



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 ファイアウォールでの VRF 対応サービス インフラストラクチャ (VASI) インターフェイスをサポートします。この機能により、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 Virtual Routing and Forwarding (VRF) インスタンスの間を流れ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) とフォワーディングプロセッサ (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 インターフェイスの概要を紹介し、VASI インターフェイスを設定する方法を説明します。

- [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 サポートに関する制約事項 \(1 ページ\)](#)
- [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 サポートに関する情報 \(2 ページ\)](#)
- [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 \(4 ページ\)](#)
- [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 \(12 ページ\)](#)
- [ファイアウォール ステートフル シャーシ間冗長性に関する追加情報 \(14 ページ\)](#)
- [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 サポートに関する機能情報 \(14 ページ\)](#)

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 サポートに関する制約事項

- VRF 対応ソフトウェア インフラストラクチャ (VASI) インターフェイス経由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 と IPv6 のマルチキャスト 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 ベース機能のアタッチメントをサポートしません。以下のコマンドは、VASI インターフェイスにアタッチされたモジュラ QoS CLI (MQC) ポリシーでサポートされません。
 - **bandwidth (policy-map class)**
 - **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 サポートに関する情報

VASI の概要

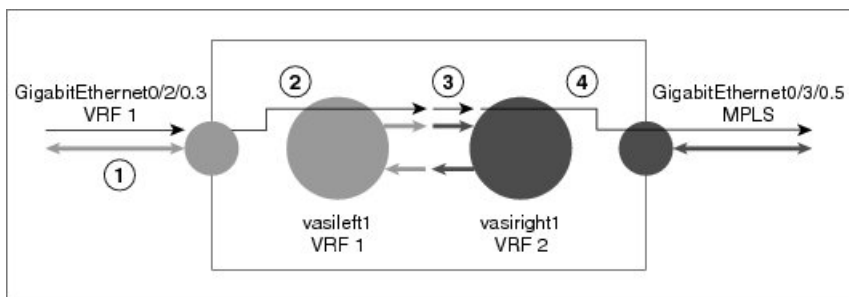
VRF 対応ソフトウェア インフラストラクチャ (VASI) を使用すると、ファイアウォール、GETVPN、IPsec、およびネットワークアドレス変換 (NAT) などのサービスを、異なる仮想ルーティングおよび転送 (VRF) インスタンスを横断するトラフィックに適用できます。VASI は仮想インターフェイスのペアを使用して実行され、ペア内の各インターフェイスは別の VRF インスタンスに関連付けられます。VASI 仮想インターフェイスは、これら 2 つの VRF インスタンス間で切り替える必要がある、すべてのパケットのネクストホップ インターフェイスです。VASI インターフェイスは、VRF インスタンス間に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。ペアリングは、vasileft インターフェイスが自動的に vasiright インターフェイスへのペアとなるように、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、下の図では、vasileft1 と vasiright1 は自動的にペアになり、vasileft1 に入るパケットは vasiright1 に内部的に渡されます。

VASI インターフェイスでは、内部ボーダー ゲートウェイ プロトコル (IBGP)、Enhanced Interior Gateway Routing Protocol (EIGRP)、および Open Shortest Path First (OSPF) を使用して、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のいずれかを設定できます。

次の図は、同じデバイスの VRF 間 VASI 設定を示しています。

図 1: VRF 間 VASI 設定



VRF 間 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。

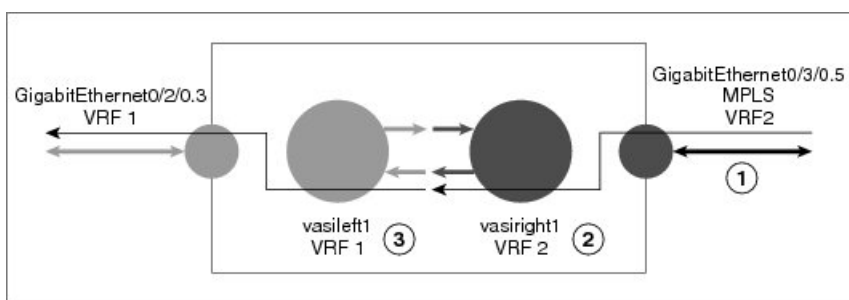
1. パケットが VRF 1 (ギガビットイーサネット 0/2/0.3) に属する物理インターフェイスに入ります。
2. パケットを転送する前に、VRF1 ルーティングテーブルでフォワーディングルックアップが実行されます。Vasileft1 がネクスト ホップとして選択され、存続可能時間 (TTL) 値がパケットから引かれます。通常、フォワーディング アドレスは VRF のデフォルト ルートに基づいて選択されます。ただし、フォワーディング アドレスはスタティック ルートまたは学習したルートになる可能性もあります。パケットは vasileft1 の出力パスに送信されてから、vasiright1 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、VRF 2 ルーティング テーブルでフォワーディング ルックアップが実行され、TTL が再度減らされます (このパケットでは 2 回目)。
4. VRF 2 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 へ転送します。

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 設定で機能するしくみを示します。



- (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有効になっていますが、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 設定を使用する VASI



VASI がマルチプロトコル ラベル スイッチング (MPLS) VPN を使用して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. パケットが VPN ラベルを持つ MPLS インターフェイスに到着します。
2. VPN ラベルがパケットから取り除かれ、VRF2 でフォワーディングルックアップが実行され、パケットが vasiright1 に転送されます。TTL 値がパケットから引かれます。
3. パケットが入力パスの vasileft1 に入り、別のフォワーディングルックアップが VRF1 で行われます。パケットが VRF1 の出力物理インターフェイス (ギガビットイーサネット 0/2/0.3) に送信されます。TTL がパケットから再度減らされます。

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 とアドレス 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	vrf definition <i>vrf-name</i> 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。

	コマンドまたはアクション	目的
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、標準の 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	アドレス ファミリ コンフィギュレーション モードを終了して、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て、特権 EXEC モードを開始します。

VASI サポート用のクラス 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	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 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いて、クラス マップ 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いて、クラス マップ 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	プロトコル固有の検査タイプ ポリシー マップを作成して、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 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。
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	定義済みのデフォルト クラスにポリシー マップ設定を適用して、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。

	コマンドまたはアクション	目的
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 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 モードを有効にします。 <ul style="list-style-type: none"> • 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。 <ul style="list-style-type: none"> ゾーンペアを作成するには2つのセキュリティ ゾーン（送信元ゾーンと宛先ゾーン）が設定に含まれる必要があります。 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。 <ul style="list-style-type: none"> 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 ポリシーに関連付けます。 <ul style="list-style-type: none"> 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 Virtual Routing and Forwarding (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 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。

	コマンドまたはアクション	目的
ステップ 11	zone member security <i>zone-name</i> 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 <i>ipv6-address/prefix-length</i> 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 <i>ipv6-address/prefix-length</i> 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。
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。

	コマンドまたはアクション	目的
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 モードを有効にします。 <ul style="list-style-type: none"> • 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 :	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。

	コマンドまたはアクション	目的
	Device(config)# interface vasileft 1	
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 Virtual Routing and Forwarding (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。
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。

	コマンドまたはアクション	目的
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 例 : Device(config)# ipv6 route vrf vrf1 2001::/64 vasiright 1 2001::/64	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。
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 とアドレス 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 サポート用のクラス 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 サポート用のゾーンとゾーン 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	『 Master Command List, All Releases 』
セキュリティ コマンド	<ul style="list-style-type: none"> 『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
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

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 サポートに関する機能情報

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 サポートに関する機能情報

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 リリース 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。この機能により、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 Virtual Routing and Forwarding (VRF) インスタンスの間を流れ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) とフォワーディングプロセッサ (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。

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。