IPv6 ゾーンベース ファイアウォールのボックスツーボックス 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ボックスツーボックス ハイ アベイラビリティ サポート機能では、IPv6 ファイアウォールの冗長グループ（RG）に基づいてハイ アベイラビリティ（HA）がサポートされています。この機能により、相互にバックアップとして動作するデバイスのペアを設定できます。この機能を設定し、複数のフェールオーバー条件に基づいてアクティブ デバイスを判断できます。この機能は、IPv6 パケット インスペクションの FTP66 アプリケーション レイヤ ゲートウェイ（ALG）をサポートしています。

このモジュールでは、ボックスツーボックス（B2B）HA サポートに関する情報を提供し、この機能を設定する方法について説明します。

IPv6 ゾーンベース ファイアウォールに対するボックスツーボックス ハイ アベイラビリティ サポートに関する前提条件

- ファイアウォールにアタッチされたインターフェイスは、冗長インターフェイス識別子（RII）を同じにする必要があります。
- アクティブ デバイスとスタンバイ デバイスは、ゾーンベース ポリシー ファイアウォール設定を同じにする必要があります。
- アクティブ デバイスとスタンバイ デバイスは、同じバージョンのシスコ ソフトウェア上で動作する必要があります。アクティブ デバイスとスタンバイ デバイスは、スイッチ経由で接続する必要があります。
- アクティブ デバイスとスタンバイ デバイスの両方のボックスツーボックス（B2B）設定は同じにする必要があります。これは、これらのデバイス間の設定の自動同期機能がないためです。
- 非対称ルーティング トラフィックを通過させるためには、class-default クラスの通過アクションを設定する必要があります。class-default クラスは、ポリシー内のユーザ定義クラスのどれとも一致しないすべてのパケットを表すシステム定義のクラス マップです。
- 2 つの LAN インターフェイス間でゾーン ペアを設定する場合は、両方のインターフェイス上で同じ冗長グループ（RG）が設定されていることを確認します。ゾーンペア設定は、LAN インターフェイスが別の RG に属している場合はサポートされません。

IPv6 ゾーンベース ファイアウォールに対するボックスツーボックス ハイ アベイラビリティ サポートに関する制約事項

- ボックスツーボックス（B2B）リンク間インターフェイスでは、IPv4 のみがサポートされます。
- マルチプロトコル ラベル スイッチング（MPLS）と Virtual Routing and Forwarding（VRF）はサポートされません。
- シャーシ内のデュアル エンベデッド サービス プロセッサ（ESP）またはデュアル ルート プロセッサ（RP）を搭載した Cisco ASR 1006 および 1013 アグリゲーション サービス ルータはサポートされません。これは、ボックス間ハイ アベイラビリティ（HA）とボックス内 HA の共存がサポートされないためです。

シャーシ内のシングル ESP とシングル RP を搭載した Cisco ASR 1006 および Cisco ASR 1013 アグリゲーション サービス ルータは、シャーシ間冗長性をサポートします。

- デュアル IOS デーモン（IOSd）が設定されている場合、デバイスはファイアウォール ステートフル シャーシ間冗長性の設定をサポートしません。
- IPv6 ファイアウォールを使用したステートレス ネットワーク アドレス変換 64（NAT64）はサポートされません。

IPv6 ゾーンベース ファイアウォールに対するボックス ツーボックス ハイ アベイラビリティ サポートに関する情報

ゾーンベース ポリシー ファイアウォール ハイ アベイラビリティの概要

ハイアベイラビリティは、ネットワークのどの場所でも起こり得る障害からの迅速な回復を可能にすることで、ネットワーク全体の保護を実現します。ハイ アベイラビリティは、ユーザ アプリケーションやネットワーク アプリケーションの中断からの迅速な回復を可能にします。

ゾーンベースポリシーファイアウォールは、アクティブ/アクティブおよびアクティブ/スタンバイ ハイ アベイラビリティ フェールオーバーと非対称ルーティングをサポートします。

アクティブ/アクティブ フェールオーバーは、フェールオーバーに関与している両方のデバイスが同時にトラフィックを転送できるようにします。

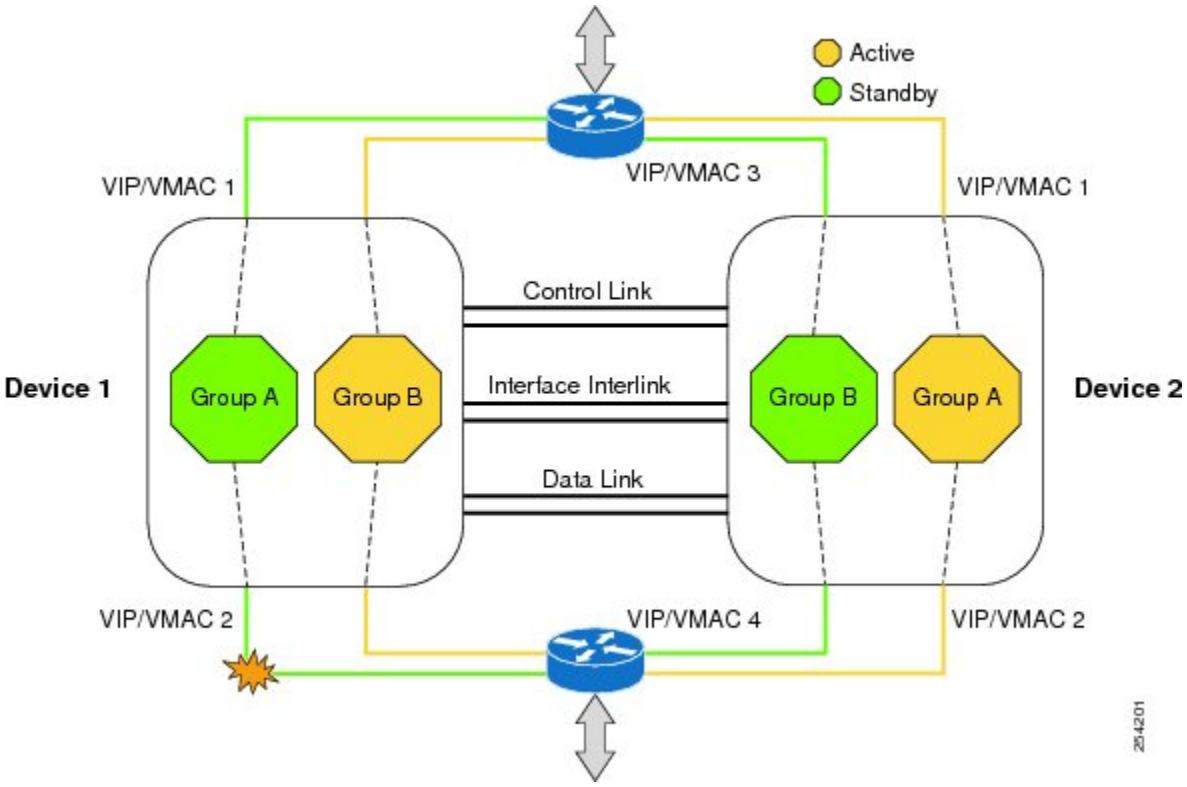
アクティブ/スタンバイ ハイ アベイラビリティ フェールオーバーが設定されている場合は、一度にフェールオーバーに関与している一方のデバイスだけがトラフィックを処理し、もう一方のデバイスはスタンバイ モードに入って定期的にアクティブ デバイスからセッション情報を同期します。

非対称ルーティングは、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デバイス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。

ボックスツーボックス ハイアベイラビリティの動作

相互にホットスタンバイとして動作するようにデバイスのペアを設定できます。冗長性はインターフェイスごとに設定します。冗長インターフェイスのペアは、冗長グループ（RG）と呼ばれます。図 1 は、アクティブ/アクティブ フェールオーバー シナリオを示しています。2 つの発信インターフェイスを持つデバイスのペアに対して2つの冗長グループがどのように設定されているかを示します。

図 *1:* 冗長グループの設定：*2* つの発信インターフェイス



冗長デバイスは、設定可能なコントロール リンク、データ同期リンク、およびインターリンク インターフェイスによって結合されます。コントロール リンクは、デバイスのステータスを通信するために使用されます。データ同期リンクは、ファイアウォールからステートフル情報を転送し、ステートフルデータベースを同期するために使用されます。冗長インターフェイスのペアは、同じ固有 ID 番号（冗長インターフェイス識別子（RII）と呼ばれます）を使用して設定されます。ルーティング テーブルは、アクティブからスタンバイには同期されません。

非対称ルーティングは、ファイアウォール HA の一部としてサポートされています。リターン トラフィックがスタンバイ デバイスに入る LAN-WAN シナリオでは、非対称ルーティングがサポートされます。非対称ルーティングの機能を実装するには、非対称トラフィックの専用インターフェイス（インターリンク インターフェイス）で両方の冗長デバイスを設定します。この専用インターフェイスは、スタンバイ WAN インターフェイスに着信するトラフィックを、アクティブ デバイスにリダイレクトします。

冗長グループ メンバーのステータスは、コントロール リンクで送信される hello メッセージを使用することで判断できます。いずれかのデバイスが、設定された時間内に hello メッセージに応答しない場合、ソフトウェアは障害が発生したと見なし、スイッチオーバーが開始されます。ミリ秒単位でエラーを検出するには、フェールオーバー プロトコルをコントロール リンクで実行します。hello メッセージについて次のパラメータを設定できます。

- Active timer。
- Standby timer。

- Hello time：hello メッセージが送信される間隔。
- Hold time：アクティブ デバイスまたはスタンバイ デバイスがダウンしていると宣言されるまでの時間。

Hello time のデフォルトは、Hot Standby Router Protocol（HSRP）に合わせるために 3 秒です。Hold time のデフォルトは 10 秒です。これらのタイマーは、**timers hellotime msec** コマンドを使用してミリ秒単位で設定することもできます。

スイッチオーバーの影響を受けるインターフェイスのペアを判断するには、冗長インターフェイスの各ペアに対して固有の ID を設定する必要があります。この ID は、インターフェイスに関連付けられている RII です。

スイッチオーバーの原因

スイッチオーバーが発生する別の要因として、各デバイスで設定可能な優先度設定があります。優先度が最も高いデバイスがアクティブ デバイスになります。アクティブ デバイスまたはスタンバイ デバイスで障害が発生した場合、重みと呼ばれる設定可能な数値分、ルータの優先度が下がります。アクティブ デバイスの優先度が、スタンバイ デバイスの優先度を下回る場合、スイッチオーバーが発生し、スタンバイ デバイスがアクティブ デバイスになります。このデフォルトの動作を無効にするには、冗長グループの preemption 属性を無効にします。また、インターフェイスのレイヤ 1 状態がダウンになった場合、各インターフェイスを設定して優先度を下げます。設定された優先度が、冗長グループのデフォルトの 優先度を上書きします。

冗長グループの優先度が変更されるエラー イベントごとに、タイム スタンプ、影響を受けた冗長グループ、変更前の優先度、変更後の優先度、およびエラーイベントの原因の説明を含む syslog エントリが生成されます。

スイッチオーバーが発生する原因となるもう 1 つの状況は、デバイスまたはインターフェイスの優先度が、設定可能なしきい値レベルを下回る場合です。

スタンバイ デバイスへのスイッチオーバーは次の条件で発生します。

- アクティブデバイスで停電またはリロードが発生した場合（クラッシュも含まれます）。
- アクティブ デバイスのランタイム優先度が、スタンバイ デバイスの優先度を下回った場合。
- アクティブ デバイスのランタイム優先度が、設定したしきい値レベルを下回った場合。
- アクティブデバイスの冗長グループを手動でリロードするには、**redundancy application reload group** *rg-number* コマンドを使用します。
- 任意のモニタ対象インターフェイスで 2 つの連続する hello メッセージに失敗した場合、インターフェイスは強制的にテストモードになります。いずれのデバイスもインターフェイス上のリンク ステータスを確認してから、次のテストを実行します。
  - ネットワーク アクティビティ テスト
  - Address Resolution Protocol（ARP）テスト
  - ブロードキャスト ping テスト

アクティブ/アクティブ フェールオーバー

アクティブ/アクティブ フェールオーバー構成では、両方のデバイスがネットワーク トラフィックを渡すことができます。アクティブ/アクティブ フェールオーバーでは、各冗長グループ（RG）のインターフェイスの仮想 MAC（VMAC）アドレスが生成されます。

アクティブ/アクティブ フェールオーバー ペアの 1 つのデバイスがプライマリ（アクティブ）デバイスとして指定され、もう1つのデバイスがセカンダリ（スタンバイ）デバイスとして指定されます。アクティブ/スタンバイ フェールオーバーの場合とは異なり、両方のデバイスが同時に起動された場合、この指定ではどちらのデバイスがアクティブになるかは指示しません。代わりに、プライマリまたはセカンダリの指定によって次の点が決定します。

- デバイスが同時に起動したときに、実行コンフィギュレーションをフェールオーバー ペアに提供するデバイス。
- デバイスが同時に起動したときに、フェールオーバー RG がアクティブ状態のデバイス。このコンフィギュレーションの各フェールオーバー RG は、プライマリまたはセカンダリ デバイス プリファレンスで設定されます。1 つのデバイスで両方のフェールオーバー RG がアクティブ状態であり、スタンバイ フェールオーバー RG がもう一方のデバイスにあるように設定できます。また、1 つのフェールオーバー RG をアクティブ状態にし、もう 1 つの RG を 1 つのデバイスでスタンバイ状態に設定することもできます。

アクティブ/スタンバイ フェールオーバー

アクティブ/スタンバイ フェールオーバーでは、スタンバイ デバイスを使用して、障害が発生したデバイスの機能を引き継ぐことができます。障害が発生したアクティブデバイスはスタンバイ状態になり、スタンバイデバイスがアクティブ状態になります。アクティブ状態になったデバイスは、障害が発生したデバイスのIPアドレスとMACアドレスを引き継いで、トラフィックの処理を開始します。スタンバイ状態になったデバイスは、スタンバイ IP アドレスと MAC アドレスを引き継ぎます。ネットワーク デバイスは MAC to IP アドレス ペアでの変更を認識しないため、ネットワーク上のいずれの場所でも Address Resolution Protocol（ARP）エントリが変更されたり、タイムアウトが生じたりすることはありません。

アクティブ/スタンバイ シナリオでは、フェールオーバー ペアの 2 つのデバイス間の主な違いは、どのデバイスがアクティブで、どのデバイスがスタンバイであるか、つまり、どの IP アドレスを使用し、どのデバイスがアクティブにトラフィックを渡すかということに関連します。両方のデバイスが同時にスタートアップした場合（さらに動作ヘルスが等しい場合）、アクティブ デバイスは常にアクティブ デバイスになります。アクティブ デバイスの MAC アドレスは常に、アクティブ IP アドレスと組み合わせられます。

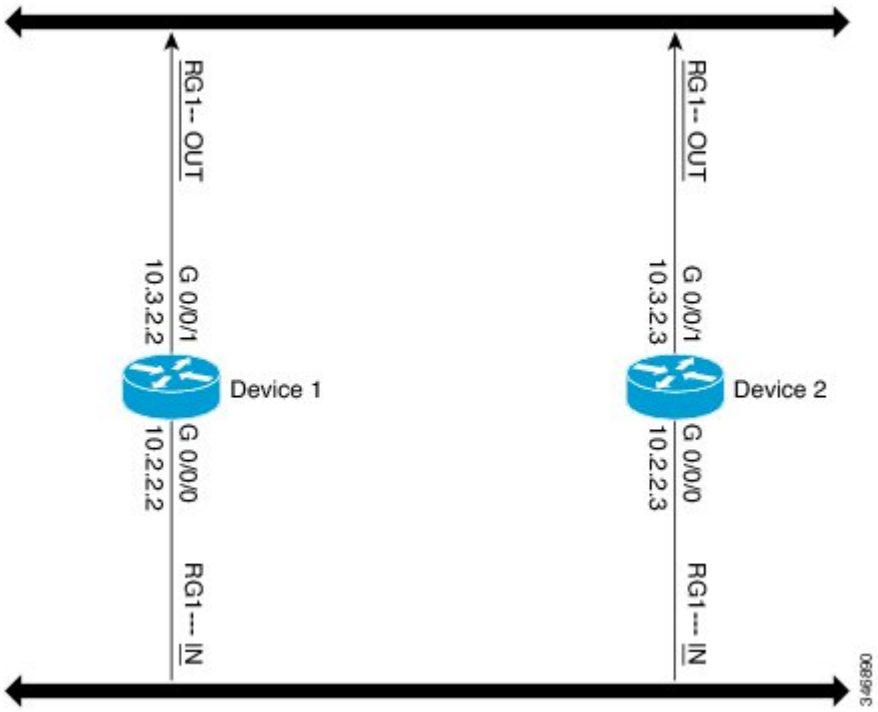
NAT ボックスツーボックス高可用性 LAN/LAN トポロジ

LAN/LANトポロジに参加するすべてのデバイスは、内部と外部の両方でLANインターフェイスを介して相互接続されます。次の図に、NATボックスツーボックスLAN/LANトポロジを示します。ネットワーク アドレス変換（NAT）はアクティブ/スタンバイ モードで行われ、ピア

は 1 つの冗長グループ（RG）にまとめられます。すべてのトラフィックまたはトラフィックのサブセットに NAT 変換が適用されます。

（注） フェールオーバーは、RGインフラストラクチャでリッスンする障害によってのみ発生します。

図 *2 : NAT* ボックスツーボックス高可用性 *LAN/LAN* トポロジ



WAN-LAN トポロジ

WAN-LAN トポロジでは、2 つのデバイスが内部の LAN インターフェイスと外部の 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。

WAN リンクは、同じサービス プロバイダーまたは別のサービス プロバイダーから提供できます。ほとんどの場合、WAN リンクは別のサービス プロバイダーから提供されます。WAN リンクを最大限に活用するには、フェールオーバーを提供するように外部デバイスを設定します。

LAN ベースのインターフェイスでは、クライアント情報の交換とフェールオーバーの高速化のために、ハイ アベイラビリティ仮想 IP アドレスが必要です。WAN ベースのインターフェイスでは、フェールオーバーに **redundancy group** *id* **ip** *virtual-ip* **decrement** *value* コマンドが使用されます。

排他的仮想 IP アドレスと排他的仮想 MAC アドレス

仮想 IP（VIP）アドレスと仮想 MAC（VMAC）アドレスは、セキュリティ アプリケーションが、トラフィックを受信するインターフェイスを制御するために使用します。インターフェイスは別のインターフェイスとペアにされ、これらのインターフェイスは同じ冗長グループ（RG）に関連付けられます。アクティブな RG に関連付けられているインターフェイスは、VIP アドレスと VMAC を排他的に所有します。アクティブデバイスの Address Resolution Protocol（ARP）プロセスによって、VIP への ARP 要求に対する ARP 応答が送信されます。また、インターフェイスのイーサネット コントローラは、VMAC 宛てのパケットを受信するようにプログラミングされます。RG のフェールオーバーが発生すると、VIP と VMAC の所有権は変化します。新しくアクティブになった RG に関連付けられたインターフェイスは、gratuitous ARP を送信し、インターフェイスのイーサネット コントローラをプログラミングして、VMAC 宛てのパケットを受け入れます。

IPv6 のサポート

各冗長グループ（RG）を、同じ冗長インターフェイス識別子（RII）で IPv4 と IPv6 の両方の仮想 IP（VIP）アドレスのトラフィック インターフェイスに割り当てることができます。各 RG は RII ごとに一意の仮想 MAC（VMAC）アドレスを使用します。RG では、IPv6 リンクローカル VIP とグローバル VIP がインターフェイス上に共存します。

トラフィック インターフェイス上の各 RG に対して IPv4 VIP、リンクローカル IPv6 VIP、および/またはグローバル IPv6 VIP を設定できます。IPv6 リンクローカル VIP は、スタティック ルートまたはデフォルト ルートを設定する場合に主に使用されます。IPv6 グローバル VIP は、LAN トポロジと WAN トポロジの両方で広く使用されています。

IPv4 VIP を設定する前に、物理 IP アドレスを設定する必要があります。

FTP66 ALG サポートの概要

ファイアウォールでは、IPv6 パケットとステートフル ネットワーク アドレス変換 64（NAT64）のインスペクションをサポートしています。FTP を IPv6 パケット インスペクションに基づいて機能させるには、アプリケーション層ゲートウェイ（ALG）（別名アプリケーション レベル ゲートウェイ（ALG））FTP66 が必要です。FTP66 ALG は、オールインワン FTP ALG およびワン FTP ALG とも呼ばれています。

FTP66 ALG では、次の機能をサポートしています。

- ファイアウォール IPv4 パケット インスペクション
- ファイアウォール IPv6 パケット インスペクション
- NAT の設定
- NAT64 の設定（FTP64 サポートを使用）
- NAT とファイアウォールの設定
- NAT64 とファイアウォールの設定

FTP66 ALG には、次のセキュリティ上の脆弱性があります。

- パケット セグメンテーション攻撃：FTP ALG ステート マシンではセグメント化されたパケットを検出できます。完全なパケットを受信するまで、ステートマシンの処理は停止します。
- バウンス攻撃：FTP ALG は、番号が 1024 未満のデータ ポートでドア（NAT の場合）やピンホール（ファイアウォールの場合）を作成しません。バウンス攻撃の防止がアクティブになるのは、ファイアウォールが有効にされている場合のみです。

IPv6 ゾーンベース ファイアウォールに対するボックスツーボックス ハイ アベイラビリティ サポートの設定方法

冗長グループ プロトコルの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **protocol** *id*
6. **name** *group-name*
7. **timers hellotime** {*seconds* | **msec** *milliseconds*} **holdtime** {*seconds* | **msec** *milliseconds*}
8. **authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key-string* **timeout** *seconds* | **key-chain** *key-chain-name*}
9. **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。

	コマンドまたはアクション	目的
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`	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	**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 6	**name** *group-name* 例： `Device(config-red-app-prtcl)# name prot1`	（任意）名前を使用して冗長グループ（RG）を設定します。
ステップ 7	**timers hellotime** {*seconds* | **msec** *milliseconds*} **holdtime** {*seconds* | **msec** *milliseconds*} 例： `Device(config-red-app-prtcl)# timers hellotime 3 holdtime 9`	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。
ステップ 8	**authentication** {**text** *string* | **md5 key-string** [**0** | **7**] *key-string* **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 9	**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。

冗長アプリケーション グループの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **redundancy**
4. **application redundancy**
5. **group** *id*
6. **name** *group-name*

7. **shutdown**
8. **priority** *value* [**failover threshold** *value*]
9. **preempt**
10. **track** *object-number* {**decrement** *value* | **shutdown**}
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`	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`	（任意）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	**shutdown** 例： `Device(config-red-app-grp)# shutdown`	（任意）冗長グループを手動でシャットダウンします。
ステップ 8	**priority** *value* [**failover threshold** *value*] 例： `Device(config-red-app-grp)# priority 100 failover threshold 50`	（任意）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 9	**preempt** 例：	グループでのプリエンプションをイネーブルにし、優先度とは無関係にスタンバイデバイスがアクティ

	コマンドまたはアクション	目的
	`Device(config-red-app-grp)# preempt`	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。
ステップ 10	**track** *object-number* {**decrement** *value* | **shutdown**} 例： `Device(config-red-app-grp)# track 200 decrement 200`	冗長グループの優先度を指定します。この値は、イベントが発生した場合に減らされます。
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。

コントロール インターフェイスおよびデータ インターフェイスの設定

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. **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。

	コマンドまたはアクション	目的
ステップ 4	**application redundancy** 例： `Device(config-red)# application redundancy`	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 0/0/0`	冗長グループに使用されるデータ 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 0/0/2 protocol 1`	冗長グループに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。 • この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、冗長グループが待機する時間を指定します。
ステップ 9	**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。

LAN トラフィック インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **encapsulation dot1q** *vlan-id*
6. **ip vrf forwarding** *name*
7. **ipv6 address** {*ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length*}
8. **zone-member security** *zone-name*
9. **redundancy rii** *RII-identifier*

10. **redundancy group** *id* {**ip** *virtual-ip* | **ipv6** {*link-local-address* | *ipv6-address/prefix-length*} | **autoconfig**} [**exclusive**] [**decrement** *value*]
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	**interface** *type number* 例： `Device(config)# interface gigabitethernet 2/0/2`	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	**description** *string* 例： `Device(config-if)# description lan interface`	（任意）インターフェイス設定に説明を追加します。
ステップ 5	**encapsulation dot1q** *vlan-id* 例： `Device(config-if)# encapsulation dot1q 18`	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。
ステップ 6	**ip vrf forwarding** *name* 例： `Device(config-if)# ip vrf forwarding trust`	VPN ルーティングおよび転送（VRF）インスタンスをインターフェイスまたはサブインターフェイスに関連付けます。 • 指定された VRF が設定されていない場合、コマンドは設定されません。
ステップ 7	**ipv6 address** {*ipv6-prefix*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} 例： `Device(config-if)# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/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、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 8	**zone-member security** *zone-name* 例： `Device(config-if)# zone member security z1`	インターフェイスをゾーン メンバーとして設定します。 • *zone-name* 引数の場合、ファイアウォール設定時に **zone security** コマンドを使って設定したゾーンの 1 つを設定する必要があります。

	コマンドまたはアクション	目的
		• インターフェイスがセキュリティ ゾーン内にある場合、そのインターフェイスを通して送受信されるすべてのトラフィックはデフォルトでドロップされます（ただしルータ宛またはルータ発のトラフィックを除く）。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できるようにするには、ポリシー適用対象のゾーン ペアにそのゾーンを含める必要があります。ポリシーの inspect または pass アクションによってトラフィックが許可される場合は、そのインターフェイスを通じてトラフィックが流れます。
ステップ 9	**redundancy rii** *RII-identifier* 例： `Device(config-if)# redundancy rii 100`	冗長グループで保護されたトラフィック インターフェイス用に RII を設定します。
ステップ 10	**redundancy group** *id* {**ip** *virtual-ip* | **ipv6** {*link-local-address* | *ipv6-address/prefix-length*} | **autoconfig**} [**exclusive**] [**decrement** *value*] 例： `Device(config-if)# redundancy group 1 ipv6 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64 exclusive decrement 50`	冗長グループ（RG）トラフィック インターフェイス設定をイネーブルにします。
ステップ 11	**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。

WAN トラフィック インターフェイスの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **description** *string*
5. **ipv6 address** {*ipv6-prefix/prefix-length* | *prefix-name sub-bits/prefix-length*}
6. **zone-member security** *zone-name*
7. **ip tcp adjust-mss** *max-segment-size*
8. **redundancy rii** *RII-identifier*
9. **redundancy asymmetric-routing enable**
10. **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 2/1/0`	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	**description** *string* 例： `Device(config-if)# description wan interface`	（任意）インターフェイス設定に説明を追加します。
ステップ 5	**ipv6 address** {*ipv6-prefix*/*prefix-length* | *prefix-name sub-bits*/*prefix-length*} 例： `Device(config-if)# ipv6 address 2001:DB8:2222::/48`	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、インターフェイスにおける IPv6 処理をイネーブルにします。
ステップ 6	**zone-member security** *zone-name* 例： `Device(config-if)# zone-member security z2`	ファイアウォールを設定する際に、インターフェイスをゾーン メンバーとして設定します。 • *zone-name* 引数の場合、**zone security** コマンドを使用して設定済みのゾーンの 1 つ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 ゾーン内にある場合、そのインターフェイスを通して送受信されるすべてのトラフィックはデフォルトでドロップされます（ただしルータ宛またはルータ発のトラフィックを除く）。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できるようにするには、ポリシー適用対象のゾーン ペアにそのゾーンを含める必要があります。ポリシーの inspect または pass アクションによってトラフィックが許可される場合は、そのインターフェイスを通じてトラフィックが流れます。

	コマンドまたはアクション	目的
ステップ 7	**ip tcp adjust-mss** *max-segment-size* 例： `Device(config-if)# ip tcp adjust-mss 1360`	ルータを通過する TCP SYN パケットの最大セグメント サイズ（MSS）の値を調整します。
ステップ 8	**redundancy rii** *RII-identifier* 例： `Device(config-if)# redundancy rii 360`	冗長グループで保護されたトラフィック インターフェイス用に RII を設定します。
ステップ 9	**redundancy asymmetric-routing enable** 例： `Device(config-if)# redundancy asymmetric-routing enable`	冗長グループを、非対称ルーティングに使用されるインターフェイスに関連付けます。
ステップ 10	**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 ファミリだけがマッチングされるようにクラス 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 ポリシーと IPv6 ポリシーのどちらにもこれを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** セッション
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）。
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`	Virtual Routing and Forwarding（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、その他のパラメータに接続できるようにし、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** セッション 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。

	コマンドまたはアクション	目的
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有効にします。
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/アプリケーション間マッピング（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の検査タイプ 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き、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`	プロトコル固有の検査タイプ 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`	アクションの実行対象となるトラフィック 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。

ゾーンの設定とインターフェイスへのゾーンの適用

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。
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 ポリシーに関連付けます。
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。

	コマンドまたはアクション	目的
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。
ステップ 13	**zone-member security** *zone-name* 例： `Device(config-subif)# zone member security z1`	インターフェイスをゾーン メンバーとして設定します。 • *zone-name* 引数の場合、**zone security** コマンドを使用して設定済みのゾーンの 1 つ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のトラフィックを除く）はデフォルトでドロップされます。トラフィックがゾーン メンバーであるインターフェイスを通過するには、そのゾーンをポリシーの適用先のゾーン ペアの一部にする必要があります。ポリシーの inspect または pass アクションによってトラフィックが許可される場合は、そのインターフェイスを通じてトラフィックが流れます。
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 マップは指定されたゾーン ペアに適用されるので、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。

例

次に示す **show policy-map type inspect zone-pair sessions** コマンドの出力例は、IPv6 アドレスから IPpv4 アドレスへ（またはその逆）のパケット変換を表示します。

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:32847=>(209.165.201.2:21) ftp SIS_OPEN
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [37:84]

        Half-open Sessions
         Session 110D930C [2001:DB8:1::104]:32848=>(209.165.201.2:21) ftp SIS_OPENING
          Created 00:00:00, Last heard 00:00:00
          Bytes sent (initiator:responder) [0:0]
```

次に示す **show policy-map type inspect zone-pair sessions** コマンドの出力例は、IPv6 アドレスから IPpv6 アドレスへのパケット変換を表示します。

```
Device# show policy-map type inspect zone-pair sessions

  Zone-pair: in-to-out
  Service-policy inspect : in-to-out

    Class-map: ipv6-class (match-any)
      Match: protocol ftp
      Match: protocol tcp
      Match: protocol udp
      Inspect
        Established Sessions
         Session 110D930C [2001:DB8:1::103]:63=>[2001:DB8:2::102]:63 udp SIS_OPEN
          Created 00:00:02, Last heard 00:00:01
          Bytes sent (initiator:responder) [162:0]
```

IPv6 ゾーンベース ファイアウォールに対するボックスツーボックス ハイ アベイラビリティ サポートの設定例

例：冗長グループ プロトコルの設定

次に、hello time メッセージと hold time メッセージ用のタイマーが設定されている冗長グループを設定する例を示します。

```
Device# configure terminal
Device(config)# redundancy
Device(config-red)# application redundancy
Device(config-red-app)# protocol 1
Device(config-red-app-prtcl)# timers hellotime 3 holdtime 9
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：冗長アプリケーション グループの設定

次に、優先順位属性とプリエンプション属性のある group1 という名前の冗長グループを設定する例を示します。

```
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 200 decrement 200
Device(config-red-app-grp)# end
```

例：コントロール インターフェイスとデータ インターフェイスの設定

```
Device# configure terminal
Device(config-red)# application redundancy
Device(config-red-app-grp)# group 1
Device(config-red-app-grp)# data GigabitEthernet 0/0/0
Device(config-red-app-grp)# control GigabitEthernet 0/0/2 protocol 1
Device(config-red-app-grp)# timers delay 100 reload 400
Device(config-red-app-grp)# end
```

例：LAN トラフィック インターフェイスの設定

```
Device# configure terminal
Device(config-if)# interface gigabitethernet 2/0/2
Device(config-if)# description lan interface
Device(config-if)# encapsulation dot1q 18
Device(config-if)# ip vrf forwarding trust
Device(config-if)# ipv6 address 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE/64
Device(config-if)# zone member security z1
Device(config-if)# redundancy rii 100
Device(config-if)# redundancy group 1 ipv6 2001:0DB8:1:1:FFFF:FFFF:FFFF:FFFE exclusive
decrement 50
Device(config-if)# end
```

例：WAN トラフィック インターフェイスの設定

次に、WAN-LAN シナリオ用の冗長グループを設定する例を示します。

```
Device# configure terminal
Device(config-if)# interface gigabitethernet 2/1/0
Device(config-if)# description wan interface
Device(config-if)# ipv6 address 2001:DB8:2222::/48
Device(config-if)# zone-member security z2
Device(config-if)# ip tcp adjust-mss 1360
Device(config-if)# redundancy rii 360
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：ゾーンの設定とインターフェイスへのゾーンの適用

```
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 ファイアウォールに対するボックスツーボックス ハイ アベイラビリティ 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』
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
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

IPv6 ゾーンベース ファイアウォールのボックスツーボックス 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ボックスツーボックス 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ボックスツーボックス 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ボックスツーボックス ハイ アベイラビリティ サポート機能では、IPv6 ファイアウォールの冗長グループ（RG）に基づいてハイ アベイラビリティ（HA）がサポートされています。この機能により、相互にバックアップとして動作するデバイスのペアを設定できます。この機能を設定し、複数のフェールオーバー条件に基づいてアクティブ デバイスを判断できます。 追加または変更されたコマンドはありません。
IPv6 ゾーン ベースのファイアウォールのボックスツーボックス ハイ アベイラビリティ サポート	Cisco IOS XE Release 3.8S	Cisco IOS XE リリース 3.10S では、Cisco ISR 4400 シリーズ ルータのサポートが追加されました。

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。