VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポート

この機能は、IPv6 ファイアウォールを介した VRF-Aware サービス インフラストラクチャ（VASI）のインターフェイスをサポートします。 この機能を使用すると、アクセス コントロール リスト（ACL）、ネットワーク アドレス変換（NAT）、ポリシング、ゾーンベース ファイアウォールなどのサービスを、2 つの異なる仮想ルーティングおよび転送（VRF）インスタンスを通過するトラフィックに適用できます。 VASI インターフェイスは、ルート プロセッサ（RP）と転送プロセッサ（FP）の冗長性をサポートします。 VASI インターフェイスは、IPv4 および IPv6 ユニキャスト トラフィックをサポートします。

このモジュールでは、VASI インターフェイスに関する情報を提供し、VASI インターフェイスを設定する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。

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートの制約事項

- VRF-Aware Software インフラストラクチャ（VASI）インターフェイス上のマルチプロトコル ラベル スイッチング（MPLS）トラフィックはサポートされません。
- IPv4 および IPv6 マルチキャスト トラフィックはサポートされません。
- VASI インターフェイスは、キュー ベースの機能の付加をサポートしません。 次のコマンドは、VASI インターフェイスに接続されたモジュラ QoS CLI（MQC）ポリシーではサポートされません。
  - **bandwidth**（**policy-map クラス**）
  - **fair-queue**
  - **priority**
  - **queue-limit**
  - **random-detect**
  - **shape**

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートについて

VASI の概要

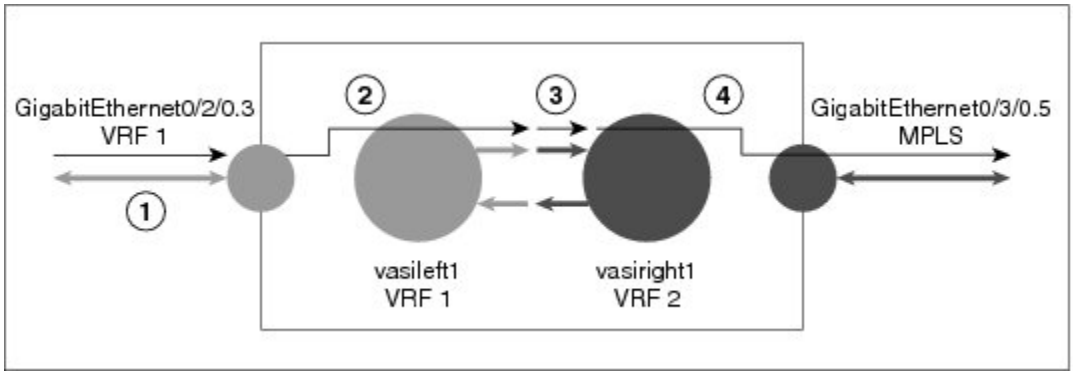
VRF-Aware Software インフラストラクチャ（VASI）を使用すると、ファイアウォール、IPsec、ネットワーク アドレス変換（NAT）などのサービスを、異なる仮想ルーティングおよび転送（VRF）インスタンスを通過するトラフィックに適用できます。 VASI は、仮想インターフェイスのペアを使用して実装され、ペアの各インターフェイスは異なる VRF インスタンスに関連付けられます。 VASI 仮想インターフェイスは、これら 2 つの VRF インスタンス間で交換される必要があるパケットのネクスト ホップ インターフェイスです。 VASI インターフェイスは、VRF インスタンス間のファイアウォールまたは NAT を設定するためのフレームワークを提供します。

各インターフェイス ペアは、異なる 2 つの VRF インスタンスに関連付けられています。 ペアリングの関連付けは、vasileft x が自動的に vasiright x へのペアを取得するという方法で、2 つのインターフェイスのインデックスに基づいて自動的に行われます。 たとえば、vasileft1 および vasiright1 は自動的にペアとなり、vasileft1 に入るパケットは、vasiright1 に内部的に渡されます。

VASI インターフェイス上で内部ボーダー ゲートウェイ プロトコル（iBGP）、Enhanced Interior Gateway Routing Protocol（EIGRP）、または Open Shortest Path First（OSPF）によるスタティック ルーティングまたはダイナミック ルーティングを設定できます。 iBGP ダイナミック ルーティング プロトコルの制約事項とコンフィギュレーションは、VASI インターフェイス間の iBGP ルーティング コンフィギュレーションに有効です。

次の図は、同じデバイス上の Inter-VRF VASI 設定を示します。

図 *1*：*Inter-VRF VASI* の設定



Inter-VRF VASI が同じデバイス上で設定されている場合、パケット フローは次の順序で発生します。

1 パケットは、VRF1（ギガビット イーサネット 0/2/0.3）に属する物理インターフェイスに入ります。

2 パケットを転送する前に、VRF1ルーティングテーブルでのフォワーディングルックアップが実行されます。 Vasileft1 は、ネクスト ホップとして選択され、存続可能時間（TTL）値がパケットから減らされます。 通常、転送アドレスは、VRF のデフォルト ルートに基づいて選択されます。 ただし、転送アドレスがスタティック ルートまたは学習されたルートになる場合もあります。 パケットは vasileft1 の出力パスに送信され、次に vasiright1 入力パスに自動的に送信されます。

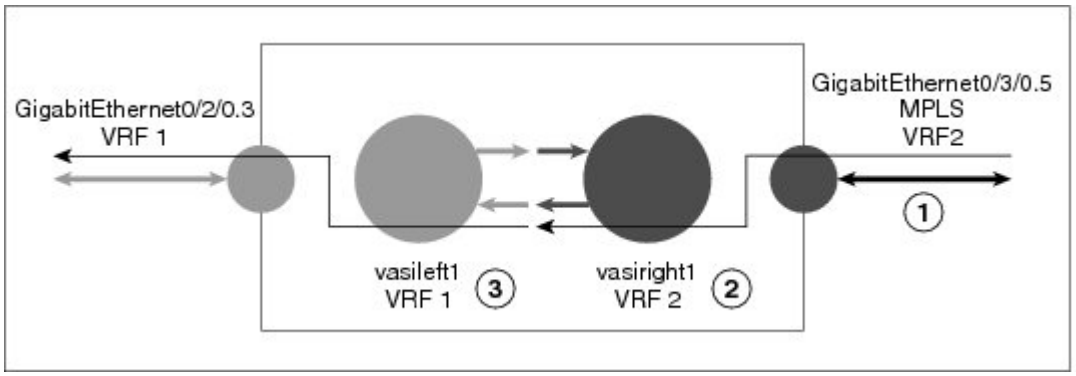
3 パケットが vasiright1 に入ると、フォワーディング ルックアップが VRF2 ルーティング テーブルで行われ、TTL が再び減らされます（このパケットでは 2 回目）。

4 VRF2は、パケットを物理インターフェイス、ギガビットイーサネット0/3/0.5に転送します。

次の図は、VASI がマルチ プロトコル ラベル スイッチング（MPLS）VPN 設定で動作する仕組みを示しています。

（注） 次の図で、MPLS はギガビット イーサネット インターフェイスでイネーブルですが、MPLS トラフィックは、VASI ペア間ではサポートされていません。

図 *2*：*MPLS VPN* 設定での *VASI*



VASI がマルチ プロトコル ラベル スイッチング（MPLS）VPN に設定されている場合、パケットフローは次の順序で発生します。

1 パケットは、VPN ラベルが付けられて MPLS インターフェイスに到着します。

2 VPN ラベルはパケットから取り除かれ、フォワーディング ルックアップが VRF2 内で実行され、パケットは vasiright1 に転送されます。 TTL 値はパケットから減らされます。

3 パケットが入力パスの vasileft1 に入ると、別のフォワーディング ルックアップが VRF1 で行われます。 パケットは、VRF1（ギガビット イーサネット 0/2/0.3）の出力物理インターフェイスに送信されます。 TTL 値はパケットから再び減らされます。

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートの設定方法

VRF およびアドレス ファミリ セッションの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **vrf definition** *vrf-name*
4. **address-family ipv6**
5. **exit-address-family**
6. **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	**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`	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。

	コマンドまたはアクション	目的
ステップ 5	**exit-address-family** 例： `Device(config-vrf-af)# exit-address-family`	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	**end** 例： `Device(config-vrf)# end`	VRF 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。

VASI サポートのクラス マップとポリシー マップの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **ipv6 unicast-routing**
4. **class-map type inspect match-any** *class-map-name*
5. **match protocol** *name*
6. **match protocol** *name*
7. **exit**
8. **policy-map type inspect** *policy-map-name*
9. **class type inspect** *class-map-name*
10. **inspect**
11. **exit**
12. **class class-default**
13. **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	**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。
ステップ 4	**class-map type inspect match-any** *class-map-name* 例： `Device(config)# class-map type inspect match-any c-map`	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 5	**match protocol** *name* 例： `Device(config-cmap)# match protocol icmp`	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 6	**match 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 7	**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。
ステップ 8	**policy-map type inspect** *policy-map-name* 例： `Device(config)# policy-map type inspect p-map`	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 9	**class type inspect** *class-map-name* 例： `Device(config-pmap)# class type inspect c-map`	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 10	**inspect** 例： `Device(config-pmap-c)# inspect`	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。

	コマンドまたはアクション	目的
ステップ 11	**exit** 例： `Device(config-pmap-c)# exit`	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、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 12	**class class-default** 例： `Device(config-pmap)# class class-default`	ポリシーマップ設定を定義済みのデフォルト クラスに適用して、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。 • 設定済みクラス マップの一致基準のいずれともトラフィックが一致しない場合、事前に定義されたデフォルト クラスに誘導されます。
ステップ 13	**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。

VASI のサポート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-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone*
6. **service-policy type inspect** *policy-map-name*
7. **exit**
8. **interface** *type number*
9. **vrf forwarding** *vrf-name*
10. **no ip address**
11. **zone member security** *zone-name*
12. **ipv6 address** *ipv6-address*/*prefix-length*
13. **ipv6 enable**
14. **negotiation auto**
15. **exit**
16. **interface** *type number*
17. **no ip address**
18. **ipv6 address** *ipv6-address*/*prefix-length*
19. **ipv6 enable**
20. **negotiation auto**
21. **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。

	コマンドまたはアクション	目的
ステップ 3	**zone security** *zone-name* 例： `Device(config)# zone security in`	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。 • 設定には、ゾーンペアを作成するために、2つのセキュリティゾーン（送信元ゾーンと宛先ゾーン）が含まれている必要があります。 • ゾーンペアでは、送信元ゾーンまたは宛先ゾーンとしてデフォルト ゾーンを使用できます。
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-pair security** *zone-pair-name* **source** *source-zone* **destination** *destination-zone* 例： `Device(config)# zone-pair security in-out source in destination out`	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。 • ポリシーを適用するには、ゾーンペアを設定する必要があります。
ステップ 6	**service-policy type inspect** *policy-map-name* 例： `Device(config-sec-zone-pair)# service-policy type inspect p-map`	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。 • ゾーンのペア間でポリシーが設定されない場合、トラフィックはデフォルトでドロップされます。
ステップ 7	**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 8	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/0`	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 9	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding VRF1`	インターフェイスまたはサブインターフェイスに仮想ルーティングおよび転送（VRF）インスタンスまたは仮想ネットワークを関連付けます。

	コマンドまたはアクション	目的
ステップ 10	**no ip address** 例： `Device(config-if)# no ip address`	IP アドレスを削除するか、IP 処理をディセーブルにします。
ステップ 11	**zone member security** *zone-name* 例： `Device(config-if)# zone member security in`	インターフェイスをセキュリティ ゾーンにアタッチします。
ステップ 12	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:2:1234/64`	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 13	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていない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 14	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビットイーサネットインターフェイス上で速度、デュプレックス モード、およびフロー制御のアドバタイズをイネーブルにします。
ステップ 15	**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 16	**interface** *type number* 例： `Device(config)# interface gigabitethernet 0/0/1`	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 17	**no ip address** 例： `Device(config-if)# no ip address`	IP アドレスを削除するか、IP 処理をディセーブルにします。
ステップ 18	**ipv6 address** *ipv6-address/prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:3:1234/64`	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。

	コマンドまたはアクション	目的
ステップ 19	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていない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 20	**negotiation auto** 例： `Device(config-if)# negotiation auto`	ギガビットイーサネットインターフェイス上で速度、デュプレックス モード、およびフロー制御のアドバタイズをイネーブルにします。
ステップ 21	**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。

VASI 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. **vrf forwarding** *vrf-name*
5. **ipv6 address** *ipv6-address*/*prefix-length* **link-local**
6. **ipv6 address** *ipv6-address*/*prefix-length*
7. **ipv6 enable**
8. **no keepalive**
9. **zone member security** *zone-name*
10. **exit**
11. **interface** *type number*
12. **ipv6 address** *ipv6-address*/*prefix-length* **link-local**
13. **ipv6 address** *ipv6-address*/*prefix-length*
14. **ipv6 enable**
15. **no keepalive**
16. **exit**
17. **ipv6 route** *ipv6-prefix*/*prefix-length interface-type interface-number ipv6-address*
18. **ipv6 route vrf** *vrf-name ipv6-prefix*/*prefix-length interface-type interface-number ipv6-address*
19. **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 vasileft 1`	VASI 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	**vrf forwarding** *vrf-name* 例： `Device(config-if)# vrf forwarding VRF1`	インターフェイスまたはサブインターフェイスに仮想ルーティングおよび転送（VRF）インスタンスまたは仮想ネットワークを関連付けます。
ステップ 5	**ipv6 address** *ipv6-address*/*prefix-length* **link-local** 例： `Device(config-if)# ipv6 address FE80::8EB6:4FFF:FE6C:E701 link-local`	インターフェイスの IPv6 リンクローカルアドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ステップ 6	**ipv6 address** *ipv6-address*/*prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:4:1234/64`	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 7	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていない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	**no keepalive** 例： `Device(config-if)# no keepalive`	キープアライブ パケットをディセーブルにします。
ステップ 9	**zone member security** *zone-name* 例： `Device(config-if)# zone member security out`	インターフェイスをセキュリティ ゾーンにアタッチします。

	コマンドまたはアクション	目的
ステップ 10	**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 11	**interface** *type number* 例： `Device(config)# interface vasiright 1`	VASI 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 12	**ipv6 address** *ipv6-address*/*prefix-length* **link-local** 例： `Device(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local`	インターフェイスの IPv6 リンクローカル アドレスを設定し、そのインターフェイスでの IPv6 処理をイネーブルにします。
ステップ 13	**ipv6 address** *ipv6-address*/*prefix-length* 例： `Device(config-if)# ipv6 address 2001:DB8:4:1234/64`	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 14	**ipv6 enable** 例： `Device(config-if)# ipv6 enable`	明示的な IPv6 アドレスが設定されていない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 15	**no keepalive** 例： `Device(config-if)# no keepalive`	キープアライブ パケットをディセーブルにします。
ステップ 16	**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 17	**ipv6 route** *ipv6-prefix*/*prefix-length* *interface-type interface-number ipv6-address* 例： `Device(config)# ipv6 route 2001::/64 vasileft 1 2001::/64`	スタティック IPv6 ルートを確立します。
ステップ 18	**ipv6 route vrf** *vrf-name* *ipv6-prefix*/*prefix-length interface-type interface-number ipv6-address*	IPv6 アドレスのすべての VRF テーブルまたは特定の VRF テーブルを指定します。

	コマンドまたはアクション	目的
	例： `Device(config)# ipv6 route vrf vrf1 2001::/64 vasiright 1 2001::/64`	
ステップ 19	**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。

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポートの設定例

例：VRF およびアドレス ファミリ セッションの設定

```
Device# configure terminal
Device(config)# vrf definition VRF1
Device(config-vrf)# address-family ipv6
Device(config-vrf-af)# exit-address-family
Device(config-vrf)# end
```

例：VASI サポートのクラス マップとポリシー マップの設定

```
Device# configure terminal
Device(config)# ipv6-unicast routing
Device(config)# class-map type inspect match-any c-map
Device(config-cmap)# match protocol icmp
Device(config-cmap)# match protocol tcp
Device(config-cmap)# match protocol udp
Device(config-cmap)# exit
Device(config)# policy-map type inspect p-map
Device(config-pmap)# class type inspect c-map
Device(config-pmap-c)# inspect
Device(config-pmap-c)# exit
Device(config-pmap)# class class-default
Device(config-pmap-c)# end
```

例：VASI のサポートのゾーンおよびゾーン ペアの設定

```
Device# configure terminal
Device(config)# zone security in
Device(config)# exit
Device(config)# zone security out
Device(config)# exit
Device(config)# zone-pair security in-out source in destination out
```

```
Device(config-sec-zone-pair)# service-policy type inspect p-map
Device(config-sec-zone-pair)# exit
Device(config)# interface gigabitethernet 0/0/0
Device(config-if)# vrf forwarding VRF1
Device(config-if)# no ip address
Device(config-if)# zone member security in
Device(config-if)# ipv6 address 2001:DB8:2:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# negotiation auto
Device(config-if)# exit
Device(config)# interface gigabitethernet 0/0/1
Device(config-if)# no ip address
Device(config-if)# ipv6 address 2001:DB8:3:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# negotiation auto
Device(config-if)# end
```

例：VASI インターフェイスの設定

```
Device# configure terminal
Device(config)# interface vasileft 1
Device(config-if)# vrf forwarding VRF1
Device(config-if)# ipv6 address FE80::8EB6:4FFF:FE6C:E701 link-local
Device(config-if)# ipv6 address 2001:DB8:4:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# no keepalive
Device(config-if)# zone-member security out
Device(config-if)# exit
Device(config)# interface vasiright 1
Device(config-if)# ipv6 address FE80::260:3EFF:FE11:6770 link-local
Device(config-if)# ipv6 address 2001:DB8:4:1234/64
Device(config-if)# ipv6 enable
Device(config-if)# no keepalive
Device(config-if)# exit
Device(config)# ipv6 route 2001::/64 vasileft 1 2001::/64
Device(config)# ipv6 route vrf vrf1 2001::/64 vasiright 1 2001::/64
Device(config)# end
```

ファイアウォールステートフルシャーシ間冗長性の追加情報

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『Master Command List, All Releases』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『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

VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール 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*：*VASI* インターフェイス経由の *IPv6* ゾーンベース ファイアウォール サポートの機能情報

機能名	リリース	機能情報
VASI インターフェイス経由の IPv6 ゾーンベース ファイアウォール サポート	Cisco IOS XE Release 3.7S	この機能は、IPv6 ファイアウォール経由の VASI インターフェイスをサポートします。 この機能を使用すると、アクセス コントロール リスト（ACL）、ネットワーク アドレス変換（NAT）、ポリシング、ゾーンベース ファイアウォールなどのサービスを、2 つの異なる仮想ルーティングおよび転送（VRF）インスタンスを通過するトラフィックに適用できます。 VASI インターフェイスは、ルートプロセッサ（RP）と転送プロセッサ（FP）の冗長性をサポートします。 VASI インターフェイスは、IPv4 および IPv6 ユニキャスト トラフィックをサポートします。 この機能について導入または変更されたコマンドはありません。