAT66 DIA

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a、Cisco Catalyst SD-WAN Manager リリース 20.13.1

nat use-vpn 0 コマンドを使用すると、Cisco IOS XE Catalyst SD-WAN デバイスで一元管理型データポリシーを使用して NAT66 DIA ルートを設定できます。これにより、データトラフィックは、トランスポート VPN にあるオーバーレイトンネルに入る前に NAT 処理されます。ポリシー一致基準に基づいて、送信元 IP アドレスが変換された後、一致する IPv6 トラフィックが DIA 回線を介して転送されます。IPv6 トラフィックは、送信元 IPv6 プレフィックスまたはプレフィックスリストか、宛先 IPv6 プレフィックスまたはプレフィックスリストの一元管理型ポリシー一致基準に基づいて、DIA 回線を介して宛先アドレスの NAT66 の後に転送されます。

デバイスのサービス側で NAT66 を設定するには、デバイスのサービス VPN 内に NAT66 インターフェイスを設定してから、Cisco Catalyst SD-WAN コントローラで一元管理型データポリシーを設定します。このポリシーは、必要なプレフィックスを持つデータトラフィックをサービス側 NAT に転送します。

ネットワークのサービス側に出入りするデータの NAT を設定できます。サービス側 NAT は、構成された一元化されたデータポリシーと一致する、内部および外部ホストアドレスのデータトラフィックを変換します。

DIAルートが使用できない場合、フォールバックオプションが設定されていないと、トラフィックはドロップされます。NAT66 フォールバック機能は、DIA ルートに送信されるすべてのトラフィックが必要に応じて代替ルートを使用できるよう、ルーティングベースのメカニズムを提供します。この機能は、サービス側とトンネル側の両方でサポートされます。

CLI を使用した Cisco SD-WAN コントローラ でのデータポリシーによる NAT66 DIA の設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a、Cisco Catalyst SD-WAN Manager リリース 20.13.1

CLI テンプレートの使用の詳細については、CLI アドオン機能テンプレートおよび CLI テンプレートを参照してください。

CLI を使用した NAT66 DIA の設定

Cisco SD-WAN コントローラ でデータポリシーによって NAT66 DIA を設定する例を次に示します。

```
Device# policy
 data-policy policy-name
 vpn-list vpn_list
 sequence number
 match
 source-ipv6 ipv6-address
 !
 action accept
 nat use-vpn 0
 nat fallback
 set
 local-tloc-color lte
```

Cisco Catalyst SD-WAN Manager を使用したデータポリシーによる NAT66 DIA の設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a および Cisco Catalyst SD-WAN Manager リリース 20.13.1。

一元管理型データポリシーを使用して、Cisco SD-WAN Manager でフォールバックとともに NAT66 DIA の IPv6 一致条件とアクション条件を設定できます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Policies]** の順に選択します。
2. [Custom] オプションのドロップダウンの [Centralized Policy] で [Traffic Data] を選択します。
3. [Add Policy] ドロップダウンから、[Create New] をクリックします。
4. [シーケンスタイプ（Sequence Type）] をクリックし、[カスタム（Custom）] を選択します。
5. [(+)シーケンスルール（Sequence Rule）] をクリックして、新規のシーケンスルールを作成します。
6. [Protocol] ドロップダウンリストで、[IPv6] を選択します。

7. マッチ条件を追加したら、[アクション（Actions）]、[承認（Accept）] の順にクリックします。
8. [NAT VPN] をクリックし、[フォールバック（Fallback）] チェックボックスをオンにします。
9. [アクションの保存と照合（Save and Match Actions）] をクリックします。
10. [データポリシーの保存（Save Data Policy）] をクリックします。

Cisco SD-WAN Manager を使用して NAT フォールバックを有効にするには、次の手順を実行してデータポリシーを作成および設定します。

- 既存の一元管理型ポリシーを編集し、ポリシーをインポートします。
  1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Policies]** の順に選択します。
  2. [Custom] オプションのドロップダウンの [Centralized Policy] で [Traffic Data] を選択します。
  3. [Add Policy] ドロップダウンから、[Create New] をクリックします。
  4. [シーケンスタイプ（Sequence Type）] をクリックし、[カスタム（Custom）] を選択します。
  5. [(+)シーケンスルール（Sequence Rule）] をクリックして、新規のシーケンスルールを作成します。
  6. マッチ条件を追加したら、[アクション（Actions）]、[承認（Accept）] の順にクリックします。
  7. [NAT VPN] をクリックし、[フォールバック（Fallback）] チェックボックスをオンにします。
  8. [アクションの保存と照合（Save and Match Actions）] をクリックします。
  9. [データポリシーの保存（Save Data Policy）] をクリックします。

ポリシーグループを使用したデータポリシーによる NAT66 DIA の設定

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a から、設定グループを使用して、Cisco SD-WAN Manager でステートレス DHCP を使用して NAT66 DIA を設定できます。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Policy Groups]** の順に選択します。
2. [Application priority & SLA policy] をクリックして、ポリシーを作成します。

   既存のポリシーを編集するには、[Action] の下にあるアプリケーション優先順位と SLA ポリシーの横にある省略記号アイコン（[...]）をクリックし、[Edit] をクリックします。

3. [Internet Offload Traffic] で、[Application List] ドロップダウンリストからアプリケーションを選択し、[Fallback to Routing] オプションをオンにして、ダイレクト インターネット アクセスを設定します。
4. [Apply Policy] で、方向、VPN、およびインターフェイスを設定します。
5. [Save] をクリックします。

NAT66 DIA の利点

- ローカル IPv6 インターネット トラフィックをサポートし、トランスポート VPN を介してサービス側 VPN からインターネットに直接出ます
- IPv6 環境で、あるネットワークから別のネットワークにパケットをリダイレクトまたは転送できます
- 優れたアプリケーション パフォーマンスを実現
- 帯域幅の消費と遅延の削減に貢献
- 帯域幅コストの削減に貢献
- リモートサイトに DIA を提供することで、ブランチオフィスのユーザーエクスペリエンスを向上させます。
- Cisco IOS XE Catalyst SD-WAN リリース 17.14.x から、セルラーおよびダイヤラインターフェイスをサポートします。

NAT66 DIA の制限事項

- ファイアウォール、AppNav-XE、およびマルチキャストはサポートされていません。

  Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a から、NAT66 ではファイアウォールを使用できます。
- NAT66 DIA トラフィックフローのみがサポートされます。サービス側のトラフィックフローはサポートされていません。
- 一元化されたデータポリシーは、NAT66 DIA ではサポートされていません。

  Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a から、一元管理型データポリシーは NAT66 DIA でサポートされます。
- NAT64 と NAT66 の組み合わせは、同じインターフェイスではサポートされていません。
- 各 VRF でサポートされるプレフィックス変換は 1 つだけです。

  Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a から、VRF ごとに複数のプレフィックス変換がサポートされます。
- NAT66 DIA での複数の WAN リンクの使用はサポートされていません。

Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a から、複数の WAN リンクが NAT66 DIA でサポートされます。

- サービス IPv6 ルーティングプロトコルを使用した NAT66 DIA ルートの再配布はサポートされていません。

  Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a から、BGP または OSPFv3 プロトコルへの NAT66 DIA ルート再配布を設定できます。

- リアルタイムの運用アプリケーションプログラミングインターフェイス（API）はサポートされていません。
- NAT66 DIA ルート操作を成功させるには、VPN 0 にデフォルトルートを含める必要があります。
- 物理イーサネット サブインターフェイスのみがサポートされています。
- ルータアドバタイズメント（RA）のプレフィックスは、NAT66 プレフィックス変換ではサポートされていません。
- マルチテナンシーリソースの制限はサポートされていません。
- NAT66 を使用した IPv6 TLOC 拡張はサポートされていません。

NAT66 DIA と DIA ルートの設定

NAT66 DIA および NAT66 DIA ルートを有効にするためのワークフロー

1. IPv6 用の [Cisco VPN Interface Ethernet] 機能テンプレートを使用して、NAT66 DIA を有効にします。

   [Cisco VPN Interface Ethernet] テンプレートは、トランスポート（WAN）インターフェイスとして使用されます。

   [Cisco VPN Interface Ethernet] テンプレートを使用して NAT66 DIA を有効にする方法の詳細については、「NAT66 DIA の設定」を参照してください。

2. サービス側 VPN（VPN 0 以外の VPN）である [Cisco VPN] 機能テンプレートを使用して、NAT66 DIA IPv6 ルートを設定します。

   NAT66 DIA IPv6 ルートの設定の詳細については、「NAT66 DIA ルートの設定」を参照してください。

NAT66 DIA の設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x リリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Cisco VPN Interface Ethernet] テンプレートを編集するには、**...** をクリックし、[Edit] を選択します。
4. [NAT] をクリックし、[IPv6] を選択します。
5. [NAT] ドロップダウンリストで、スコープを [Default] から [Global] に変更します。

   [On] をクリックして NAT66 を有効にします。
6. [NAT Selection] フィールドで、[NAT66] を選択します。
7. [New Static NAT] をクリックします。
8. [Source Prefix] フィールドで、送信元 IPv6 プレフィックスを指定します。
9. [Translated Source Prefix] フィールドで、変換された送信元プレフィックスを指定します。
10. [Source VPN ID] フィールドで、送信元 VPN ID を指定します。
11. [更新（Update）] をクリックします。

CLI アドオンテンプレートを使用した DHCPv6 プレフィックス委任の有効化

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. [Add template] をクリックします。
4. [Select Devices] で、テンプレートを作成するデバイスを選択します。
5. [Select Template] で、[OTHER TEMPLATES] セクションまで下にスクロールし、[CLI Add-On Template] をクリックします。
6. [Template Name] フィールドに、機能テンプレートの名前を入力します。
7. [Description] フィールドに機能テンプレートの説明を入力します。
8. [CLI CONFIGURATION] 領域で、DHCPv6 設定を入力します。

```
interface GigabitEthernet1
ipv6 dhcp client pd prefix-from-provider
ipv6 dhcp client request vendor
```

9. **[Save（保存）]** をクリックします。

   CLI アドオンテンプレートは、[CLI CONFIGURATION] テーブルに表示されます。

10. CLI アドオン機能テンプレートを使用するには、デバイステンプレートを次のように編集します。
    1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
    2. [Device Template] をクリックします。

（注） Cisco vManage リリース 20.7.x 以前のリリースでは、[Device Templates] のタイトルは [Device] です。

    3. **[. . .** をクリックし、[Edit] を選択します。
    4. [Additional Templates] までスクロールダウンし、[CLI Add-On Template] ドロップダウンリストから、以前に作成した CLI アドオン機能テンプレートを選択します。
    5. [更新（Update）] をクリックします。

NAT66 DIA ルートの設定

[Cisco VPN] テンプレートで NAT66 DIA を使用して IPv6 ルートを有効にします。

VPN 1 などのすべてのサービス VPN は、DIA トラフィックのトランスポート VPN（VPN 0）にパケットをルーティングします。

Cisco VPN テンプレートを使用した NAT66 DIA ルートの設定

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

（注） Cisco vManage リリース 20.7.x リリースでは、[Feature Templates] のタイトルは [Feature] です。

3. [Cisco VPN] テンプレートを編集するには、テンプレートの横にある **. .** をクリックし、[Edit] を選択します。
4. [IPv6 Route] をクリックします。
5. [New IPv6 Route] をクリックします。
6. [Prefix] フィールドに、NAT66 変換の IPv6 プレフィックスを入力します。

   グローバルな内部および外部プレフィックスは、 virtual routing and forwarding（VRF）ごとに一意である必要があります。

   IPv6 プレフィックス委任（PD）プレフィックス長は、/56 以下である必要があります。

   グローバル外部プレフィックスは、VRF ごとに一意である必要があります。

内部のプレフィックス長と外部のプレフィックス長は同じである必要があります。

/56 の PD プレフィックスで最大 250 の VRF がサポートされます。

7. [Gateway] フィールドで、[VPN] をクリックします。
8. [Enable VPN] ドロップダウンリストで、スコープを [Default] から [Global] に変更し、[On] をクリックして VPN を有効にします。
9. [NAT] ドロップダウンリストで、スコープを [Default] から [Global] に変更し、[On] をクリックして NAT66 を有効にします。
10. [更新（Update）] をクリックします。

Cisco Catalyst SD-WAN Manager によるステートレス DHCP を使用した NAT66 DIA の設定

Cisco Catalyst SD-WAN Manager リリース 20.13.1 から、設定グループを使用して、Cisco SD-WAN Manager でステートレス DHCP を使用して NAT66 DIA を設定できます。

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]** を選択します。
2. [Add Configuration Group] をクリックして、新しい設定グループを作成するか、[Actions] の下の [Edit] をクリックして既存の設定グループを編集します。
3. 設定グループを編集するには、横にある [...] をクリックして、 [Edit] を選択します。
4. [Transport Profile] をクリックします。
5. **[. . .]**（VPN 機能の横にある）をクリックして、[Add Sub-Feature] を選択します。
6. ドロップダウンリストからイーサネット インターフェイスを選択します。
7. **[NAT]** > **[IPv6 Settings]** の順にクリックします。
8. [NAT] ドロップダウンリストで、スコープを [Default] から [Global] に変更し、NAT66 を有効にします。
9. [NAT66] オプションで、[Add Nat66] をクリックし、[Source Prefix] と [Source VPN ID] を設定します。
10. [Translated Source] フィールドはシステムのデフォルト値のままにします。
11. [Egress Interface] ドロップダウンリストで、スコープを [Default] から [Global] に変更し、出力インターフェイスを有効にします。
12. [Add] をクリックします。
13. [Save] をクリックします。

機能テンプレートによるステートレス DHCP を使用した NAT66 DIA の設定

Cisco IOS XE Catalyst SD-WAN リリース 17.13.1a から、機能テンプレートを使用して、Cisco SD-WAN Manager でステートレス DHCP を使用して NAT66 DIA を設定できます。

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. [Add template] をクリックします。
4. [Select Devices] で、テンプレートを作成するデバイスを選択します。
5. [Select Template] で、[VPN] セクションまで下にスクロールし、[Cisco VPN Interface Ethernet] をクリックします。
6. [Template Name] フィールドに、機能テンプレートの名前を入力します。
7. [Description] フィールドに機能テンプレートの説明を入力します。
8. **[NAT]** > **[IPv6]** の順にクリックします。
9. [NAT] ドロップダウンリストで、スコープを [Default] から [Global] に変更します。
10. NAT を有効にするには、[ON] をクリックします。
11. [NAT Selection] ドロップダウンリストで、スコープを [Default] から [Global] に変更し、[NAT66] を選択します。
12. [New Static NAT] をクリックします。
13. [Source Prefix] と [Source VPN ID] を設定します。
14. [Translated Source Prefix] フィールドはシステムのデフォルト値のままにします。
15. [Egress Interface] ドロップダウンリストで、スコープを [Default] から [Global] に変更し、[Yes] をクリックします。
16. [Add] をクリックします。
17. [Save] をクリックします。

CLI を使用した NAT66 DIA の設定

NAT66 DIA のスタティック NAT プレフィックス変換の設定

```
interface GigabitEthernet1
 ip address 10.1.15.15 255.0.0.0
 no ip redirects
 load-interval 30
 negotiation auto
 nat66 outside
```

```
 ipv6 address 2001:DB8:A1:F::F/64
 no ipv6 redirects
 service-policy output shape_GigabitEthernet1
!
nat66 prefix inside 2001:DB8:380:1::/80 outside 2001:DB8:A1:F:0:1::/80 vrf 1
nat66 prefix inside 2001:DB8:A14:18::/80 outside 2001:DB8:A1:F::/80 vrf 1
nat66 route vrf 1 2001:DB8:A14:19::/64 global
nat66 route vrf 1 2001:DB8:3D0:1::/64 global
```

CLI でステートレス DHCP を使用した DIA の設定

```
interface GigabitEthernet1
 nat66 outside
 ip address 10.1.15.15 255.0.0.0
 ipv6 address autoconfig
 ipv6 enable
 ipv6 nd autoconfig default-route
 no ip redirects
 load-interval 30
 negotiation auto
 no ipv6 redirects
 service-policy output shape_GigabitEthernet1
!
nat66 prefix inside 2001:a14:18::/64 outside interface GigabitEthernet1 vrf 1
nat66 prefix inside 2001:a14:18::/64 outside interface GigabitEthernet1
```

NAT66 DIA の複数リンクの設定

Cisco IOS XE Catalyst SD-WAN リリース 17.12.1a から、NAT66 DIA の複数の出力インターフェイスを設定できます。

次に、GigabitEthernet1 と GigabitEthernet4 の 2 つのインターフェイスを使用して NAT66 DIA を設定する例を示します。

```
interface GigabitEthernet1
 no shutdown
 ipv6 address 2001:a1:f::f/64
 ipv6 nd ra suppress all
 no mop enabled
 no mop sysid
 negotiation auto
 nat66 outside
!
interface GigabitEthernet4
 no shutdown
 ipv6 address 2001:a0:14::f/64
 ipv6 enable
 ipv6 nd ra suppress all
 no mop enabled
 no mop sysid
 negotiation auto
 nat66 outside
!
nat66 prefix inside 2001:a14:18:0::/64 outside 2001:a1:f::/64 vrf 1 egress-interface
GigabitEthernet1
nat66 prefix inside 2001:a14:18:0::/64 outside 2001:a0:14::/64 vrf 1 egress-interface
GigabitEthernet4
nat66 prefix inside FC00:1:2:3::/80 outside 3001:a1:5::/80 vrf 100
nat66 route vrf 1 2001:a0:5::/64 global
nat66 route vrf 100 ::/0 global
```

詳細については、『Cisco IOS XE SD-WAN Qualified Command Reference Guide』の nat66 prefix コマンドを参照してください。

NAT66 DIA の DHCPv6 プレフィックス委任の設定

```
interface GigabitEthernet1
ip address 10.1.15.15 255.0.0.0
no ip redirects
load-interval 30
negotiation auto
nat66 outside
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
ipv6 nd autoconfig default-route
ipv6 dhcp client pd prefix-from-provider
ipv6 dhcp client request vendor
arp timeout 1200
no mop enabled
no mop sysid
service-policy output shape_GigabitEthernet1
!
nat66 prefix inside 2001:DB8:10:1::/64 outside prefix-from-provider vrf 1
nat66 prefix inside 2001:DB8:100:1::/64 outside prefix-from-provider vrf 100
nat66 prefix inside 2001:DB8:101:1::/64 outside prefix-from-provider vrf 101
nat66 route vrf 1 2001:DB8:A14:19::/64 global
nat66 route vrf 1 2001:DB8:3D0:1::/64 global
nat66 route vrf 100 ::/0 global
nat66 route vrf 101 ::/0 global
```

NAT66 DIA および DIA ルート設定の確認

NAT66 プレフィックス変換エントリの表示

```
Device# show nat66 prefix
Prefixes configured: 2
NAT66 Prefixes
Id: 1 Inside 2001:DB8:380:1::/80 Outside 2001:DB8:A1:F:0:1::/80
Id: 2 Inside 22001:DB8:A14:18::/80 Outside 2001:DB8:A1:F::/80
```

NAT66 DIA ルートの確認

```
Device# show nat66 route-dia
Total interface NAT66 DIA enabled count [1]
route add [1] addr [2001:DB8:A14:19::] vrfid [2] prefix len [64]
route add [1] addr [2001:DB8:3D0:1::] vrfid [2] prefix len [64]
```

NAT66 ネイバー探索の表示

```
Device# show nat66 nd
NAT66 Neighbor Discovery

ND prefix DB:
  2001:DB8:A1:F::/80
  2001:DB8:A1:F:0:1::/80
  2001:DB8:A1:F:1::/64
  2001:DB8:A1:F:2::/64
  2001:DB8:A1:F:3::/64
```

```
ipv6 ND entries:
  2001:DB8:A1:F::F
  2001:DB8:A1:F::11
```

変換されたパケットの NAT66 グローバル統計の確認

```
Device# show nat66 statistics
NAT66 Statistics

Global Stats:
   Packets translated (In -> Out)
      : 7
   Packets translated (Out -> In)
      : 7
```

ステートレス DHCP を使用した NAT66 DIA の確認

バインディングエントリを表示するには、次の手順を実行します。

```
Device# show platform hardware qfp active feature nat66 datapath bind-dump
bind 0xdf612cc0 v6outaddr 2001:A1:F::96 v6addr 2001:A14:18::96 vrfid 3 domain 0 create
time 513092 refcnt 0 flags 0x0 mapping 0xdf54ba40 last_use_ts 513186 output_ifhandle
0x1b
```

内部および外部変換時における各プレフィックスカウンタの NAT66 プラットフォームの表示

```
Device# show platform hardware qfp active feature nat66 datapath prefix
prefix hasht 0x89628400 max 2048 chunk 0x8c392bb0 hash_salt 719885386
NAT66 hash[1] id(1) len(64) vrf(0) in: 2001:db8:ab01:0000:0000:0000:0000:0000 out:
 2001:db8:ab02:0000:0000:0000:0000:0000 in2out: 7 out2in: 7
```

NAT66 プラットフォーム グローバル カウンタの確認

```
Device# show platform software nat66 fp active statistics
QFP Stats:
Interface:
    Add: 2, Ack: 2, Err: 0
    Mod: 0, Ack: 0, Err: 0
    Del: 0, Ack: 0, Err: 0
Prefix Trans:
    Add: 5, Ack: 5, Err: 0
    Mod: 0, Ack: 0, Err: 0
    Del: 0, Ack: 0, Err: 0
AOM Stats:
Interface:
    Add: 2, Err: 0
    Mod: 0, Err: 0
    Del: 0, Err: 0
    Free: 0, Err: 0
Prefix Translation:
    Add: 5, Err: 0
    Mod: 0, Err: 0
    Del: 0, Err: 0
    Free: 0, Err: 0
DB Stats:
  Interface:
    Add: 2, Err: 0
    Mod: 0, Err: 0
    Del: 0, Err: 0
  Prefix Translations:
    Add: 5, Err: 0
    Mod: 0, Err: 0
```

```
    Del: 0, Err: 0
Message RX Stats:
  Interface:
    Add: 2
```

NAT66 DIA の設定例

以下は、NAT66 DIA のエンドツーエンドの設定例です。

```
interface GigabitEthernet1
ip address 10.1.15.15 255.0.0.0
no ip redirects
load-interval 30
negotiation auto
nat66 outside
ipv6 address dhcp
ipv6 address autoconfig
ipv6 enable
ipv6 nd autoconfig default-route
ipv6 dhcp client pd prefix-from-provider
ipv6 dhcp client request vendor
arp timeout 1200
no mop enabled
no mop sysid
service-policy output shape_GigabitEthernet1
!
nat66 prefix inside 2001:DB8:380:1::/80 outside 2001:DB8:A1:F:1::/80 vrf 1
nat66 prefix inside 2001:DB8:A14:18::/80 outside 2001:DB8:A1:F::/80 vrf 1
nat66 prefix inside 2001:DB8:10:1::/64 outside prefix-from-provider vrf 1
nat66 prefix inside 2001:DB8:100:1::/64 outside prefix-from-provider vrf 100
nat66 prefix inside 2001:DB8:101:1::/64 outside prefix-from-provider vrf 101
nat66 route vrf 1 2001:DB8:A14:19::/64 global
nat66 route vrf 1 2001:DB8:3D0:1::/64 global
nat66 route vrf 100 ::/0 global
nat66 route vrf 101 ::/0 global
```

次は、NAT66 DIA の複数リンクを使用したエンドツーエンドの設定例です。

```
interface GigabitEthernet3
 no shutdown
 ipv6 address 2001:a1:f::f/64
 ipv6 nd ra suppress all
 no mop enabled
 no mop sysid
 negotiation auto
 nat66 outside
!
interface GigabitEthernet4
 no shutdown
 ipv6 address 2001:a0:14::f/64
 ipv6 enable
 ipv6 nd ra suppress all
 no mop enabled
 no mop sysid
 negotiation auto
 nat66 outside
!
nat66 prefix inside 2001:a14:18:0::/64 outside 2001:a1:f::/64 vrf 1 egress-interface
GigabitEthernet3
nat66 prefix inside 2001:a14:18:0::/64 outside 2001:a0:14::/64 vrf 1 egress-interface
GigabitEthernet4
nat66 prefix inside FC00:1:2:3::/80 outside 3001:a1:5::/80 vrf 100
```

```
nat66 route vrf 1 2001:a0:5::/64 global
nat66 route vrf 100 ::/0 global
```

NAT66 DIA ルート再配布

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a、Cisco Catalyst SD-WAN Manager リリース 20.14.1

NAT66 ルート再配布に関する情報

ルート再配布は、異なるルーティングプロトコルを実行している複数のドメイン間でルーティング情報を共有します。NAT66 DIA ルート再配布を設定すると、変換された IPv6 アドレスの Open Shortest Path First（OSPFv3）またはボーダー ゲートウェイ プロトコル（BGP）への再配布が有効になります。

リモートサイトからのトラフィックがオーバーレイネットワークまたはトンネルを通過するとき、NAT66 外部アドレス変換サービスはリモートホストの送信元 IP アドレス（外部ホスト）を変換します。変換は、トラフィックがネットワークの LAN（VPN1）側に送信される前に行われます。ルート再配布が設定されている場合、NAT 外部プールアドレスまたはルートは、OSPFv3 または BGP プロトコルを介してネットワークの LAN 側に再配布されます。そのため、あるネットワークの内部ホストは、異なるルーティングプロトコルを実行している別のネットワークのリモートホストに到達するためのパスを認識します。

NAT66 ルート再配布 は、ローカルに学習、またはルーティングピアから学習した次のタイプのルートに適用されます。

- BGP
- OSPFv3

CLI ベースの設定グループまたは機能テンプレートを使用して NAT66 DIA ルート再配布を設定できます。

機能テンプレートを使用した NAT66 DIA ルート再配布の設定

Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a から、Cisco SD-WAN Manager の機能テンプレートを使用して、BGP または OSPFv3 プロトコルへの NAT66 DIA ルート再配布を設定できます。

機能テンプレートを使用した BGP への NAT66 DIA ルート再配布の設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a、Cisco Catalyst SD-WAN Manager リリース 20.14.1

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。

3. [Add template] をクリックします。
4. [Select Devices] で、テンプレートを作成するデバイスを選択します。
5. [Select Template] で、[OTHER TEMPLATES] セクションまで下にスクロールし、[Cisco BGP] をクリックします。
6. [Template Name] フィールドに、機能テンプレートの名前を入力します。
7. [Description] フィールドに機能テンプレートの説明を入力します。
8. [UNICAST ADDRESS FAMILY] をクリックします。
9. [IPv6] をクリックします。
10. [New Redistribute] をクリックします。
11. [Protocol] ドロップダウンリストで [NAT] を選択します。
12. [Add] をクリックします。
13. [Save] をクリックします。

機能テンプレートを使用した OSPFv3 への NAT66 DIA ルート再配布の設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a、Cisco Catalyst SD-WAN Manager リリース 20.14.1

1. Cisco SD-WAN Manager メニューから、**[Configuration]** > **[Templates]** を選択します。
2. [Feature Templates] をクリックします。
3. [Add template] をクリックします。
4. [Select Devices] で、テンプレートを作成するデバイスを選択します。
5. [Select Template] で、[OTHER TEMPLATES] セクションまで下にスクロールし、[Cisco OSPFv3] をクリックします。
6. [Template Name] フィールドに、機能テンプレートの名前を入力します。
7. [Description] フィールドに機能テンプレートの説明を入力します。
8. [IPv6] をクリックします。
9. [Redistribute] タブで、[New Redistribute] をクリックします。
10. [Protocol] ドロップダウンリストで [nat-route] を選択します。
11. [Add] をクリックします。
12. [Save] をクリックします。

CLI ベースの設定グループを使用した NAT66 DIA ルート再配布の設定

Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a から、Cisco SD-WAN Manager の CLI ベースの設定グループを使用して、BGP または OSPFv3 プロトコルへの NAT66 DIA ルート再配布を設定できます。

CLI ベースの設定グループを使用した BGP への NAT66 DIA ルート再配布の設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a、Cisco Catalyst SD-WAN Manager リリース 20.14.1

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]** を選択します。
2. [Add CLI based Configuration Group] をクリックします。
3. CLI ベースの設定グループの名前を入力します。
4. [Solution] ドロップダウンリストで、[sdwan] を選択します。
5. [Description] フィールドに、CLI ベースの設定グループの説明を入力します。
6. [Next] をクリックします。
7. フィールドに CLI ベースの設定を入力します。
    1. BGP ルーティングプロセスを設定し、指定したルーティングプロセスのルータ コンフィギュレーション モードを開始します。*autonomous-system-number* 引数を使用して、0 ～ 65534 の範囲の整数を 1 つ指定します。これは、その他の BGP スピーカーへのデバイスを表します。

        router bgp *autonomous-system-number*

    2. ルータ ID を、BGP を実行するローカルデバイスの識別子として設定します。*ip-address* 引数を使用して、ネットワーク内でルータ IP アドレスを指定します。

        bgp router-id *ip-address*

    3. IPv6 アドレスファミリを指定して、アドレス ファミリ コンフィギュレーション モードを開始します。

        address-family ipv6 unicast vrf *vrf-name*

    4. 指定された AS のネイバーの IP アドレスを、ローカルデバイスの IPv6 マルチプロトコル BGP ネイバー テーブルに追加します。

        neighbor *ip-address* **remote-as** *autonomous-system-number*

    5. ネイバーが IPv6 ユニキャスト アドレス ファミリのプレフィックスをローカルデバイスと交換できるようにします。

        neighbor *ip-address* **activate**

    6. NAT ルートを再配布します。

redistribute nat-route

7. アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

   exit-address-family

8. [Save] をクリックします。

BGP への NAT66 DIA ルート再配布を設定する例を次に示します。

```
router bgp 15
bgp router-id 10.1.1.1
address-family ipv6 unicast vrf 1
  neighbor 2001:a14:18::64 remote-as 2
  neighbor 2001:a14:18::64 activate
  redistribute nat-route
  exit-address-family
!
```

CLI ベースの設定グループを使用した OSPFv3 への NAT66 DIA ルート再配布の設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a、Cisco Catalyst SD-WAN Manager リリース 20.14.1

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]** を選択します。
2. [Add CLI based Configuration Group] をクリックします。
3. CLI ベースの設定グループの名前を入力します。
4. [Solution] ドロップダウンリストで、[sdwan] を選択します。
5. [Description] フィールドに、CLI ベースの設定グループの説明を入力します。
6. [Next] をクリックします。
7. フィールドに CLI ベースの設定を入力します。
   1. インターフェイスを設定します。

      interface *interface-name*

   2. OSPFv3 プロセス ID を入力し、インターフェイスが接続するネットワークタイプとして [point-to-point] を指定します。

      ospfv3 *process-id* **network point-to-point**

   3. IPv6 アドレスファミリの OSPFv3 エリアを設定します。

      ospfv3 *process-id* **ipv6 area** *area-id*

   4. ルータ コンフィギュレーション モードを開始し、OSPFv3 プロセス ID を入力します。

      router ospfv3 *process-id*

5. OSPFv3 を実行しているローカルデバイスの識別子としてルータ ID を設定します。*ip-address* 引数を使用して、ネットワーク内でルータ IP アドレスを指定します。

   router-id *ip-address*

6. IPv6アドレスファミリを指定して、アドレスファミリ コンフィギュレーション モードを開始します。

   address-family ipv6 unicast

7. OSPFv3 ネイバーが起動または停止したときに、デバイスが syslog メッセージを送信するように設定します。

   log-adjacency-changes

8. 接続ルートを OSPFv3 に再配布します。

   redistribute connected

9. NAT ルートを再配布します。

   redistribute nat-route

10. アドレス ファミリ コンフィギュレーション モードを終了して、特権 EXEC モードに戻ります。

    exit-address-family

8. [Save] をクリックします。

OSPFv3 への NAT66 DIA ルート再配布を設定する例を次に示します。

```
interface GigabitEthernet5
ospfv3 1 network point-to-point
ospfv3 1 ipv6 area 0
    router ospfv3 1
    router-id 10.1.1.1
address-family ipv6 unicast
  log-adjacency-changes
  redistribute connected
  redistribute nat-route
  exit-address-family
!
```

NAT66 DIA を使用したダイヤラインターフェイス

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a、Cisco Catalyst SD-WAN Manager リリース 20.14.1

NAT66 DIA でのダイヤラインターフェイスに関する情報

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a、Cisco Catalyst SD-WAN Manager リリース 20.14.1

ダイヤラインターフェイスは、デフォルトルーティング情報、カプセル化プロトコル、使用するダイヤラプールなど、クライアントからのダイヤラトラフィックを処理する方法を指定します。ダイヤラインターフェイスは、実際にダイヤルアップを実行する物理インターフェイスの抽象化レイヤを提供します。この機能は、NAT66 DIA の Point-to-Point Protocol（PPP）ダイヤラインターフェイスをサポートしています。

次のダイヤラインターフェイスがサポートされています。

- Point-to-Point Protocol over Ethernet（PPPoE）
- Point-to-Point Protocol over Asynchronous Transfer Mode（PPPoA）
- Point-to-Point Protocol over Ethernet over Asynchronous Transfer Mode（PPPoEoA）

PPP は、一般的な顧客宅内機器を介して、イーサネット ローカル エリア ネットワーク経由で複数のユーザーをリモートサイトに接続します。PPP は一般的に、デジタル加入者線（DSL）などのブロードバンドアグリゲーションで使用されます。PPP は、チャレンジハンドシェイク認証プロトコル（CHAP）またはパスワード認証プロトコル（PAP）での認証を提供しますが、物理インターフェイスでは認証は実行されません。

PPPoE の設定の詳細については、『*Cisco Catalyst SD-WAN Systems and Interfaces Guide, Cisco IOS XE Catalyst SD-WAN リリース 17.x*』の「Configuring PPPoE」セクションを参照してください。

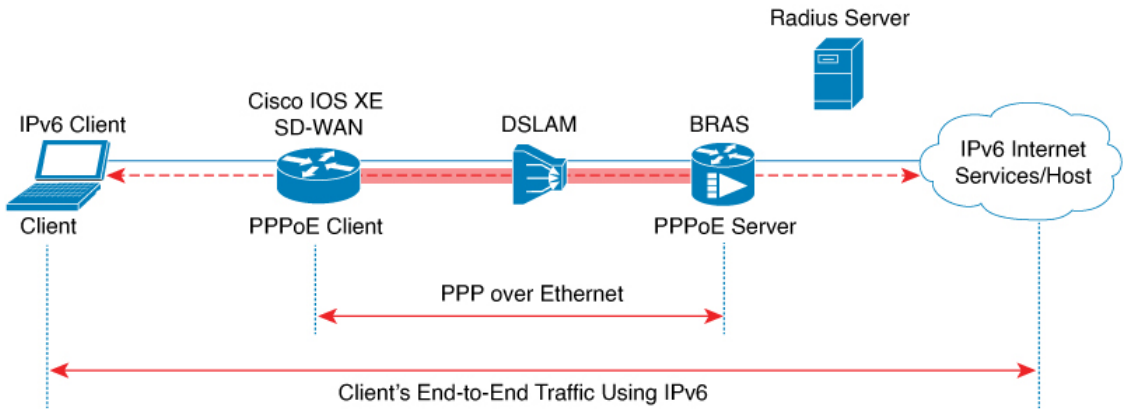
NAT66 DIA でダイヤラインターフェイスを使用する利点

- 着信コールまたは発信コールの要件に基づいた物理インターフェイスのさまざまな特性
- NAT66 DIA を使用したルートベースおよびデータポリシーベースの設定サポート

NATDIAダイヤラインターフェイスを介したIPv6トラフィックのフロー

次の図は、IPv6 クライアントトラフィックがダイヤラインターフェイスを介してルーティングされ、IPv6 インターネットサイトおよびサービスに到達する方法を示しています。

図 *10 : NAT66 DIA* ダイヤラ インターフェイス サポートのワークフロー



NAT66 DIA でダイヤラインターフェイスを使用する際の制限事項

- DIA のサポート：

  ダイヤラインターフェイスでは NAT66 DIA のみがサポートされています。

- サービス側 NAT66：

  ダイヤラインターフェイスではサービス側 NAT66 はサポートされていません。

- PPPoE ジャンボ フレーム：

  CLI アドオンテンプレートを使用する場合、PPPoE ジャンボフレームは 1800 バイトに制限されます。

- PPPoA ダイヤラインターフェイスのカプセル化：

  次の PPPoA ダイヤラ インターフェイス カプセル化の設定はサポートされていません。Cisco SD-WAN Manager 機能テンプレートを使用した AAL5MUX、AAL5SNAP、AAL5NLPID、または bridge-dot1q です。これらの PPPoA カプセル化を設定する場合は、CLI テンプレートを使用してカプセル化を設定する必要があります。

- DIA トラッカー：

  NAT66 DIA トラッカーは、IP アンナンバード インターフェイスを持つダイヤラインターフェイスではサポートされていません。

- DIA パスの設定：

  NAT66 DIA パスの設定は、WAN インターフェイスのループバックではサポートされていません。

NAT66 DIA を使用したダイヤラインターフェイスの設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a および Cisco Catalyst SD-WAN Manager リリース 20.14.1

設定グループまたは CLI テンプレートを使用して、NAT66 DIA でダイヤラインターフェイスを設定できます。

設定グループを使用した NAT66 DIA でのダイヤラインターフェイスの設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a および Cisco Catalyst SD-WAN Manager リリース 20.14.1

1. Cisco SD-WAN Manager のメニューから、**[Configuration]** > **[Configuration Groups]** を選択します。

   設定グループの作成の詳細については、「Configuration Group Workflows」を参照してください。

2. [Transport and Management Profile] で、VPN 0 機能のインターフェイスの横にある [...] をクリックします。
3. [Add Sub Feature] をクリックし、ドロップダウンリストから次のいずれかのダイヤラインターフェイスを選択します。
   - DSL PPPoE
   - DSL PPPoA
4. DSL PPPoE または DSL PPPoA のオプションを設定します。

   詳細については、「Transport and Management Profile」の「DSL PPPoE」または「DSL PPPoA」セクションを参照してください。
5. [Save] をクリックします。

CLI テンプレートを使用した NAT66 DIA でのダイヤラインターフェイスの設定

サポートされている最小リリース：Cisco IOS XE Catalyst SD-WAN リリース 17.14.1a および Cisco Catalyst SD-WAN Manager リリース 20.14.1

CLI テンプレートの使用の詳細については、CLI テンプレートおよび CLI アドオン機能テンプレートを参照してください。

1. NAT66 DIA を有効にして PPPoE ダイヤラインターフェイスを設定します。

```
interface interface-type-number
 pppoe enable group global
 pppoe-client dial-pool-number dialer-pool-number
!
interface Dialer dialer-number
 mtu bytes
 ipv6 address negotiated
 ipv6 mtu bytes
 nat66 outside
 encapsulation encapsulation-type
 ipv6 tcp adjust-mss bytes
 dialer pool dialer-pool-number
 dialer down-with-vInterface
 ppp chap hostname hostname
 ppp chap password password
 ppp authentication chap callin
 ppp ipcp route default
 service-policy output shape_Dialer dialer-number
```

2. ダイヤラインターフェイスを介して **nat66 outside** を有効にします。

```
nat66 outside
nat66 prefix inside ipv6-address outside interface Dialer interface name vrf Sevice
 VPN number
nat66 prefix inside ipv6-address outside interface Dialer interface name
```

3. サービス側 VPN の NAT66 DIA ルートを設定します。

   サービス側 VPN の NAT DIA ルートの設定に関する詳細については、「NAT DIA ルートの設定」を参照してください。

または

一元管理型データポリシーを使用して、サービス側 VPN の NAT66 DIA ルートを設定します。

nat66 route vrf *vrf-id route-prefix prefix-mask* global

（注） Pool-overload-config を使用した NAT66 マッピングと同じトランザクションでダイヤラインターフェイスを削除すると、追加の非 NAT66 設定が生成されます。次のように別のトランザクションを使用して、各 NAT66 設定を個別に削除します。

```
Device(config)# no nat66 inside source list global-list pool natpool-Dialer100-0 overload
 egress-interface Dialer100
Device(config)# commit

Device(config)# no interface Dialer100
Device(config)# commit
```

NAT66 DIA を使用して PPPoE ダイヤラインターフェイスを設定する例を次に示します。

```
interface Dialer100
 mtu 1492
 ipv6 address negotiated
 nat66 outside
 encapsulation ppp
 ipv6 tcp adjust-mss 1452
 dialer pool 100
 dialer down-with-vInterface
 endpoint-tracker tracker-google
 ppp authentication chap callin
 ppp chap hostname branch1.ppp1
 ppp chap password 7 01100F175804
 ppp ipcp route default
 service-policy output shape_GigabitEthernet0/0/1
!
interface GigabitEthernet0/0/1
 no ipv6 redirects
 pppoe enable group global
 pppoe-client dial-pool-number 100
!
sdwan
 interface Dialer100
  tunnel-interface
   encapsulation ipsec weight 1
   color mpls restrict
  exit
 exit
nat66 prefix inside 2001:A14:18::/80 outside interface Dialer100 vrf 100
nat66 route vrf 100 ::/0 global
```

NAT66 DIA のダイヤラインターフェイス設定の確認

次のセクションでは、ダイヤラインターフェイスの設定を確認する方法について説明します。

NAT66 DIA ルートの確認

```
Device# show nat66 route-dia
Total interface NAT66 DIA enabled count [1]
route add [1] addr [2001:A14:18::] vrfid [2] prefix len [64]
route add [1] addr [2001:A14:19::] vrfid [2] prefix len [64]
```

内部および外部変換時における各プレフィックスカウンタの NAT66 プラットフォームの表示

```
Device# show platform hardware qfp active feature nat66 datapath prefix
prefix hasht 0x89628400 max 2048 chunk 0x8c392bb0 hash_salt 719885386
NAT66 hash[1] id(1) len(64) vrf(0) in: 2001:0a14:0018:0000:0000:0000:0000:0000 out:
 2001:db8:ab02:0000:0000:0000:0000:0000 in2out: 7 out2in: 7
```

PPPoE セッションの表示

show pppoe session コマンドのこの出力例では、PPPoE ダイヤラインターフェイスが `UP` と表示されています。

```
Device# show pppoe session
     1 client session

Uniq ID  PPPoE  RemMAC          Port                    VT  VA         State
           SID  LocMAC                                      VA-st      Type
    N/A    391  84b2.61cc.9903  Gi0/0/1.100          Di100 Vi2        UP
                c884.a1f4.b981  VLAN: 100                  UP
```

次に、**show ppp all** コマンドの出力例を示します。

```
Device# show ppp all
Interface/ID OPEN+ Nego* Fail-     Stage    Peer Address    Peer Name
------------ -------------------- -------- --------------- --------------------
Vi2          LCP+ IPV6CP+ CDPCP-   LocalT   0.0.0.0         SDWAN-AGGREGE
```

PPP ネゴシエーション情報の確認

show interfaces Dialer コマンドのこの出力例では、`Dialer100` が稼働しており、回線プロトコルが稼働しています。

```
Device# show ipv6 interface Dialer100
Dialer100 is up, line protocol is up
 IPv6 is enabled, link-local address is FE80::72EA:1AFF:FE1E:C800
  No Virtual link-local address(es):
  Global unicast address(es):
2001:a0:14:0:8132:C37E:1172:A9C7, subnet is 2001:a0:14:0::/64
valid lifetime 2587577 preferred lifetime 600377
Joined group address(es):
    FF02::1
    FF02::2
    FF02::1:FF00:1
    FF02::1:FF78:5E00
  MTU is 1500 bytes
  ICMP error messages limited to one every 100 milliseconds
  ICMP redirects are enabled
  ICMP unreachables are sent
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds (using 30000)
  ND advertised reachable time is 0 (unspecified)
  ND advertised retransmit interval is 0 (unspecified)
  ND router advertisements are sent every 200 seconds
  ND router advertisements live for 1800 seconds
```

```
  ND advertised default router preference is Medium
  Hosts use stateless autoconfig for addresses.
```

NAT66 DIA でダイヤラインターフェイスを使用するための設定例

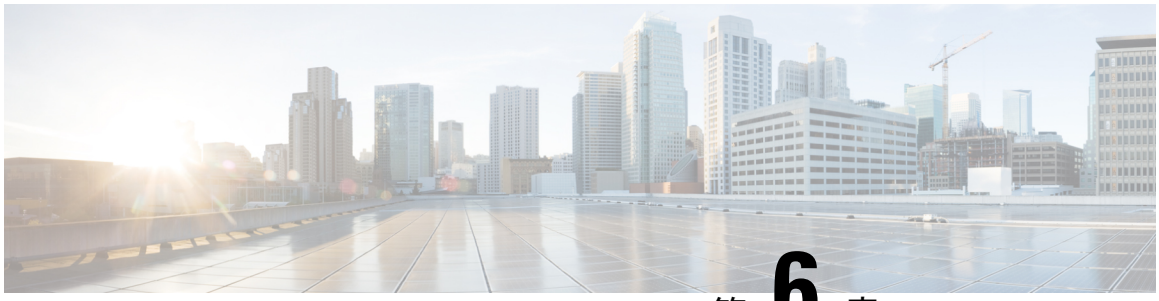
次に、ダイヤラインターフェイスの設定例を示します。

NAT66 DIA のスタティック NAT プレフィックス変換の設定

```
interface Dialer100
    nat66 outside
!
nat66 prefix inside 2001:DB8:380:1::/80 outside 2001:DB8:A1:F:0:1::/80 vrf 1
nat66 prefix inside 2001:DB8:A14:18::/80 outside 2001:DB8:A1:F::/80 vrf 1
nat66 route vrf 1 2001:DB8:A14:19::/64 global
nat66 route vrf 1 2001:DB8:3D0:1::/64 global
```

CLI でステートレス DHCP を使用した DIA の設定

```
interface Dialer100
     nat66 outside
!
nat66 prefix inside 2001:a14:18::/64 outside interface Dialer100 vrf 1
nat66 prefix inside 2001:a14:18::/64 outside interface Dialer100
```



第 6 章

NAT のトラブルシューティング

（注） 簡素化と一貫性を実現するために、Cisco SD-WAN ソリューションは Cisco Catalyst SD-WAN としてブランド名が変更されました。さらに、Cisco IOS XE SD-WAN リリース 17.12.1a および Cisco Catalyst SD-WAN リリース 20.12.1 以降、次のコンポーネントの変更が適用されます。**Cisco vManage** から **Cisco Catalyst SD-WAN Manager** への変更、**Cisco vAnalytics** から **Cisco Catalyst SD-WAN Analytics** への変更、**Cisco vBond** から **Cisco Catalyst SD-WAN Validator** への変更、**Cisco vSmart** から **Cisco Catalyst SD-WAN コントローラ**への変更、および **Cisco コントローラ**から **Cisco Catalyst SD-WAN 制御コンポーネント**への変更。すべてのコンポーネントブランド名変更の包括的なリストについては、最新のリリースノートを参照してください。新しい名前への移行時は、ソフトウェア製品のユーザーインターフェイス更新への段階的なアプローチにより、一連のドキュメントにある程度の不一致が含まれる可能性があります。

概要

この章では、シスコの主題専門家（SME）が作成したドキュメントへのリンクを提供します。サポートチケットを必要とせずに技術的な問題を解決できるようにすることを目的としています。これらのドキュメントで問題を解決できない場合は、該当するシスココミュニティにアクセスすることをお勧めします。この問題をすでに経験し、解決策を提供している可能性のある他のシスコのお客様からは、豊富な情報とアドバイスを入手できます。コミュニティで解決策が見つからない場合は、シスコサポートでサポートチケットを提出するのが最善の方法です。サポートチケットを発行する必要がある場合、これらのドキュメントは、収集してサポートチケットに追加する必要があるデータに関するガイダンスを提供します。参照したサポートドキュメントを指定すると、TAC はドキュメントの所有者と改善要求を作成できます。

サポート記事

このセクションのドキュメントは、各記事の「使用するコンポーネント」セクションにリストされている特定のソフトウェアとハードウェアを使用して作成されています。ただし、これは、それらが使用されるコンポーネントにリストされているものに限定されるという意味ではなく、通常、ソフトウェアおよびハードウェアの新しいバージョンに関連し続けます。ソフトウェアまたはハードウェアに変更があり、コマンドが動作しなくなったり、構文が変更されたり、GUI や CLI がリリースごとに異なって見える可能性があることに注意してください。

このテクノロジーに関連したサポート記事は次のとおりです。

マニュアル	説明
Cisco IOS XE Catalyst SD-WAN ルータでのサービスからトランスポートへのスタティック NAT の設定	このドキュメントでは、Cisco IOS XE Catalyst SD-WAN デバイス でサービス側 VRF からトランスポート VRF へのスタティック NAT を実行するための設定について説明します。
Cisco IOS XE Catalyst SD-WAN ルータでのサービス側スタティック NAT の設定	このドキュメントでは、Cisco IOS-XE® SD-WAN ルータでサービス側 VRF との間でスタティック NAT を実行するための設定について説明します。
Cisco Catalyst SD-WAN のダイレクト インターネット アクセス（DIA）の実装	このドキュメントでは、Cisco Catalyst SD-WAN DIA を実装する方法について説明します。インターネットトラフィックがブランチルータから直接発生する場合の設定について説明します。

フィードバックのリクエスト

ユーザー入力が役立ちます。これらのサポートドキュメントを改善するための重要な側面は、お客様からのフィードバックです。これらのドキュメントは、シスコ内の複数のチームによって所有および管理されていることに注意してください。ドキュメントに固有の問題（不明瞭、混乱、情報不足など）を見つけた場合：

- 対応する記事の右側のパネルにある [Feedback] ボタンを使用して、フィードバックを提供します。ドキュメントの所有者に通知され、記事が更新されるか、削除のフラグが付けられます。
- ドキュメントのセクション、領域、または問題に関する情報と、改善できる点を含めてください。できるだけ詳細に記述してください。

免責事項と注意事項

このマニュアルの情報は、特定のラボ環境に置かれたデバイスに基づいて作成されました。このマニュアルで使用されるデバイスはすべて、初期設定（デフォルト）の状態から作業が開始されています。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。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。