NAT の設定

Cisco IOS XE 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 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 リリース 17.5.1a	この機能を使用すると、Cisco 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 vManage デバイス CLI テンプレートを介してのみ設定できます。
IPv6 トンネルを介した NAT DIA IPv4 のサポート	Cisco IOS XE 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。

機能名	リリース情報	説明
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 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 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。
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 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。

機能名	リリース情報	説明
NAT DIA によるポートフォワーディングのサポート	Cisco IOS XE 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 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 でのみ利用可能でした。
NAT 高速ロギングのサポート	Cisco IOS XE 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。

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 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

- NAT DIA プールは NAT64 ではサポートされていません。
- インターフェイスごとに複数の NAT DIA プールはサポートされていません。
- 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に複数の NAT マッピングが存在することはできません。
- 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。
- 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 vManage 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。

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。
   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。
   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。

1. Cisco vManage 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。

   [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
[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。

パラメータ名	説明
[NAT Pool Prefix Length]	NAT プールのプレフィックス長を入力します。
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。 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

9. 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 *3 : 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。

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 vManage 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

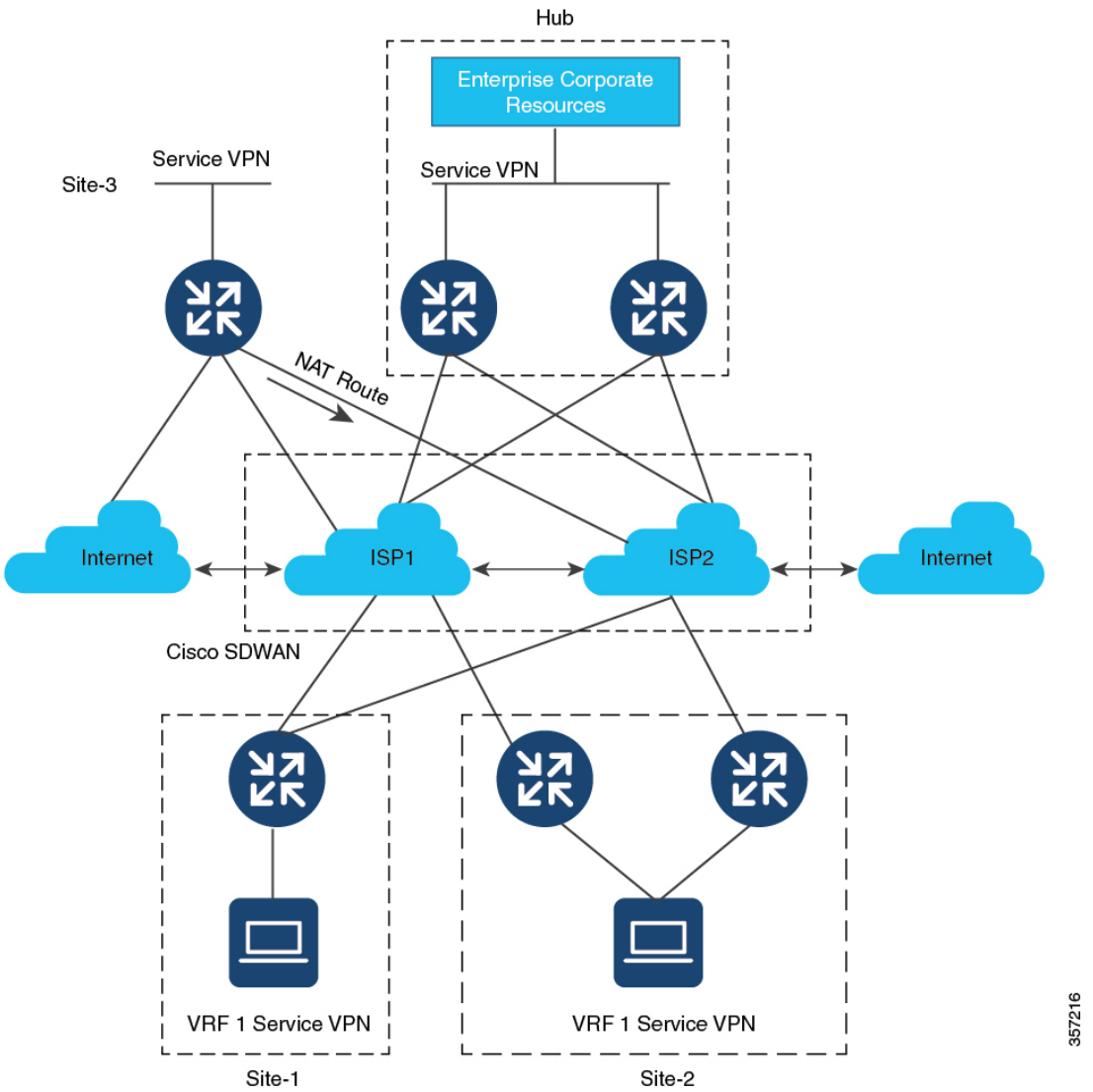
次のセクションでは、OMP を介した NAT ルートのアドバタイズについて説明します。

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 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 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 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 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。

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。

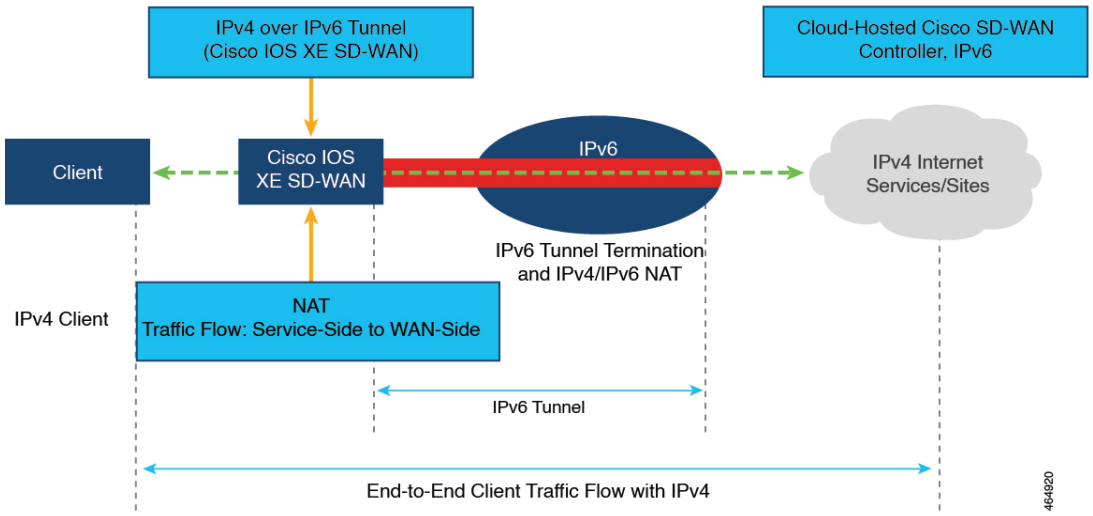
IPv6 トンネルを介した NAT DIA IPv4 の制限事項

- 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*



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 vManage 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 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

Before You Begin

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 vManage 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 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 SD-WAN Systems and Interfaces Guide, Cisco IOS XE* 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 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 SD-WAN Systems and Interfaces Guide, Cisco IOS XE 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

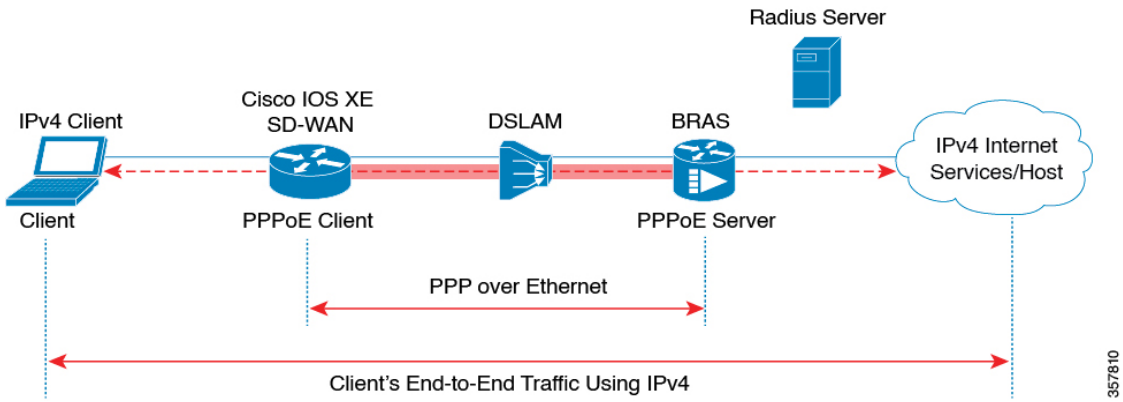
- NAT DIA によるインターフェイス過負荷モードのサポート
- NAT DIA を使用したルートベースおよびデータポリシーベースの構成のサポート
- NAT プールとループバックのサポート
- スタティック NAT 設定のサポート
- スタティック NAT ポート転送のサポート
- 着信コールまたは発信コールの要件に基づいた物理インターフェイスのさまざまな特性
- NAT DIA によるダイヤラインターフェイス経由のスタティックまたはネゴシエートされた IP アドレスのサポート

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 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 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 vManage 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 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 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
```

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 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 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 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 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 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 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 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 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 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。

- DNS
- 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。

（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 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

サポートされている最小リリース：Cisco IOS XE 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
   ```

   ip nat service コマンドに関する詳細については、『*Cisco IOS XE SD-WAN Qualified Command Reference Guide*』を参照してください。

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
   ```

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
```

ALG 設定の確認

サポートされている最小リリース：Cisco IOS XE 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、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 vManage を使用してパケットをキャプチャします。

Cisco vManage を使用したパケットのキャプチャの詳細については、『*Cisco 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。

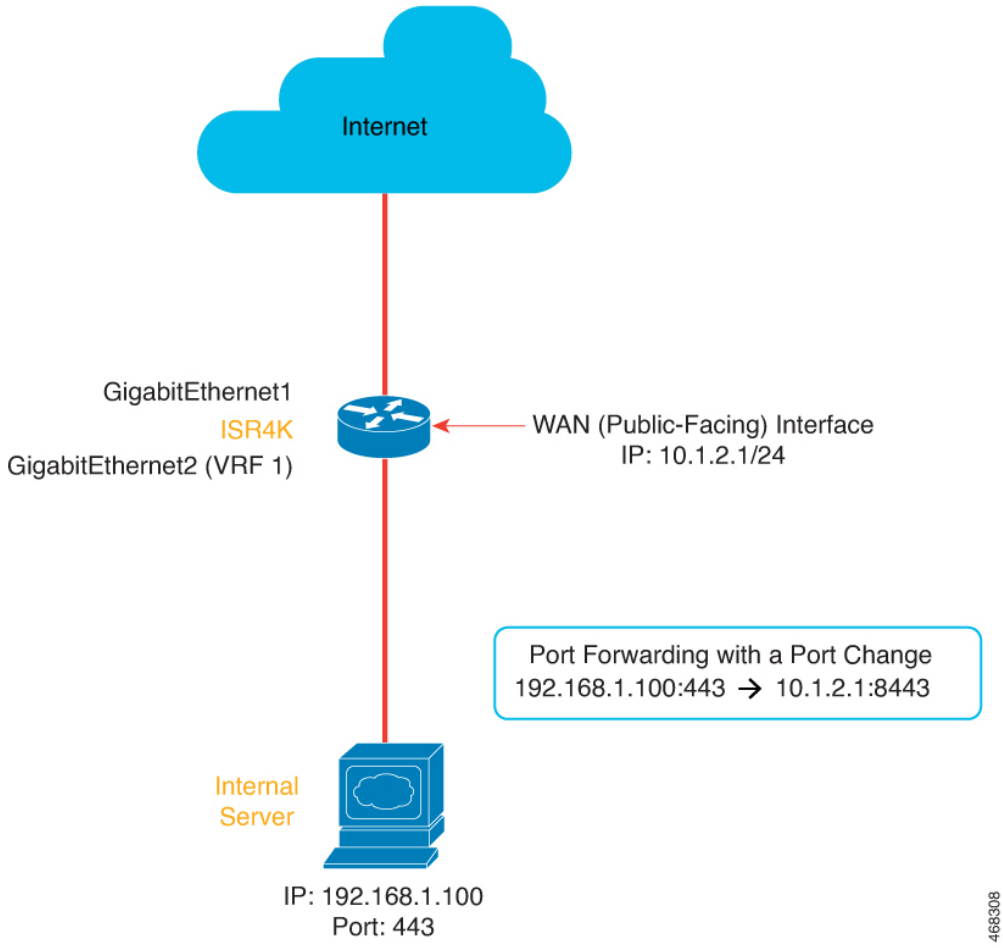
NAT DIA を使用したポートフォワーディングに関する情報

サポートされている最小リリース：Cisco IOS XE 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 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



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 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 負荷分散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。

- 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 でポートフォワーディングを設定するときに、Cisco vManage-reserved ポートを使用することはできません。
- 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。
- 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 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 vManage 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 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。

はじめる前に

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 vManage 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 *4 : 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。
[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 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。

パラメータ名	説明
[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 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） CLI テンプレートのみを使用してインターフェイスポート転送を設定します。Cisco vManage 機能テンプレートを使用してインターフェイスポート転送を設定することはできません。

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
```

NAT DIA を使用したポートフォワーディングの設定の確認

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

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  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。

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 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
```

NAT DIA トラッカー

表 *5 :* 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE SD-WAN デバイス の NAT DIA トラッカー	Cisco IOS XE 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。
Cisco IOS XE SD-WAN デバイスでのインターフェイス ステータス トラッキングのデュアル エンドポイント サポート	Cisco IOS XE リリース 17.7.1a Cisco vManage リリース 20.7.1	この機能により、Cisco vManage 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。

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、ルーターはサービス 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、ルーター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 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。

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）

NAT DIA トラッカーの制限事項

- 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 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 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 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。

NAT DIA トラッカーのワークフロー

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 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。

トラフィックの設定

[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 vManage 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 *6:* 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 *7:* 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。

CLI を使用した NAT DIA トラッカーの設定

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）

Cisco vManage CLI アドオン機能テンプレートおよび 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 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。

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 20
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 20
```

インターフェイスにトラッカーを適用するには、Cisco VPN Interface Cellular または Cisco VPN Interface Ethernet テンプレートでトラッカーを設定します。

（注） インターフェイスに適用できるトラッカーは 1 つだけです。

CLI を使用した NAT DIA トラッキングの設定例

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 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 トラッカー設定のモニタリング

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、次を実行します。

1. Cisco vManage 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 vManage 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 Info] を選択します。

CLI を使用した NAT DIA トラッカー設定のモニタリング

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
 vrf forwarding 0
 endpoint-tracker tracker-t1
```

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
```

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 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
```

サービス側 NAT

表 *8:* 機能の履歴

機能名	リリース情報	説明
Cisco IOS XE SD-WAN デバイス のサービス側 NAT	Cisco IOS XE 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。

機能名	リリース情報	説明
VPN 内サービス側 NAT に対応	Cisco IOS XE 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。
サービス側条件付きスタティック NAT サポート	Cisco IOS XE 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。

機能名	リリース情報	説明
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 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 vManage 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 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 vSmart 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 リリース 17.4.1a および Cisco IOS XE 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 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 リリース 17.4.1a より前のリリースと Cisco IOS XE 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 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 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 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 リリース 17.4.1a および Cisco IOS XE 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 vManage では、最大 32 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 リリース 17.4.1a、Cisco IOS XE リリース 17.3.1a、Cisco IOS XE 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 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 vSmart 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 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

一元化されたデータポリシーは、Cisco vSmart コントローラ で構成され、Cisco 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 vManage 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。一元化されたデータポリシーの作成の詳細については、「Cisco vManage を使用した一元化されたポリシーの構成」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 *9*: 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
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 vSmart 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 vManage 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 10 : 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 ～ 32）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。

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

はじめる前に

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 vManage 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 *11 :* 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 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 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。
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 リリース 17.4.1a および Cisco IOS XE 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 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。

はじめる前に

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 vManage 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 *12*：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 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 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 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 リリース 17.3.1a 以降、**ip nat settings central-policy** コマンドは、Cisco IOS XE SD-WAN デバイス の NAT が Cisco SD-WAN モードで機能するために必要です。Cisco vManage 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 vManage 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 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 vManage 機能テンプレートのサポートは Cisco IOS XE 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 vManage 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 vSmart 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 vManage 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 vSmart 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 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 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 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 vManage 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 vManage 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 *13*：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 *14 :* 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 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 vManage 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 vManage、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 vManage、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 vManage 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 vManage 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 vManage、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 IOS XE 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 vManage 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 vManage 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 vManage 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 vManage 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 vSmart 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 vManage] 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 *15*：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 *16*：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 vManage] 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 vSmart 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 vManage 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 vManage 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 vManage 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。

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。