ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポート

ゾーンベース ファイアウォールおよび NAT のシャーシ間非対称ルーティングサポート機能では、スタンバイ冗長グループからアクティブ冗長グループへのパケット処理のためのパケット転送がサポートされています。この機能が有効になっていない場合は、初期同期（SYN）メッセージを受信しなかったルータに転送されたリターン TCP パケットがドロップされます。これは、パケットが既知のセッションに属していないためです。

このモジュールでは、非対称ルーティングの概要とその設定方法について説明します。

ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポートに関する制約事項

次の制約事項が、シャーシ間非対称ルーティング サポート機能に適用されます。

- 仮想 IP アドレスと仮想 MAC（VMAC）アドレスを使用する LAN は、非対称ルーティングをサポートしません。
- In Service Software Upgrade（ISSU）はサポートされません。

以下の機能は、VRF 対応非対称ルーティング サポート機能でサポートされません。

- Cisco Trustsec
- エッジ スイッチング サービス
- ヘッダー圧縮
- IPSec
- Policy Based Routing（PBR）
- ポート バンドル
- 合法的傍受
- レイヤ 2 トンネリング プロトコル（L2TP）
- Locator/ID Separation Protocol（LISP）内部パケット インスペクション
- セキュア シェル（SSL）VPN
- セッション ボーダー コントローラ（SBC）

ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポートに関する情報

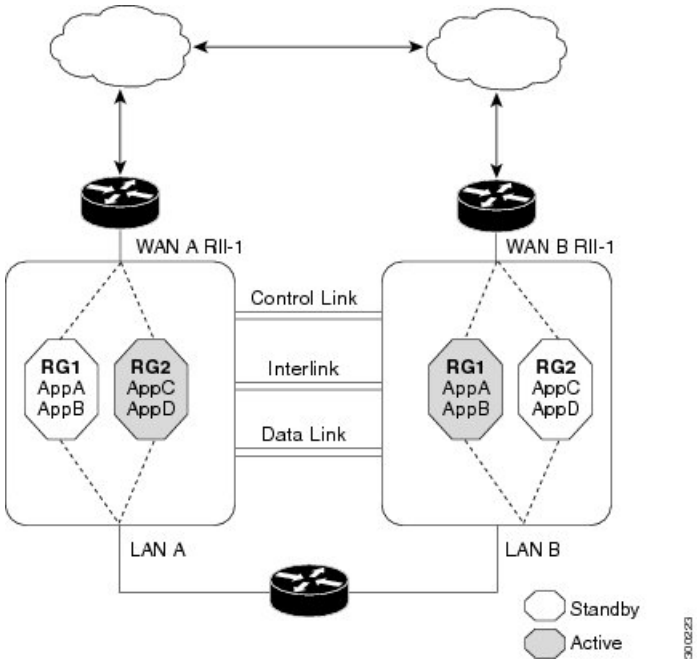
非対称ルーティングの概要

非対称ルーティングは、TCP または UDP 接続の複数のパケットが、異なるルートを経由して異なる方向に送信される場合に発生します。非対称ルーティングでは、1 つの TCP または UDP 接続に属しているパケットは、冗長グループ（RG）の 1 つのインターフェイスを介して転送されますが、同じ RG の別のインターフェイスを介して戻されます。非対称ルーティングでは、パケットフローは同じ RG に残ります。非対称ルーティングを設定する場合、スタンバイ RG で受信したパケットは、処理のためにアクティブ RG にリダイレクトされます。非対称ルーティングが設定されていない場合、スタンバイ RG で受信したパケットはドロップされる可能性があります。

非対称ルーティングは、特定のトラフィックフローの RG を決定します。RG の状態は、パケット処理の決定において重要です。RG がアクティブの場合は、通常のパケットの処理が実行されます。RG がスタンバイ状態で、非対称ルーティングおよび **asymmetric-routing always-divert enable** コマンドを設定している場合、パケットはアクティブ RG に転送されます。スタンバイ RG で受信したパケットをアクティブ RG に常に転送するには、 **asymmetric-routing always-divert enable** コマンドを使用します。

次の図は、別の非対称ルーティング インターリンク インターフェイスを使用して、パケットをアクティブ RG に転送する非対称ルーティング シナリオを示しています。

図 *1* : 非対称ルーティング シナリオ



非対称ルーティングには次のルールが適用されます。

- 冗長インターフェイス識別子（RII）とインターフェイス間のマッピングは 1:1 です。
- インターフェイスと RG 間のマッピングは 1:*n* です。（1 つの非対称ルーティング インターフェイスは複数の RG との間でトラフィックを送受信できます。非対称ルーティング インターフェイス以外のインターフェイス（通常の LAN インターフェイス）では、インターフェイスと RG 間のマッピングは 1:1 です）
- RG およびその RG を使用するアプリケーション間のマッピングは 1:*n* です。（複数のアプリケーションが同じ RG を使用できます）。
- RG とトラフィック フロー間のマッピングは 1:1 です。トラフィック フローは、単一 RG だけにマッピングされる必要があります。トラフィック フローが複数の RG にマッピングされると、エラーが発生します。
- 非対称ルーティング インターリンクに、すべての RG インターリンク トラフィックをサポートできる十分な帯域幅がある限り、RG と非対称ルーティング インターリンク間のマッピングは 1:1 または 1:*n* です。

非対称ルーティングは、転送されるすべてのトラフィックを処理するインターリンク インターフェイスで構成されます。非対称ルーティング インターリンク インターフェイスの帯域幅は、転送が予期されるすべてのトラフィックを処理できるだけの十分な大きさが必要です。IPv4 アドレスは、非対称ルーティング インターリンク インターフェイスで設定され、非対称ルーティング インターフェイスの IP アドレスは、このインターフェイスから到達可能である必要があります。

（注） 非対称ルーティング インターリンク インターフェイスは、インターリンク トラフィックのみに使用し、ハイ アベイラビリティ制御インターフェイスまたはデータ インターフェイスと共有しないことを推奨します。これは、非対称ルーティング インターリンク インターフェイス上のトラフィック量が非常に高くなる可能性があるためです。

ファイアウォールでの非対称ルーティング サポート

ボックス内非対称ルーティングのサポートのために、ファイアウォールは、Internet Control Message Protocol（ICMP）、TCP、および UDP パケットのステートフル レイヤ 3 およびレイヤ 4 インスペクションを行います。ファイアウォールは、パケットのウィンドウ サイズと順序を確認して、TCP パケットのステートフル インスペクションを実行します。ファイアウォールでは、ステートフルインスペクションのためにトラフィックの双方向からのステート情報も必要です。ファイアウォールは ICMP 情報フローの限定的なインスペクションを行います。ICMP エコー要求および応答に関連付けられているシーケンス番号が確認されます。ファイア ウォールでスタンバイ冗長グループ（RG）とパケットフローの同期が行われるのは、そのパケットに対してセッションが確立された後です。確立されるセッションは、TCP、UDP の 2 番目のパケット、および ICMP の情報メッセージに対するスリーウェイ ハンドシェイクです。すべての ICMP フローはアクティブ RG に送信されます。

ファイアウォールにより、ICMP、TCP、および UDP プロトコルに属さないパケットについて、ポリシーのステートレス検証が行われます。

ファイアウォールは、双方向トラフィックを使用して、パケット フローがエージングアウトする時期を決定し、すべての検査対象パケット フローをアクティブ RG に転送します。パス ポリシーを持つパケット フローと、ポリシーなしまたはドロップポリシーと同じゾーンが含まれるパケット フローは転送されません。

（注） スタンバイ RG で受信したパケットをアクティブ RG へ転送する **asymmetric-routing always-divert enable** コマンドは、ファイアウォールではサポートされていません。デフォルトでは、ファイアウォールはすべてのパケット フローをアクティブ RG に強制的に転送します。

NAT での非対称ルーティング

デフォルトでは、非対称ルーティングが設定されている場合、ネットワーク アドレス変換（NAT）は非 ALG パケットをアクティブ RG に転送するのではなく、スタンバイ RG で処理します。NAT のみの設定（ファイアウォールが設定されていない場合）では、パケットの処理にアクティブ RG およびスタンバイ RG の両方を使用できます。NAT のみの設定を使用しており、非同期ルーティングを設定している場合、デフォルトの非同期ルーティング ルールは、NAT がスタンバイ RG でパケットを選択的に処理するというルールです。スタンバイ RG で受信したパケットをアクティブ RG へ転送するように **asymmetric-routing always-divert enable** コ

マンドを設定できます。あるいは、NAT と共にファイアウォールを設定している場合は、デフォルトの非同期ルーティング ルールではパケットが常にアクティブ RG に転送されます。

NAT がスタンバイ RG でパケットを受信したときに、パケットの転送が設定されていない場合、NAT は検索を実行してそのパケットのセッションが存在するかどうかを確認します。セッションが存在しており、そのセッションに関連付けられた ALG がない場合、NAT はスタンバイ RG でパケットを処理します。セッションが存在している場合にスタンバイ RG でパケットを処理すると、NAT トラフィックの帯域幅が大幅に増加します。

NAT ではペイロードの特定と変換、および子フローの作成に ALG が使用されます。ALG が適切に機能するには、双方向トラフィックが必要です。NAT は、ALG に関連付けられているすべてのパケット フローのトラフィックをアクティブ RG に転送する必要があります。このため、セッションに関連付けられている ALG データがスタンバイ RG で検出されたかどうかを確認します。ALG データが存在している場合、非対称ルーティングのためにパケットが転送されます。

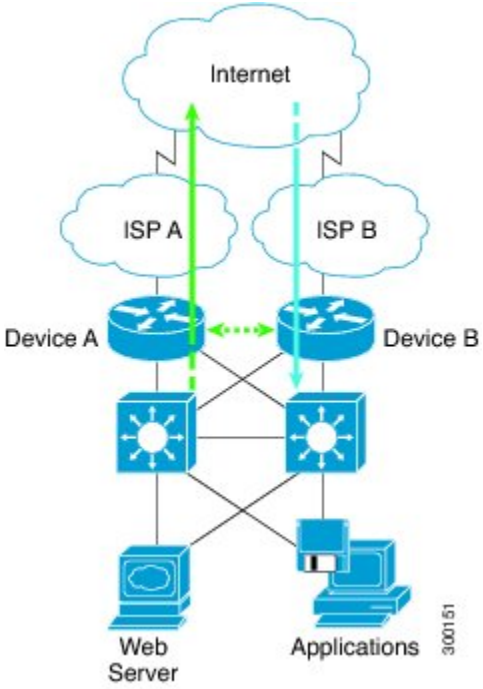
VRF 対応ソフトウェア インフラストラクチャ（VASI）サポートが Cisco IOS XE リリース 3.16S で追加されました。マルチプロトコル ラベル スイッチング（MPLS）非対称ルーティングもサポートされています。

Cisco IOS XE リリース 3.16S では、NAT は ALG、キャリア グレード NAT（CGN）、および Virtual Routing and Forwarding（VRF）インスタンスによる非対称ルーティングをサポートしています。ALG、CGN、または VRF による非対称ルーティングを有効にするために設定を変更する必要はありません。詳細については、「例：VRF による非対称ルーティングの設定」を参照してください。

WAN-LAN トポロジでの非対称ルーティング

非対称ルーティングでは WAN-LAN トポロジだけがサポートされています。WAN-LAN トポロジでは、デバイスが内部の LAN インターフェイスおよび外部の WAN インターフェイスを介して接続されます。WAN リンク経由で受信されるリターン トラフィックのルーティングは制御できません。非対称ルーティングは、WAN-LAN トポロジの WAN リンク経由で受信したリターン トラフィックのルーティングを制御します。次に、WAN-LAN トポロジを示します。

図 *2: WAN-LAN* トポロジでの非対称ルーティング



ゾーンベース ファイアウォールでの VRF 対応非対称ルーティング

Cisco IOS XE リリース 3.14S では、ゾーンベース ファイアウォールで、VRF 対応シャーシ間非対称ルーティング機能がサポートされます。この機能は、マルチプロトコル ラベル スイッチング（MPLS）をサポートします。

非対称ルーティング転送中に、VPN ルーティングおよび転送（VRF）名ハッシュ値が転送パケットとともに送信されます。VRF 名ハッシュ値は、転送後にアクティブ デバイス上でローカル VRF ID とテーブル ID に変換されます。

転送パケットが、ネットワーク アドレス変換（NAT）とゾーンベース ファイアウォールが設定されたアクティブ デバイスに到着すると、ファイアウォールが NAT または NAT64 から VRF ID を取得して、それをファイアウォール セッション キーに保存します。

ここでは、ゾーンベース ファイアウォールのみがデバイスに設定されている場合の非対称ルーティング パケット フローについて説明します。

- デバイスに MPLS が設定されている場合は、転送パケットの VRF ID 処理が非対称ルーティング転送パケットの処理と同じになります。MPLS パケットは、スタンバイ デバイスで MPLS ラベルが削除される場合でも、アクティブ デバイスに転送されます。ゾーンベース ファイアウォールは、出力インターフェイスでパケットを検査し、このインターフェイスで MPLS が検出された場合は、出力 VRF ID を 0 に設定します。入力インターフェイスで MPLS が設定されている場合は、ファイアウォールが入力 VRF ID を 0 に設定します。

- マルチプロトコル ラベル スイッチング（MPLS）パケットがスタンバイ デバイスからアクティブ デバイスに転送されるときに、非対称ルーティング転送が実行される前に MPLS ラベルが削除されます。
- デバイスで MPLS が設定されていない場合は、IP パケットがアクティブ デバイスに転送され、VRF ID が設定されます。ファイアウォールは、出力インターフェイスでパケットを検査するときに、ローカル VRF ID を取得します。

アクティブ デバイスとスタンバイ デバイス間の VRF マッピングは、コンフィギュレーションの変更を必要としません。

NAT での VRF 対応非対称ルーティング

Cisco IOS XE リリース 3.14S では、ネットワーク アドレス変換で VRF 対応シャーシ間非対称ルーティングがサポートされます。VRF 対応シャーシ間非対称ルーティングでは、VPN ルーティングおよび転送（VRF）名のメッセージ ダイジェスト（MD）5 ハッシュを使用して、アクティブ デバイスとスタンバイ デバイス内の VRF とデータパスを特定し、VRF 名ハッシュからローカル VRF ID を、またはローカル VRF ID から VRF 名ハッシュを取得します。

VRF 対応シャーシ間非対称ルーティングでは、アクティブ デバイスとスタンバイ デバイスの VRF に同じ VRF 名を付ける必要があります。ただし、VRF ID は、非対称ルーティング転送またはボックスツーボックス ハイ アベイラビリティ同期の最中にスタンバイ デバイスとアクティブ デバイスの VRF 名に基づいてマップされるため、両方のデバイスで同じにする必要はありません。

VRF 名の MD5 ハッシュ衝突が発生した場合は、VRF に属しているファイアウォール セッションと NAT セッションがスタンバイ デバイスと同期しません。

アクティブ デバイスとスタンバイ デバイス間の VRF マッピングは、コンフィギュレーションの変更を必要としません。

ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポートの設定方法

冗長アプリケーション グループおよび冗長グループ プロトコルの設定

冗長グループは、次の設定要素で構成されています。

- オブジェクトごとに優先度が減らされる量。
- 優先度を減少させる障害（オブジェクト）
- フェールオーバー優先度

- フェールオーバーしきい値
- グループ インスタンス
- グループ名
- 初期化遅延タイマー

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **name** *group-name*
7. **priority** *value* [**failover threshold** *value*]
8. **preempt**
9. **track** *object-number* **decrement** *number*
10. **exit**
11. **protocol** *id*
12. **timers hellotime** {*seconds* | **msec** *msec*} **holdtime** {*seconds* | **msec** *msec*}
13. **authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*] | **key-chain** *key-chain-name*}
14. **bfd**
15. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードをイネーブルにします。 • プロンプトが表示されたら、パスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーションモードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーション冗長性を設定し、冗長性アプリケーション コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長性グループを設定し、冗長性アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**name** *group-name* 例： `Device(config-red-app-grp)# name group1`	プロトコル インスタンス用に、任意指定のエイリアスを指定します。
ステップ 7	**priority** *value* [**failover threshold** *value*] 例： `Device(config-red-app-grp)# priority 100 failover threshold 50`	冗長グループの初期優先度とフェールオーバーしきい値を指定します。
ステップ 8	**preempt** 例： `Device(config-red-app-grp)# preempt`	冗長グループでのプリエンプションをイネーブルにし、スタンバイ デバイスがアクティブ デバイスをプリエンプション処理できるようにします。 • スタンバイ デバイスは、優先度がアクティブ デバイスよりも高いときにのみプリエンプション処理します。
ステップ 9	**track** *object-number* **decrement** *number* 例： `Device(config-red-app-grp)# track 50 decrement 50`	冗長グループの優先度値を指定します。この値は、トラッキング対象のオブジェクトでイベントが発生した場合に減らされます。
ステップ 10	**exit** 例： `Device(config-red-app-grp)# exit`	冗長アプリケーション グループ コンフィギュレーション モードを終了して、冗長アプリケーション コンフィギュレーション モードを開始します。
ステップ 11	**protocol** *id* 例： `Device(config-red-app)# protocol 1`	コントロール インターフェイスに接続されるプロトコルインスタンスを指定し、冗長アプリケーション プロトコル コンフィギュレーション モードを開始します。
ステップ 12	**timers hellotime** {*seconds* | **msec** *msec*} **holdtime** {*seconds* | **msec** *msec*} 例： `Device(config-red-app-prtcl)# timers hellotime 3 holdtime 10`	hello メッセージが送信される間隔、およびデバイスがダウン状態と宣言されるまでの時間を指定します。 • 保留時間は、hellotime の少なくとも 3 倍でなければなりません。
ステップ 13	**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*] | **key-chain** *key-chain-name*}	認証情報を指定します。

	コマンドまたはアクション	目的
	例： `Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100`	
ステップ 14	**bfd** 例： `Device(config-red-app-prtcl)# bfd`	双方向フォワーディング検出（BFD）を使用してコントロール インターフェイスで実行されているフェールオーバー プロトコルを統合し、ミリ秒単位での障害検出を達成できるようにします。 • BFD はデフォルトでイネーブルになっています。
ステップ 15	**end** 例： `Device(config-red-app-prtcl)# end`	冗長アプリケーションプロトコルコンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

データ、コントロール、および非対称ルーティングインターフェイスの設定

この作業では、次の冗長グループ（RG）要素を設定します。

- コントロール インターフェイスとして使用されるインターフェイス。
- データ インターフェイスとして使用されるインターフェイス。
- 非対称ルーティングに使用されるインターフェイス。これはオプションのタスクです。この作業は、ネットワーク アドレス変換（NAT）の非対称ルーティングを設定する場合にのみ実行します。

（注） 別個のインターフェイスで非対称ルーティング、データ、およびコントロールを設定する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **data** *interface-type interface-number*
7. **control** *interface-type interface-number* **protocol** *id*
8. **timers delay** *seconds* [**reload** *seconds*]

9. **asymmetric-routing interface** *type number*
10. **asymmetric-routing always-divert enable**
11. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**redundancy** 例： `Device(config)# redundancy`	冗長コンフィギュレーションモードを開始します。
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーション冗長性を設定し、冗長性アプリケーション コンフィギュレーション モードを開始します。
ステップ 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長性グループ（RG）を設定し、冗長性アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 6	**data** *interface-type interface-number* 例： `Device(config-red-app-grp)# data GigabitEthernet 0/0/1`	RG で使用されるデータ インターフェイスを指定します。
ステップ 7	**control** *interface-type interface-number* **protocol** *id* 例： `Device(config-red-app-grp)# control GigabitEthernet 1/0/0 protocol 1`	RG で使用されるコントロール インターフェイスを指定します。 • また、コントロール インターフェイスは、コントロール インターフェイス プロトコルのインスタンスにも関連付けられます。
ステップ 8	**timers delay** *seconds* [**reload** *seconds*] 例： `Device(config-red-app-grp)# timers delay 100 reload 400`	障害の発生後、またはシステムのリロード後に開始されるロール ネゴシエーションを RG で遅延させるのに必要な時間を指定します。
ステップ 9	**asymmetric-routing interface** *type number* 例：	RG で使用される非対称ルーティング インターフェイスを指定します。

	コマンドまたはアクション	目的
	`Device(config-red-app-grp)# asymmetric-routing interface GigabitEthernet 0/1/1`	
ステップ 10	**asymmetric-routing always-divert enable** 例： `Device(config-red-app-grp)# asymmetric-routing always-divert enable`	スタンバイ RGから受信したパケットをアクティブ RG に常に転送します。
ステップ 11	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了して特権 EXEC モードを開始します。

インターフェイスでの冗長インターフェイス識別子および非対称ルーティングの設定

（注）
- データ インターフェイスまたはコントロール インターフェイスとして設定されているインターフェイスでは、冗長インターフェイス識別子（RII）を設定してはなりません。
- アクティブ デバイスとスタンバイ デバイスの両方で RII および非対称ルーティングを設定する必要があります。
- 仮想 IP アドレスが設定されているインターフェイスでは、非対称ルーティングをイネーブルにすることはできません。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **redundancy rii** *id*
5. **redundancy group** *id* [**decrement** *number*]
6. **redundancy asymmetric-routing enable**
7. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。

	コマンドまたはアクション	目的
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface GigabitEthernet 0/1/3`	冗長グループ（RG）に関連付けるインターフェイスを選択し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**redundancy rii** *id* 例： `Device(config-if)# redundancy rii 600`	冗長性インターフェイス識別子（RII）を設定します。
ステップ 5	**redundancy group** *id* [**decrement** *number*] 例： `Device(config-if)# redundancy group 1 decrement 20`	RG 冗長性トラフィック インターフェイスの設定をイネーブルにし、インターフェイスのダウン時に優先度から減らされる量を指定します。 （注） 非対称ルーティングがイネーブルになっているトラフィック インターフェイスで RG を設定する必要はありません。
ステップ 6	**redundancy asymmetric-routing enable** 例： `Device(config-if)# redundancy asymmetric-routing enable`	各 RG の非対称フロー転送トンネルを確立します。
ステップ 7	**end** 例： `Device(config-if)# end`	インターフェイス コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

非対称ルーティングを使用したダイナミック内部送信元変換の設定

次の設定は、非対称ルーティングを使用したダイナミック内部送信元変換の例です。非対称ルーティングを設定する際に使用できる NAT 設定のタイプは、ダイナミック外部送信元、スタティック内部および外部送信元、ポートアドレス変換（PAT）内部および外部送信元変換です。NAT 設定のそれぞれのタイプの詳細については、「IP アドレス節約のための NAT 設定」の章を参照してください。

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip address** *ip-address mask*

5. **ip nat outside**
6. **exit**
7. **redundancy**
8. **application redundancy**
9. **group** *id*
10. **asymmetric-routing always-divert enable**
11. **end**
12. **configure terminal**
13. **ip nat pool** *name start-ip end-ip* {*mask* | **prefix-length** *prefix-length*}
14. **exit**
15. **ip nat inside source list** *acl-number* **pool** *name* **redundancy** *redundancy-id* **mapping-id** *map-id*
16. **access-list** *standard-acl-number* **permit** *source-address wildcard-bits*
17. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/1/3`	インターフェイスを設定し、インターフェイス コンフィギュレーション モードを開始します。
ステップ 4	**ip address** *ip-address mask* 例： `Device(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイスのプライマリ IP アドレスを設定します。
ステップ 5	**ip nat outside** 例： `Device(config-if)# ip nat outside`	外部と接続されることを示すマークをインターフェイスに付けます。
ステップ 6	**exit** 例： `Device(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードに入ります。
ステップ 7	**redundancy** 例：	冗長性を設定し、冗長性コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
	`Device(config)# redundancy`	
ステップ 8	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーション冗長性を設定し、冗長性アプリケーション コンフィギュレーション モードを開始します。
ステップ 9	**group** *id* 例： `Device(config-red-app)# group 1`	冗長性グループを設定し、冗長性アプリケーション グループ コンフィギュレーション モードを開始します。
ステップ 10	**asymmetric-routing always-divert enable** 例： `Device(config-red-app-grp)# asymmetric-routing always-divert enable`	アクティブデバイスにトラフィックを転送します。
ステップ 11	**end** 例： `Device(config-red-app-grp)# end`	冗長アプリケーション グループ コンフィギュレーション モードを終了して特権 EXEC モードを開始します。
ステップ 12	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 13	**ip nat pool** *name start-ip end-ip* {*mask* | **prefix-length** *prefix-length*} 例： `Device(config)# ip nat pool pool1 prefix-length 24`	グローバル アドレスのプールを定義します。 • IP NAT プール コンフィギュレーション モードを開始します。
ステップ 14	**exit** 例： `Device(config-ipnat-pool)# exit`	IP NAT プール コンフィギュレーション モードを終了し、グローバル コンフィギュレーション モードを開始します。
ステップ 15	**ip nat inside source list** *acl-number* **pool** *name* **redundancy** *redundancy-id* **mapping-id** *map-id* 例： `Device(config)# ip nat inside source list pool pool1 redundancy 1 mapping-id 100`	内部送信元アドレスの NAT を有効にし、マッピング ID を使用して NAT を冗長グループに関連付けます。
ステップ 16	**access-list** *standard-acl-number* **permit** *source-address wildcard-bits* 例： `Device(config)# access-list 10 permit 10.1.1.1 255.255.255.0`	変換される内部アドレス用の標準アクセス リストを定義します。

	コマンドまたはアクション	目的
ステップ 17	**end** 例： `Device(config)# end`	グローバル コンフィギュレーション モードを終了し、特権 EXEC モードを開始します。

ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポートの設定例

例：冗長アプリケーション グループと冗長グループ プロトコルの設定

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name group1
Device(config-red-app-grp)# priority 100 failover threshold 50
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# track 50 decrement 50
Device(config-red-app-grp)# exit
Device(config-red-app)# protocol 1
Device(config-red-app-prtcl)# timers hellotime 3 holdtime 10
Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100
Device(config-red-app-prtcl)# bfd
Device(config-red-app-prtcl)# end
```

例：データ、コントロール、および非対称ルーティングインターフェイスの設定

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# data GigabitEthernet 0/0/1
Device(config-red-app-grp)# control GigabitEthernet 1/0/0 protocol 1
Device(config-red-app-grp)# timers delay 100 reload 400
Device(config-red-app-grp)# asymmetric-routing interface GigabitEthernet 0/1/1
Device(config-red-app-grp)# asymmetric-routing always-divert enable
Device(config-red-app-grp)# end
```

例：インターフェイスでの冗長インターフェイス識別子と非対称ルーティングの設定

```
Device# configure terminal
Device(config)# interface GigabitEthernet 0/1/3
Device(config-if)# redundancy rii 600
Device(config-if)# redundancy group 1 decrement 20
Device(config-if)# redundancy asymmetric-routing enable
Device(config-if)# end
```

例：非対称ルーティングを使用したダイナミック内部送信元変換の設定

```
Device(config)# interface gigabitethernet 0/1/3
Device(config-if)# ip address 10.1.1.1 255.255.255.0
Device(config-if)# ip nat outside
Device(config-if)# exit
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# asymmetric-routing always-divert enable
Device(config-red-app-grp)# end
Device# configure terminal
Device(config)# ip nat pool pool1 prefix-length 24
Device(config-ipnat-pool)# exit
Device(config)# ip nat inside source list pool pool1 redundancy 1 mapping-id 100
Device(config)# access-list 10 permit 10.1.1.1 255.255.255.0
```

例：対称ルーティング ボックスツーボックス冗長性を使用した WAN-WAN トポロジ用の VRF 対応 NAT の設定

次に、WAN 間対称ルーティング設定の例を示します。

```
vrf definition Mgmt-intf
 address-family ipv4
  exit-address-family
!
address-family ipv6
 exit-address-family
!
!
vrf definition VRFA
 rd 100:1
 route-target export 100:1
 route-target import 100:1
 address-family ipv4
  exit-address-family
!
!
```

```
no logging console
no aaa new-model
!
multilink bundle-name authenticated
!
redundancy
 mode sso
 application redundancy
  group 1
   preempt
   priority 120
   control GigabitEthernet 0/0/1 protocol 1
   data GigabitEthernet 0/0/2
!
!
!
!
ip tftp source-interface GigabitEthernet0
ip tftp blocksize 8192
!
track 1 interface GigabitEthernet 0/0/4 line-protocol
!
interface Loopback 0
 ip address 209.165.201.1 255.255.255.224
!
interface GigabitEthernet 0/0/0
 vrf forwarding VRFA
 ip address 192.168.0.1 255.255.255.248
 ip nat inside
 negotiation auto
 bfd interval 50 min_rx 50 multiplier 3
 redundancy rii 2
!
interface GigabitEthernet 0/0/1
 ip address 209.165.202.129 255.255.255.224
 negotiation auto
!
interface GigabitEthernet 0/0/2
 ip address 192.0.2.1 255.255.255.224
 negotiation auto
!
interface GigabitEthernet 0/0/3
 ip address 198.51.100.1 255.255.255.240
 negotiation auto
!
interface GigabitEthernet 0/0/4
 ip address 203.0.113.1 255.255.255.240
 negotiation auto
!
interface GigabitEthernet 0
 vrf forwarding Mgmt-intf
 ip address 172.16.0.1 255.255.0.0
 negotiation auto
!
interface vasileft 1
 vrf forwarding VRFA
 ip address 10.4.4.1 255.255.0.0
 ip nat outside
 no keepalive
!
interface vasiright 1
ip address 10.4.4.2 255.255.0.0
no keepalive
!
```

```
router mobile
!
router bgp 577
 bgp router-id 1.1.1.1
 bgp log-neighbor-changes
 neighbor 203.0.113.1 remote-as 223
 neighbor 203.0.113.1 description PEERING to PTNR neighbor 10.4.4.1 remote-as 577
 neighbor 10.4.4.1 description PEEERING to VASI VRFA interface
!
address-family ipv4
 network 203.0.113.1 mask 255.255.255.240
 network 10.4.0.0 mask 255.255.0.0
 network 209.165.200.224 mask 255.255.255.224
 neighbor 203.0.113.1 activate
 neighbor 10.4.4.1 activate
 neighbor 10.4.4.1 next-hop-self
 exit-address-family
!
address-family ipv4 vrf VRFA
 bgp router-id 4.4.4.4
 network 192.168.0.0 mask 255.255.255.248
 network 10.4.0.0 mask 255.255.0.0
 redistribute connected
 redistribute static
 neighbor 192.168.0.2 remote-as 65004
 neighbor 192.168.0.2 fall-over bfd
 neighbor 192.168.0.2 activate
 neighbor 10.4.4.2 remote-as 577
 neighbor 10.4.4.2 description PEERING to VASI Global intf
 neighbor 10.4.4.2 activate
 exit-address-family
!
ip nat switchover replication http
ip nat pool att_pool 209.165.200.225 209.165.200.225 prefix-length 16
ip nat inside source list 4 pool att_pool redundancy 1 mapping-id 100 vrf VRFA overload
ip forward-protocol nd
!
no ip http server
no ip http secure-server
ip route 203.0.113.1 255.255.255.224 10.4.4.1
ip route 192.168.0.0 255.255.0.0 10.4.4.1
ip route 209.165.200.224 255.255.255.224 10.4.4.1
ip route vrf Mgmt-intf 209.165.200.1 255.255.255.224 172.16.0.0
!
ip prefix-list VRF_Pool seq 5 permit 209.165.200.0/27
ip prefix-list p1-adv-1 seq 5 permit 209.165.200.0/27
ip prefix-list p1-exist-1 seq 5 permit 203.0.113.193/27
logging esm config
access-list 4 permit 203.0.113.193 255.255.255.224
!
control-plane
line console 0
 stopbits 1
!
line vty 0 3
 login
!
line vty 4
 password lab
 login
!
end
```

例：VRF を使用した非対称ルーティングの設定

次に、Virtual Routing and Forwarding（VRF）インスタンスを使用して非対称ルーティングを設定する例を示します。

```
Device(config)# redundancy
Device(config-red)# mode sso
Device(config-red)# application redundancy
Device(config-red-app)# group 1
Device(config-red-app-grp)# name RG1
Device(config-red-app-grp)# preempt
Device(config-red-app-grp)# priority 100 failover threshold 40
Device(config-red-app-grp)# control GigabitEthernet 1/0/3 protocol 1
Device(config-red-app-grp)# data GigabitEthernet 1/0/3
Device(config-red-app-grp)# asymmetric-routing interface GigabitEthernet 1/0/4
Device(config-red-app-grp)# asymmetric-routing always-divert enable
Device(config-red-app-grp)# exit
Device(config-red-app)# exit
Device(config-red)# exit
!
Device(config)# interface TenGigabitEthernet 2/0/0
Device(config-if)# ip vrf forwarding vrf001
Device(config-if)# ip address 10.0.0.1 255.255.255.0
Device(config-if)# ip nat inside
Device(config-if)# exit
!
Device(config)# interface TenGigabitEthernet 3/0/0
Device(config-if)# ip vrf forwarding vrf001
Device(config-if)# ip address 192.0.2.1 255.255.255.0
Device(config-if)# ip nat outside
Device(config-if)# exit
!
Device(config-if)# ip nat pool pool-vrf001 209.165.201.1 209.165.201.30 prefix-length
24
Device(config-if)# ip nat inside source list 1 pool pool-vrf001 redundancy 1 mapping-id
 1 vrf vrf001 match-in-vrf overload
Device(config-if)# end
```

ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポートに関する追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Cisco IOS Master Command List, All Releases』

関連項目	マニュアル タイトル
セキュリティ コマンド	• 『Cisco IOS Security Command Reference Commands A to C』 • 『Cisco IOS Security Command Reference Commands D to L』 • 『Cisco IOS Security Command Reference Commands M to R』 • 『Cisco IOS Security Command Reference Commands S to Z』
ファイアウォール シャーシ間冗長性	「ファイアウォール ステートフル シャーシ間冗長性の設定」モジュール
NAT シャーシ間冗長性	「ステートフル シャーシ間冗長性の設定」モジュール

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

ゾーンベース ファイアウォールおよびNATのシャーシ間非対称ルーティング サポートの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェア イメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1:* ゾーンベース ファイアウォールおよび *NAT* のシャーシ間非対称ルーティング サポートの機能情報

機能名	リリース	機能情報
NAT44 対応の非対称ルーティング拡張	Cisco IOS XE リリース 3.16S	NAT 44 対応の非対称ルーティング拡張機能は、CGN、ALG、VRF、VASI、および MPLS を使用した非対称ルーティングをサポートしています。 追加または変更されたコマンドはありません。
ゾーンベース ファイアウォールと NAT に対するシャーシ間非対称ルーティング サポート	Cisco IOS XE Release 3.5S	ゾーンベース ファイアウォールおよび NAT のシャーシ間非対称ルーティングサポート機能では、スタンバイ冗長グループからアクティブ冗長グループへのパケット処理のためのパケット転送がサポートされています。 次のコマンドが導入または変更されました。**asymmetric-routing**、**redundancy asymmetric-routing enable**
ゾーンベース ファイアウォールの VRF 対応シャーシ間非対称ルーティング サポート	Cisco IOS XE リリース 3.14S	ゾーンベース ファイアウォールでは、VRF 対応シャーシ間非対称ルーティング機能がサポートされています。この機能は MPLS をサポートしています。この機能については設定の変更はありません。 追加または変更されたコマンドはありません。
NAT の VRF 対応シャーシ間非対称ルーティング サポート	Cisco IOS XE リリース 3.14S	NAT では、VRF 対応シャーシ間非対称ルーティング機能がサポートされています。この機能は MPLS をサポートしています。この機能については設定の変更はありません。 追加または変更されたコマンドはありません。

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。