IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポート

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポート機能は、IPv4 トラフィックと IPv6 トラフィックを同時に実行するファイアウォールでの非対称ルーティングをサポートします。 非対称ルーティングは、パケット処理のために、スタンバイ冗長グループからのパケットをアクティブな冗長グループに転送することをサポートします。 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デバイス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IPv6ファイアウォールでの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。

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポートの制約事項

- IPv4 のみが、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サポートされています。
- FTP64 アプリケーション レベル ゲートウェイ（ALG）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。
- マルチプロトコル ラベル スイッチング（MPLS）および仮想ルーティングおよび転送（VRF）インスタンスは、VRF ID マッピングが、アクティブおよびスタンバイの Cisco ASR 1000 シリーズ アグリゲーション サービス ルータ間にないためサポートされていません。

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポートについて

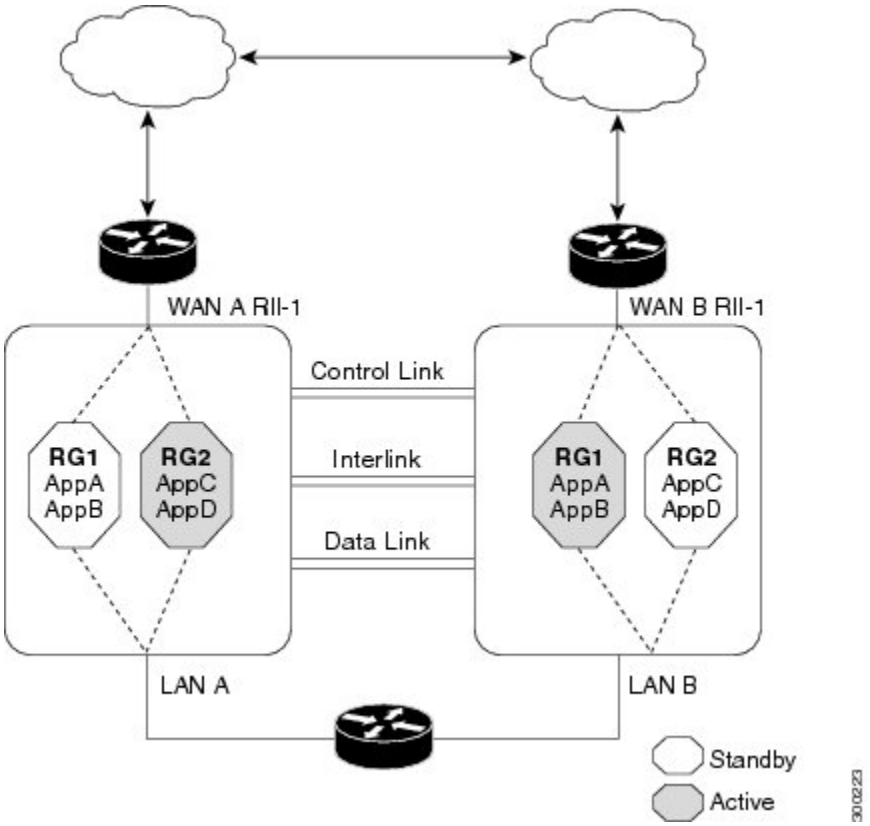
非対称ルーティングの概要

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。

デュアル スタック ファイアウォール

デュアル スタック ファイアウォールは、IPv4 および IPv6 トラフィックを同時に実行するファイアウォールです。 デュアル スタック ファイアウォールは、次のシナリオで設定できます。

- IPv4 トラフィックを実行する 1 つのファイアウォール ゾーン、および IPv6 トラフィックを実行する別のファイアウォール ゾーン。
- IPv4 と IPv6 は、ステートフル ネットワーク アドレス変換 64（NAT64）を使用して展開している場合に共存します。 このシナリオでは、トラフィックは IPv6 から IPv4 へ、およびその逆に流れます。
- 同じゾーン ペアは、IPv4 および IPv6 トラフィックの両方を許可します。

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。

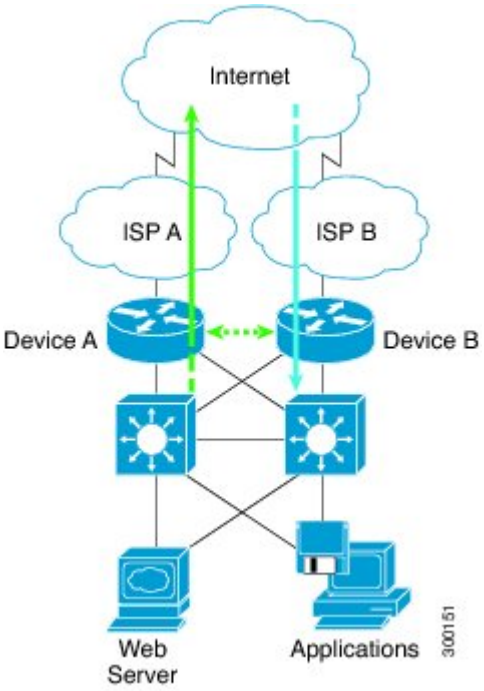
（注） ファイアウォールは、スタンバイ RG で受信したパケットをアクティブ RG に転送する **asymmetric-routing always-divert enable** コマンドをサポートしません。 デフォルトでは、ファイアウォールはすべてのパケット フローをアクティブ RG に強制的に転送します。

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



アプリケーション冗長性のチェックポイント機能サポート

チェックポインティングは、デバイスの現在の状態を保持し、デバイスでの障害発生時にその情報を使用して再起動するプロセスです。 チェックポイント機能（CF）は、プロセス間通信（IPC）プロトコル、および IP ベースの Stream Control Transmission Protocol（SCTP）を使用して、ピア間の通信をサポートします。 CF では、クライアントまたはデバイスにインフラストラクチャを提供して、複数ドメイン内のそれらのピアと通信できるようにします。 デバイスは、アクティブ デバイスからスタンバイ デバイスにチェックポイント メッセージを送信できます。

アプリケーションの冗長性は、同じシャーシ内およびシャーシ間に存在する複数のドメイン（グループとも呼ばれます）をサポートします。 複数のグループに登録されているデバイスは、1 つのグループからそれらのピア グループにチェックポイント メッセージを送信できます。 アプリケーションの冗長性は、シャーシ間ドメイン通信をサポートします。 チェックポインティングは、アクティブ デバイスからスタンバイ グループに対して発生します。 グループの任意の組み合わせがシャーシ間に存在する場合もあります。 シャーシ間の通信は、アプリケーションの冗長性専用のデータ リンク インターフェイス上の SCTP トランスポートによって行われます。

（注） 同じシャーシ内のドメインは相互に通信できません。

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ 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。
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。

	コマンドまたはアクション	目的
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。
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）。

	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	**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。
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。

	コマンドまたはアクション	目的
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。
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。

IPv6 ファイアウォールの設定

IPv4 ファイアウォールと IPv6 ファイアウォールを設定する手順は同じです。IPv6 ファイアウォールを設定するには、IPv6 アドレス ファミリだけが一致するようにクラスマップを設定する必要があります。

match protocol コマンドは、IPv4 トラフィックと IPv6 トラフィックの両方に適用され、IPv4 ポリシーまたは IPv6 ポリシーに含めることができます。

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf-definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **exit**
7. **parameter-map type inspect** *parameter-map-name*
8. **sessions maximum** *sessions*
9. **exit**
10. **ipv6 unicast-routing**
11. **ip port-map** *appl-name* **port** *port-num* **list** *list-name*
12. **ipv6 access-list** *access-list-name*
13. **permit ipv6 any any**
14. **exit**
15. **class-map type inspect match-all** *class-map-name*
16. **match access-group name** *access-group-name*
17. **match protocol** *protocol-name*
18. **exit**
19. **policy-map type inspect** *policy-map-name*
20. **class type inspect** *class-map-name*
21. **inspect** [*parameter-map-name*]
22. **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 モードを開始します。 • 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	**vrf-definition** *vrf-name* 例： `Device(config)# vrf-definition VRF1`	仮想ルーティングおよび転送（VRF）ルーティング テーブル インスタンスを設定し、VRF 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	**address-family ipv6** 例： `Device(config-vrf)# address-family ipv6`	VRF アドレス ファミリ コンフィギュレーション モードを開始して、標準 IPv6 アドレス プレフィックスを伝送するセッションを設定します。
ステップ 5	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	VRF アドレス ファミリ コンフィギュレーション モードを終了し、VRF 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	**exit** 例： `Device(config-vrf)# exit`	VRF コンフィギュレーション モードを終了して、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 7	**parameter-map type inspect** *parameter-map-name* 例： `Device(config)# parameter-map type inspect ipv6-param-map`	ファイアウォールのグローバル検査タイプ パラメータ マップを、検査アクションに関連するしきい値、タイムアウト、およびその他のパラメータに関連付けることができるようにし、パラメータ マップ タイプ検査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	**sessions maximum** *sessions* 例： `Device(config-profile)# sessions maximum 10000`	ゾーン ペア上に存在可能な最大許容セッション数を設定します。
ステップ 9	**exit** 例： `Device(config-profile)# exit`	パラメータ マップ タイプ検査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 10	**ipv6 unicast-routing** 例： `Device(config)# ipv6 unicast-routing`	IPv6 ユニキャスト データグラムの転送をイネーブルにします。

	コマンドまたはアクション	目的
ステップ 11	**ip port-map** *appl-name* **port** *port-num* **list** *list-name* 例： `Device(config)# ip port-map ftp port 8090 list ipv6-acl`	IPv6 アクセス コントロール リスト（ACL）を使用してポートツーアプリケーション マッピング（PAM）を確立します。
ステップ 12	**ipv6 access-list** *access-list-name* 例： `Device(config)# ipv6 access-list ipv6-acl`	IPv6 アクセス リストを定義し、IPv6 アクセス リスト 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	**permit ipv6 any any** 例： `Device(config-ipv6-acl)# permit ipv6 any any`	IPv6 アクセス リストに許可条件を設定します。
ステップ 14	**exit** 例： `Device(config-ipv6-acl)# exit`	IPv6 アクセス リスト 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	**class-map type inspect match-all** *class-map-name* 例： `Device(config)# class-map type inspect match-all ipv6-class`	アプリケーション固有検査タイプ クラス マップを作成し、QoS クラスマップ コンフィギュレーション モードを開始します。
ステップ 16	**match access-group name** *access-group-name* 例： `Device(config-cmap)# match access-group name ipv6-acl`	指定した ACL をベースにクラス マップに対して一致基準を設定します。
ステップ 17	**match protocol** *protocol-name* 例： `Device(config-cmap)# match protocol tcp`	指定されたプロトコルに基づくクラス マップの一致基準を設定します。
ステップ 18	**exit** 例： `Device(config-cmap)# exit`	QoS クラスマップ 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。

	コマンドまたはアクション	目的
ステップ 19	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect ipv6-policy`	プロトコル固有検査タイプ ポリシー マップを作成し、QoS ポリシーマップ コンフィギュレーション モードを開始します。
ステップ 20	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect ipv6-class`	アクションを実行する対象のトラフィック クラスを指定し、QoS ポリシーマップ クラス コンフィギュレーション モードを開始します。
ステップ 21	**inspect** [*parameter-map-name*] 例： `Device(config-pmap-c)# inspect ipv6-param-map`	ステートフル パケット インスペクションをイネーブルにします。
ステップ 22	**end** 例： `Device(config-pmap-c)# end`	QoS ポリシーマップ クラス 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のゾーンおよびゾーン ペアの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *zone-name*
4. **exit**
5. **zone security** *zone-name*
6. **exit**
7. **zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*]
8. **service-policy type inspect** *policy-map-name*
9. **exit**
10. **interface** *type number*
11. **ipv6 address** *ipv6-address*/*prefix-length*
12. **encapsulation dot1q** *vlan-id*
13. **zone-member security** *zone-name*
14. **end**
15. **show policy-map type inspect zone-pair sessions**

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 モードを開始します。 • 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	**zone security** *zone-name* 例： `Device(config)# zone security z1`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 4	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン 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。

	コマンドまたはアクション	目的
ステップ 5	**zone security** *zone-name* 例： `Device(config)# zone security z2`	セキュリティ ゾーンを作成し、セキュリティ ゾーン コンフィギュレーション モードを開始します。
ステップ 6	**exit** 例： `Device(config-sec-zone)# exit`	セキュリティ ゾーン 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 7	**zone-pair security** *zone-pair-name* [**source** *source-zone* **destination** *destination-zone*] 例： `Device(config)# zone-pair security in-2-out source z1 destination z2`	ゾーン ペアを作成し、セキュリティ ゾーンペア 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	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy`	ポリシー マップをトップレベル ポリシー マップに付加します。
ステップ 9	**exit** 例： `Device(config-sec-zone-pair)# exit`	セキュリティ ゾーンペア 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 10	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0.1`	サブインターフェイスを設定し、サブインターフェイス コンフィギュレーション モードを開始します。
ステップ 11	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-subif)# ipv6 address 2001:DB8:2222:7272::72/64`	IPv6 の一般的なプレフィックスに基づいて IPv6 アドレスを設定し、インターフェイスまたはサブインターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 12	**encapsulation dot1q** *vlan-id* 例： `Device(config-subif)# encapsulation dot1q 2`	インターフェイスで使用するカプセル化方式を設定します。

	コマンドまたはアクション	目的
ステップ 13	**zone-member security** *zone-name* 例： `Device(config-subif)# zone-member security z1`	ゾーン メンバーとしてインターフェイスを設定します。 • *zone-name* 引数では、**zone security** コマンドを使用して設定したゾーンのいずれかを設定する必要があります。 • インターフェイスがセキュリティ ゾーンにある場合、そのインターフェイスを通るトラフィックはどちらの方向でもすべて（デバイス宛またはデバイス発信のトラフィックを除く）デフォルトでドロップされます。 ゾーン メンバーであるインターフェイスをトラフィックが通過することを許可するには、そのゾーンをゾーンペアの一部にして、そのゾーンペアにポリシーを適用する必要があります。 ポリシーで、inspect または pass アクションを通してトラフィックが許可されると、トラフィックはインターフェイスを通過します。
ステップ 14	**end** 例： `Device(config-subif)# end`	サブインターフェイス コンフィギュレーション モードを終了して、特権 EXEC モードを開始します。
ステップ 15	**show policy-map type inspect zone-pair sessions** 例： `Device# show policy-map type inspect zone-pair sessions`	ポリシー マップが指定したゾーン ペアに適用されているため、作成されたステートフル パケット インスペクション セッションを表示します。 • このコマンドの出力は、IPv4 と IPv6 の両方のファイアウォール セッションを表示します。

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ 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：IPv6 ファイアウォールの設定

```
Device# configure terminal
Device(config)# vrf-definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# exit
Device(config)# parameter-map type inspect ipv6-param-map
Device(config-profile)# sessions maximum 10000
Device(config-profile)# exit
Device(config)# ipv6 unicast-routing
Device(config)# ip port-map ftp port 8090 list ipv6-acl
Device(config)# ipv6 access-list ipv6-acl
Device(config-ipv6-acl)# permit ipv6 any any
Device(config-ipv6-acl)# exit
Device(config)# class-map type inspect match-all ipv6-class
Device(config-cmap)# match access-group name ipv6-acl
Device(config-cmap)# match protocol tcp
Device(config-cmap)# exit
Device(config)# policy-map type inspect ipv6-policy
Device(config-pmap)# class type inspect ipv6-class
Device(config-pmap-c)# inspect ipv6-param-map
Device(config-pmap-c)# end
```

例：非対称ルーティングのゾーンおよびゾーン ペアの設定

```
Device# configure terminal
Device(config)# zone security z1
Device(config-sec-zone)# exit
Device(config)# zone security z2
Device(config-sec-zone)# exit
Device(config)# zone-pair security in-to-out source z1 destination z2
Device(config-sec-zone-pair)# service-policy type inspect ipv6-policy
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0.1
Device(config-if)# ipv6 address 2001:DB8:2222:7272::72/64
Device(config-if)# encapsulation dot1q 2
Device(config-if)# zone member security z1
Device(config-if)# end
```

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ 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』
ファイアウォール 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』

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

IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ 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*：*IPv6* ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポートの機能情報

機能名	リリース	機能情報
IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポート	Cisco IOS XE Release 3.8S	IPv6 ゾーンベース ファイアウォールのシャーシ間ハイ アベイラビリティ サポート機能は、IPv4 トラフィックと IPv6 トラフィックを同時に実行するファイアウォールでの非対称ルーティングをサポートします。 非対称ルーティングは、パケット処理のために、スタンバイ冗長グループからのパケットをアクティブな冗長グループに転送することをサポートします。 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デバイス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。 この機能によって導入または変更されたコマンドはありません。