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

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 サポート機能は、パケット処理のための、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の転送をサポートします。 この機能がイネーブルでない場合、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 パケットは、既存で既知のいずれのセッションにも属していないため、ドロップされます。

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

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。 最新の注意事項と機能情報については、Bug Search Tool およびご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。 このモジュールに記載されている機能の詳細を検索し、各機能がサポートされているリリースのリストを確認する場合は、このモジュールの最後にある機能情報の表を参照してください。

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。

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 サポートの制約事項

- マルチプロトコル ラベル スイッチング（MPLS）および VPN を介した非対称ルーティングはサポートされません。
- 仮想IPアドレスおよび仮想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。
- VPN ルーティングおよび転送（VRF）はサポートされません。

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 サポートについて

非対称ルーティングの概要

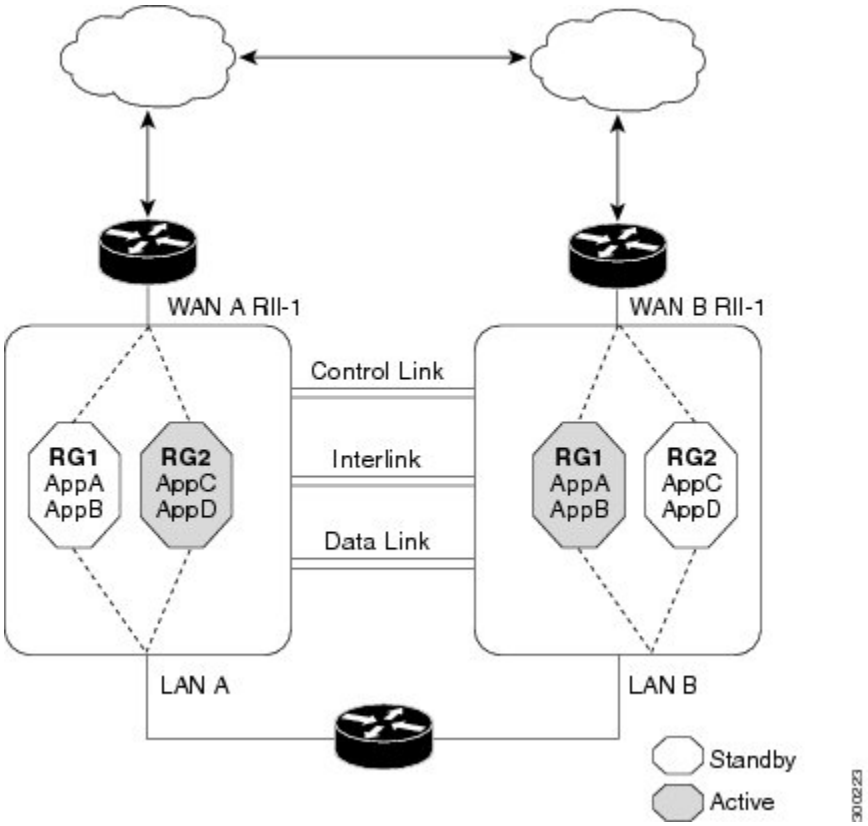
非対称ルーティングは、TCPまたはUDP接続のパケットが異なるルートを介して異なる方向に流れる場合に発生します。 非対称ルーティングでは、1 つの TCP または UDP 接続に属しているパケットは、冗長グループ（RG）の 1 つのインターフェイスを介して転送されますが、同じ RG の別のインターフェイスを介して戻されます。 非対称ルーティングでは、パケット フローは同じ RG に残ります。 非対称ルーティングを設定する場合、スタンバイ RG で受信したパケットは、処理のためにアクティブな RG にリダイレクトされます。 非対称ルーティングが設定されていない場合、スタンバイ RG で受信したパ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

下の図は、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のシナリオ



次のルールが非対称ルーティングに適用されます。

- 1:1 マッピングは、冗長インターフェイス識別子（RII）とインターフェイス間です。
- 1:*n* マッピングは、インターフェイスと RG 間です。（1 つのインターフェイスが複数の RG を持つことができます）。
- 1:*n* マッピングは、RG およびその RG を使用するアプリケーション間です。（複数のアプリケーションが同じ RG を使用できます）。
- 1:1 マッピングは、RG とトラフィック フロー間です。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。
- 1:1 または 1:*n* マッピングは、非対称ルーティング インターリンクがすべての 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 インターリンク間に存在します。

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（HA）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 サポートでは、ファイアウォールは、インターネット制御メッセージ プロトコル（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 ウィンドウ サイズおよびパケットの順序を確認して、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両方向のトラフィック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を確認します。 ファイアウォールは、そのパケットに対するセッションが確立されるまで、スタンバイ冗長グループ（RG）へのパケット フローを同期しません。 確立されたセッションは、TCP、UDP の 2 番目のパケット、および ICMP の情報メッセージのスリーウェイ ハンドシェイクです。 すべての ICMP フローがアクティブな RG に送信されます。

ファイアウォールは、ICMP、TCP、および UDP プロトコルに属さないパケットのポリシーのステートレスな検証を実行します。

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 ポリシーを持ち、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） ファイアウォールは、スタンバイ RG で受信したパケットをアクティブ RG に転送する **asymmetric-routing always-divert enable** コマンドをサポートしません。 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）はスタンバイ RG の非 ALG パケットをアクティブ RG に転送するのはなく、処理します。 NAT

だけの設定（つまり、ファイアウォールが設定されていない場合）では、パケット処理のためにアクティブ RG とスタンバイ RG の両方を使用できます。 NAT のみの設定で、非対称ルーティングを設定している場合、デフォルトの非対称ルーティング ルールでは、NAT はスタンバイ RG でパケットを選択的に処理します。 スタンバイ RG で受信したパケットをアクティブ RG に転送するために、**asymmetric-routing always-divert enable** コマンドを設定できます。 また、NAT とともにファイアウォールを設定した場合、デフォルトの非対称ルーティング ルールでは、パケットをアクティブ RG に常に転送します。

NAT がスタンバイ RG でパケットを受信した場合、パケット転送を設定していないと、NAT は、セッションがそのパケットに存在するかどうかを確認するために検索を実行します。 セッションが存在し、そのセッションに関連付けられた ALG がない場合、NAT はそのパケットをスタンバイ RG で処理します。 セッションが存在している場合、スタンバイ RG のパケットの処理は、NAT トラフィックの帯域幅を大幅に増加させます。

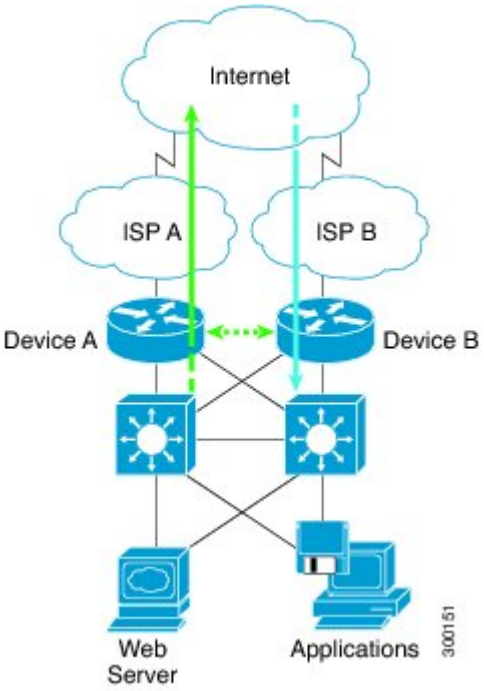
NAT は ALG を使用して、ペイロードを特定および変換し、子フローを作成します。 ALG では、双方向トラフィックが正しく機能する必要があります。 NAT は、ALG に関連付けられたパケット フローに関して、すべてのトラフィックをアクティブ RG に転送する必要があります。 これは、セッションに関連付けられている ALG データがスタンバイ RG にあるかどうかをチェックすることで実現されます。 ALG データが存在する場合、パケットは非対称ルーティングのために転送されます。

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は、WAN-LAN トポロジだけをサポートします。 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 リンク経由で受信したリターン トラフィックのルーティングに対する制御は行われ

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。 下の図は、WAN-LAN トポロジを示しています。

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 ファイアウォールおよびNATの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を減らす量。
- 優先度を減らす障害（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`	アプリケーションの冗長性を設定し、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。

	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`	冗長グループを設定し、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 インスタンスに任意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、その優先度がアクティブ デバイスの優先度よりも高い場合にだけプリエンプトします。
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、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と、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。 • holdtime は、hellotime の少なくとも 3 倍以上にする必要があります。

	コマンドまたはアクション	目的
ステップ 13	**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key* [**timeout** *seconds*] | **key-chain** *key-chain-name*} 例： `Device(config-red-app-prtcl)# authentication md5 key-string 0 n1 timeout 100`	認証情報を指定します。
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の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）に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） 非対称ルーティング、データ、およびコントロールは、ゾーンベース ファイアウォールの個別のインターフェイスで設定する必要があります。ただし、ネットワーク アドレス変換（NAT）では、非対称ルーティング、データ、およびコントロールを同じインターフェイス上に設定できます。

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 モードをイネーブルにします。 • 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`	アプリケーションの冗長性を設定し、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 5	**group** *id* 例： `Device(config-red-app)# group 1`	冗長グループ（RG）を設定し、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 モードを開始します。

	コマンドまたはアクション	目的
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。 • 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起動するロールのネゴシエートを遅らせるために、RG が待機する時間を指定します。
ステップ 9	**asymmetric-routing interface** *type number* 例： `Device(config-red-app-grp)# asymmetric-routing interface GigabitEthernet 0/1/1`	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。
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常にアクティブ RG 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、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たインターフェイス上に冗長インターフェイス識別子（RII）を設定する必要はありません。
- 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上では非対称ルーティングをイネーブルにできません。

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 モードをイネーブルにします。 • 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`	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。

	コマンドまたはアクション	目的
ステップ 4	**redundancy rii** *id* 例： `Device(config-if)# redundancy rii 600`	冗長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`	インターフェイスがダウンした場合、RG 冗長トラフィック インターフェイス コンフィギュレーションをイネーブルにし、優先度から減らす量を指定します。 （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 インターフェイス上で 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 に非同期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による動的な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動的な内部送信元変換の例です。 非対称ルーティングは、NAT 設定のタイプ（動的な内部送信元変換、静的な内部および外部送信元変換、ポートアドレス変換（PAT）の内部および外部送信元変換）を使用して設定できます。 NAT 設定のさまざまなタイプの詳細については、「Configuring NAT for IP Address Conservation」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 モードをイネーブルにします。 • 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。

	コマンドまたはアクション	目的
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： `Device(config)# redundancy`	冗長性を設定し、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 8	**application redundancy** 例： `Device(config-red)# application redundancy`	アプリケーションの冗長性を設定し、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 9	**group** *id* 例： `Device(config-red-app)# group 1`	冗長グループを設定し、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、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。

	コマンドまたはアクション	目的
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 をイネーブルにし、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`	変換する内部アドレスの標準アクセス リストを定義します。
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 ファイアウォールおよびNATの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 グループおよび冗長グループ 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の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および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による動的な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
```

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	「Configuring Firewall Stateful Inter-Chassis Redundancy」モジュール
NAT シャーシ間冗長性	「Configuring Stateful Inter-Chassis Redundancy」モジュール

シスコのテクニカル サポート

説明	リンク
シスコのサポートおよびドキュメンテーション Web サイトでは、ダウンロード可能なマニュアル、ソフトウェア、ツールなどのオンライン リソースを提供しています。 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
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	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 サポート機能は、パケット処理のための、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の転送をサポートします。 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**。