VRF 対応 Cisco IOS XE ファイアウォール

サービス プロバイダー（SP）または大企業のエッジ ルータで VRF 対応 Cisco IOS XE ファイアウォールが設定されている場合は、Cisco IOS XE ファイアウォール機能が VPN ルーティングおよび転送（VRF）インターフェイスに適用されます。SP は中小企業市場にマネージドサービスを提供しています。

VRF 対応 Cisco IOS XE ファイアウォールは、さまざまなプロトコルの VRF-Lite（別名 Multi-VRF CE）と Application Inspection and Control（AIC）をサポートします。

VRF 対応ファイアウォールは、さまざまなプロトコルの VRF-Lite（別名 Multi-VRF CE）と Application Inspection and Control（AIC）をサポートします。

（注） Cisco IOS XE リリースは、コンテキストベースのアクセス コントロール（CBAC）ファイアウォールをサポートしません。

VRF 対応 Cisco IOS XE ファイアウォールの前提条件

- Cisco IOS XE ファイアウォールについて理解します。
- VRF を設定します。

VRF 対応 Cisco IOS XE ファイアウォールに関する制約事項

- 2 つの VPN ネットワークに重複するアドレスがある場合、VRF 対応ファイアウォールをサポートするには、VRF 対応ネットワーク アドレス変換（NAT）が必要です。NAT は VRF 間ルーティングはサポートしません。VRF 間ルーティング機能向けの VRF 対応ソフトウェア インフラストラクチャ（VASI）を使用できます。
- 複数の VPN に属するクリプトトンネルが単一のインターフェイスで終端する場合、VRF ごとのファイアウォールポリシーを適用できません。
- VASI インターフェイスのサイト間クリプトマップは、次のプラットフォームではサポートされていません。
  - Cisco 1000 シリーズ サービス統合型ルータ
  - Cisco 4000 シリーズ サービス統合型ルータ
  - Cisco 1000v クラウドサービスルータ
- 同じゾーンは、異なる複数の VRF に設定されたインターフェイスに適用できません。

VRF 対応 Cisco IOS XE ファイアウォールについて

VRF 対応 Cisco IOS XE ファイアウォール

VRF 対応ファイアウォールは、VRF 内で送受信される IP パケットを検査します。VRF では、ルーティングテーブルの複数のインスタンスを単一のルータ内で共存させることができます。これにより、VPN の分離が可能になり、IP アドレス空間の独立した重複が実現されます。VRF では、あるサービス プロバイダーの顧客からのトラフィックを他のサービス プロバイダーの顧客から分離することができます。Cisco IOS XE VRF サポートは、インターフェイス、ルーティングテーブル、および転送テーブルの個別のセットで構成されるそれぞれのルーティング ドメインを使って、ルータを複数のルーティング ドメインに分割します。各ルーティング ドメインは、テーブル ID と呼ばれる固有識別子によって参照されます。グローバル ルーティング ドメインとデフォルト ルーティング ドメイン（どの VRF にも関連付けられていない）は 0 のテーブル ID で解決されます。VRF は重複する IP アドレス空間をサポートするため、相互に重なりのない VRF からのトラフィックに同じ IP アドレスを割り当てることができます。

VRF 対応 Cisco IOS XE ファイアウォールは次のようなメリットを提供します。

- スケーラブルな展開：あらゆるネットワークの帯域幅とパフォーマンスの要件を満たすようにスケールします。
- VPN サポート：Cisco IOS XE IPSec とその他のソフトウェアベースのテクノロジー（Layer 2 Tunneling Protocol（L2TP）トンネリングや Quality of Service（QoS）など）に基づく、すべてが揃った VPN ソリューションを提供します。

- AIC サポート：Internet Message Access Protocol（IMAP）、Post Office Protocol 3（POP3）、Simple Mail Transfer Protocol（SMTP）、および Sun リモート プロシージャ コール（SUN RPC）用のポリシー マップを提供します。
- ユーザは VRF 単位でファイアウォールを設定できます。ファイアウォールは、VRF 内で送受信した IP パケットを検査します。また、2 つの異なる VRF（相互に重なりのある VRF）間のトラフィックも検査します。
- SP は、プロバイダー エッジ（PE）ルータにファイアウォールを展開できます。
- 重複する IP アドレス空間をサポートするため、相互に重なりのない VRF のトラフィックが同じ IP アドレスを持つことができます。
- VRF（グローバルではない）ファイアウォール コマンドパラメータとサービス妨害（DoS）パラメータをサポートするため、VRF 対応ファイアウォールは、さまざまな VPN 顧客に割り当てられた複数のインスタンス（VRF インスタンスを含む）として実行できます。
- VRF ID を含む高速ロギング（HSL）メッセージを生成します。ただし、これらのメッセージは 1 つのコレクタによって収集されます。

VRF 対応ファイアウォールを使用すれば、ファイアウォール セッションの数を制限することができます。ファイアウォール セッションが制限されていない場合は、複数の VRF でルータ リソースを共有することが困難になります。これは、1 つの VRF がリソースのほとんどを消費して、他の VRF のリソースが足りなくなることで、他の VRF でサービス妨害（DoS）が発生する可能性があるためです。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、ファイアウォールが最大 4000 の VRF をサポートします。

アドレス空間の重複

VRF はデバイスを複数のルーティング ドメインに分割します。これらの各ルーティング ドメインには、インターフェイスおよびルーティング テーブルの固有のセットが含まれています。ルーティング テーブルは、VRF ごとの一意のテーブル ID を使用して参照されます。ゼロは、VPN ルーティングおよび転送（VRF）に関連付けられていないデフォルトのグローバル ルーティング テーブル ID です。

交差しない VRF では、重複するアドレス空間を使用できます（つまり、ある VRF の IP アドレスが他の VRF に含まれることがあります）。

VRF

VPN ルーティングおよび転送（VRF）により、ルーティング テーブルの複数のインスタンスが同じデバイス内に共存できます。VRF はプロバイダー エッジ（PE）デバイス内に VRF テーブルのテンプレートを含みます。

通常、アドレスの重複は、カスタマー ネットワークでプライベート IP アドレスを使用していることから発生します。アドレスの重複は、ピアツーピア（P2P）VPN の実装を展開するうえで主要な障害物の 1 つです。重複アドレスの問題を解消するために、マルチプロトコル ラベル スイッチング（MPLS）VPN テクノロジーを使用できます。

各 VPN は、デバイスに独自のルーティングおよびフォワーディング テーブルがあるため、VPN に属するすべてのカスタマーまたはサイトには、そのテーブルに含まれるルートセットに対してのみアクセス権があります。そのため、MPLS VPN ネットワークの PE デバイスには、多数の VPN 別のルーティング テーブルと、サービス プロバイダー（SP）ネットワーク内の他のデバイスに到達するために使用される 1 つのグローバル ルーティング テーブルが含まれます。事実上、数多くの仮想デバイスが単一の物理デバイスに作成されます。

VRF-Lite

MPLS 対応ファイアウォールを使用しない VRF とも呼ばれる VRF-Lite 対応ファイアウォール機能は、ファイアウォール ゾーンを非 MPLS 対応 VPN ルーティングおよび転送（VRF）インターフェイスに適用できるようにします。

VRF-Lite 対応ファイアウォール機能を使用すれば、サービス プロバイダー（SP）は複数の VPN をサポートし、それらの VPN の間で IP アドレスを重複させることが可能です。VRF-lite は、入力インターフェイスを使用して異なる VPN のルートを区別し、1 つまたは複数のレイヤ 3 インターフェイスを各 VRF に関連付けることで仮想パケット転送テーブルを編成します。VRF には、イーサネット ポートなどの物理インターフェイス、または VLAN スイッチ仮想インターフェイス（SVI）などの論理インターフェイスを使用できます。ただし、1 つのレイヤ 3 インターフェイスは同時に複数の VRF に所属できません。

（注） すべての VRF-Lite インターフェイスをレイヤ 3 インターフェイスにする必要があります。

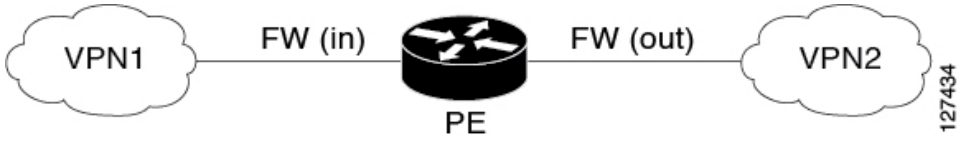
VRF-Lite には、次のデバイスが含まれます。

- カスタマー エッジ（CE）デバイスは、データ リンクによる SP ネットワークへのアクセスを顧客に提供します。CE デバイスは、サイトのローカル ルートをプロバイダー エッジ（PE）デバイスにアドバタイズして、PE デバイスからリモート VPN ルートに関する情報を入手します。
- PE デバイスは、スタティック ルーティングまたはルーティング プロトコル（Border Gateway Protocol（BGP）、Routing Information Protocol バージョン 1（RIPv1）、RIPv2 など）を使用して、CE デバイスとルーティング情報を交換します。
- PE デバイス（またはコア デバイス）は、CE デバイスに接続されていない SP ネットワーク内の任意のデバイスです。
- PE デバイスは、直接接続された VPN に関する VPN ルートのみを維持する必要があるだけで、すべての SP VPN ルートを維持する必要はありません。各 PE デバイスは、直接接続しているサイトごとに VRF を維持します。すべてのサイトが同じ VPN に属している場合は、PE デバイス上の複数のインターフェイスを 1 つの VRF に関連付けることができま

す。各 VPN は、指定された VRF にマッピングされます。CE デバイスからローカル VPN ルートを学習した後、PE デバイスは、内部 BGP（iBGP）を使用して他の PE デバイスと VPN ルーティング情報を交換します。

VRF-Lite を使用すると、複数の顧客が 1 つの CE デバイスを共有できます。その場合は、CE デバイスと PE デバイス間で 1 つの物理リンクのみが使用されます。共有 CE デバイスは、顧客ごとに別々の VRF テーブルを維持し、独自のルーティング テーブルに基づいて、顧客ごとにパケットをスイッチングまたはルーティングします。VRF-Lite は限定された PE デバイスの機能を CE デバイスに拡張して、個別の VRF テーブルを維持する機能を提供し、VPN のプライバシーとセキュリティをブランチ オフィスまで拡張します。

図 *1 : VRF* 間シナリオでのファイアウォール



MPLS VPN

マルチプロトコル ラベル スイッチング（MPLS）VPN 機能を使用すると、サービス プロバイダー（SP）のネットワーク全体で複数のサイトを透過的に相互接続できます。1 つの SP ネットワークで、複数の IP VPN をサポートできます。VPN ユーザから見ると、各 VPN はその他すべてのネットワークとは隔離されたプライベート ネットワークです。1 つの VPN 内では、各拠点は同一 VPN 内のいずれの拠点にも IP パケットを送信できます。

各 VPN は、1 つ以上の VPN ルーティングおよび転送（VRF）インスタンスに関連付けられています。VRF は、1 つの IP ルーティング テーブル、派生した 1 つの Cisco Express Forwarding（CEF）テーブル、およびそのフォワーディング テーブルを使用する一連のインターフェイスで構成されます。

デバイスは、各 VRF に対し別々のルーティングおよび Cisco Express Forwarding テーブルを保持します。これにより、情報が VPN 外に送信されることが回避でき、重複 IP アドレスの問題を起こすことなく同一のサブネットが複数の VPN で使用可能になります。

マルチプロトコル BGP（MP-BGP）を使用しているデバイスは、MP-BGP 拡張コミュニティを使用して VPN のルーティング情報を配布します。

VRF 対応 NAT

ネットワーク アドレス変換（NAT）を使用すると、なんらかの単一のデバイスが、インターネット（またはパブリック ネットワーク）とローカル（またはプライベート）ネットワーク間でエージェントとして機能できます。NAT システムは多様なレベルのセキュリティ機能を提供できますが、主な目的は、アドレス空間を節約することです。

組織が NAT を使用すると、既存のネットワークを持っていてインターネットにアクセスする必要がある場合に、IP アドレスが枯渇する問題を解決できます。ネットワーク インフォメーション センター（NIC）登録 IP アドレスを所有していないサイトは、取得する必要がありま

す。NAT は、何千もの非公開の内部アドレスを取得しやすいアドレスの範囲に動的にマップすることで、NIC 登録 IP アドレスの懸案事項を排除します。

NAT システムは、攻撃者が以下の情報を特定するのを困難にします。

- ネットワーク上で動作しているシステムの数。
- ネットワーク上で動作しているマシンとオペレーティング システムのタイプ。
- ネットワーク トポロジと配置。

NAT とマルチプロトコル ラベル スイッチング（MPLS）VPN の統合により、単一のデバイス上で複数の MPLS VPN を連動するように設定することができます。すべての MPLS VPN で同じ IP アドレス方式が使用されている場合でも、NAT で IP トラフィックを受信する MPLS VPN を区別できます。そのため、複数の MPLS VPN ユーザでサービスを共有しながら、各 MPLS VPN を相互に隔離できます。

インターネット接続、ドメイン ネーム サーバ（DNS）、VoIP サービスなどの付加価値サービスを顧客に提供するには、MPLS サービス プロバイダーが NAT を使用する必要があります。NAT は、MPLS VPN 顧客がネットワーク上で重複した IP アドレスを使用できるようにします。

また、NAT は、カスタマーエッジ（CE）デバイスまたはプロバイダーエッジ（PE）デバイスに実装できます。NAT と MPLS VPN の統合機能により、MPLS クラウド内の PE デバイスへの NAT の実装が可能になります。

VRF 対応 ALG

アプリケーション層ゲートウェイ（ALG）は、アプリケーション パケットのペイロード内の IP アドレス情報を変換するアプリケーションです。ALG は NAT で上書きする必要があるパケット ペイロード内のアドレス情報を特定し、その情報を NAT とファイアウォールに提供してデータが正しく流れるようにするための下位フローまたはドアを作成します（データ フローの一例は FTP データフローです）。ドアは、特定の基準を満たす着信トラフィックを通過させる一時的な構造です。ドアは、完全な NAT セッション エントリを作成するのに十分な情報が得られなかった場合に作成されます。ドアには、送信元と宛先の IP アドレス、および宛先ポートに関する情報が含まれています。ただし、送信元ポートに関する情報は含まれていません。メディア データが到着すると、送信元ポート情報が知らされ、ドアは実際の NAT セッションに昇格します。

VRF 対応 IPSec

VRF 対応 IPsec 機能は、IPsec トンネルを Multiprotocol Label Switching（MPLS）VPN にマップします。VRF 対応 IPsec 機能を使用すれば、単一の公開 IP アドレスを使用して、IPsec トンネルを VPN ルーティングおよび転送（VRF）にマップすることができます。

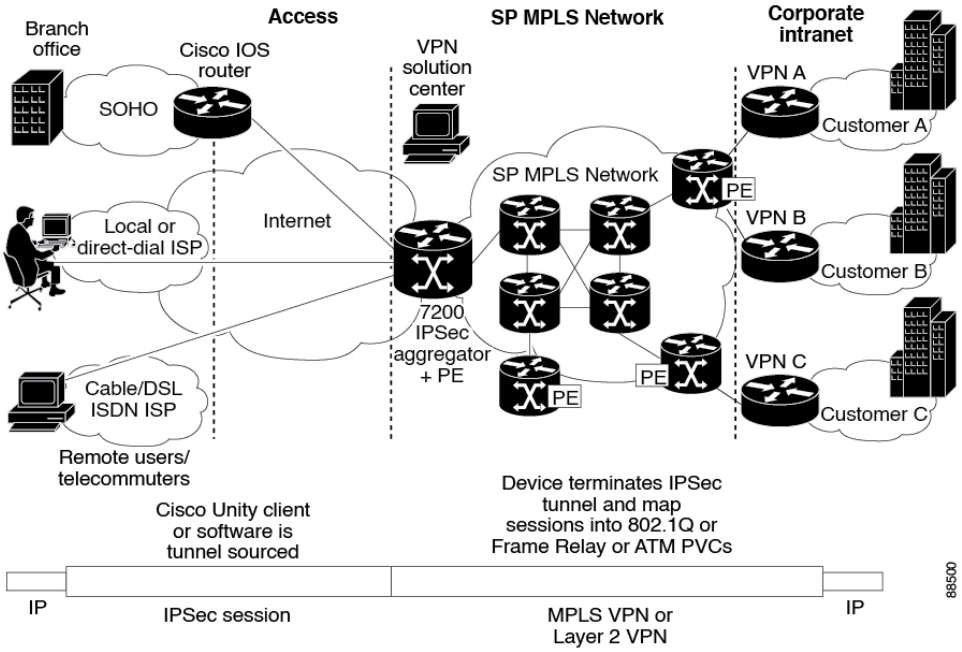
各 IPsec トンネルは、2 つの VRF ドメインに関連付けられます。外部のカプセル化されたパケットは Front Door VRF（FVRF）という VRF ドメインに属します。内部の保護された IP パケットは、Inside VRF（IVRF）というドメインに属します。つまり、IPSec トンネルのローカ

ル エンドポイントは FVRF に属しますが、内部パケットの送信元アドレスと宛先アドレスは IVRF に属すということです。

1 つ以上の IPsec トンネルを、単一のインターフェイス上で終了できます。これらのトンネルのすべての FVRF は同じものであり、そのインターフェイス上で設定されている VRF に設定されます。これらのトンネルの IVRF は異なる可能性があり、クリプト マップ エントリに付加された Security Association and Key Management Protocol（ISAKMP）プロファイル内で定義されている VRF に依存します。

次の図に、IPSec と MPLS VPN およびレイヤ 2 VPN 間のシナリオを示します。

図 *2 : IPsec* と *MPLS VPN* およびレイヤ *2 VPN* 間



VRF 対応ソフトウェア インフラストラクチャ

VRF 対応ソフトウェア インフラストラクチャ（VASI）を使用すれば、2 つの異なる VRF インスタンスを経由するトラフィックにアクセス コントロール リスト（ACL）、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適用することができます。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。この機能は、VASI インターフェイス上で IPv4 と IPv6 のユニキャスト トラフィックをサポートします。

VASI の主な用途は、VRF のより適切な分離を実現することです。VASI は、共通のインターフェイスを共有している（すべての VRF がインターネット向けの同じインターフェイスを共有している場合など）他の VRF に影響を与えることなく、各 VRF 固有の機能を VASI インターフェイスに適用できるようにします。ファイアウォールでは、この機能により、ゾーンを VASI に適用することができます。

VASI は、仮想インターフェイスのペアを使用して実装されます。ペア内の各インターフェイスが別々の VRF に関連付けられます。VASI 仮想インターフェイスは、この 2 つの VRF 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、2 つの VRF 間で NAT をサポートする必要がある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。2 つの仮想インターフェイスのペア（vasileft と vasiright）は、論理的にバックツーバックで接続されており、完全な対称性を有しています。各インターフェイスにはインデックスがあります。ペアリングの関連付けは、vasileft が自動的に vasiright にペア化されるように、2 つのインターフェイス インデックスに基づいて自動的に実行されます。BGP、Enhanced Interior Gateway Routing Protocol（EIGRP）、または Open Shortest Path First（OSPF）を使用して、スタティック ルーティングとダイナミック ルーティングのどちらかを設定することができます。BGP 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が、VASI インターフェイス間の BGP ルーティング コンフィギュレーションに適用されます。VASI の詳細については、「*VRF* 対応ソフトウェア インフラストラクチャの設定」機能を参照してください。

セキュリティ ゾーン

セキュリティ ゾーンとは、ポリシーを適用できるインターフェイスのグループです。

インターフェイスをゾーンにグループ化するには、次の 2 つの手順を実行します。

- インターフェイスを付加できるようにゾーンを作成します。
- インターフェイスを特定のゾーンのメンバーとなるように設定します。

デフォルトでは、トラフィックは、同じゾーンのメンバーであるインターフェイス間を通ります。

インターフェイスがセキュリティゾーンのメンバーである場合、そのインターフェイスと別のゾーンにあるインターフェイスの間を通るすべてのトラフィック（デバイスに送信されるか、デバイスによって開始されたトラフィックを除く）はデフォルトでドロップされます。ゾーン メンバーインターフェイスおよび別のインターフェイスに対する両方向のトラフィックを許可するには、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。ポリシーが inspect または pass アクションによってトラフィックを許可する場合、トラフィックはインターフェイスを通過できます。

ゾーンを設定するときに考慮する基本的な規則を次に示します。

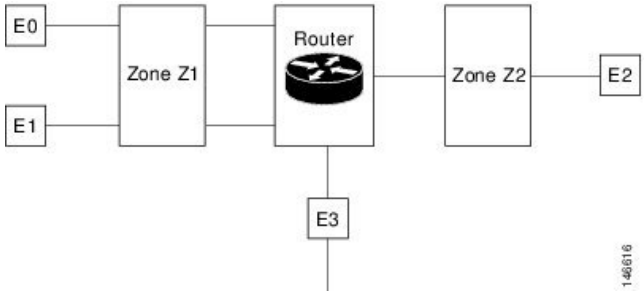
- ゾーンインターフェイスからゾーン外のインターフェイスへのトラフィックまたはゾーン外のインターフェイスからゾーンインターフェイスへのトラフィックは常にドロップされます。ただし、デフォルトゾーンが有効でないことが条件です（デフォルトゾーンはゾーン外のインターフェイスです）。
- 2 つのゾーンインターフェイス間のトラフィックは、各ゾーンにゾーンペアの関係があるかどうか、およびそのゾーンペアにポリシーが設定されているかどうかが検査されます。
- デフォルトでは、同一ゾーン内の 2 つのインターフェイス間のすべてのトラフィックは常に許可されます。

- ゾーンペアは、ゾーンを送信元ゾーンおよび宛先ゾーンの両方として設定できます。このゾーンペアで検査ポリシーを設定して、2 つのゾーン間のトラフィックを検査、転送、またはドロップできます。
- インターフェイスがメンバーになれるのは、1 つのセキュリティ ゾーンだけです。
- インターフェイスがセキュリティ ゾーンのメンバーの場合、そのゾーンを含むゾーン ペアで明示的なゾーン間ポリシーを設定しない限り、方向に関係なくそのインターフェイスを通過するすべてのトラフィックがブロックされます。
- トラフィックがデバイスのすべてのインターフェイス間を通過するようにするには、これらのインターフェイスが 1 つのセキュリティゾーンまたは別のセキュリティゾーンのメンバーである必要があります。すべてのデバイスインターフェイスがセキュリティゾーンのメンバーである必要はありません。
- ゾーンに関連付けられたすべてのインターフェイスは、同じ仮想ルーティングおよび転送（VRF）に含まれている必要があります。

図 1 には、次のことが示されています。

- インターフェイス E0 と E1 はセキュリティ ゾーン Z1 のメンバーです。
- インターフェイス E2 は、セキュリティ ゾーン Z2 のメンバーです。
- インターフェイス E3 は、どのセキュリティ ゾーンのメンバーでもありません。

図 *3*：セキュリティ ゾーンの制約



- ゾーン ペアとポリシーは、同じゾーンで設定されます。インターフェイス E0 と E1 は同じセキュリティ ゾーン（Z1）のメンバーなので、2 つのインターフェイス間のトラフィックは自由に流れます。
- ポリシーが設定されていない場合、他のインターフェイス間（E0 と E2 の間、E1 と E2 の間、E3 と E1 の間、E3 と E2 の間など）でトラフィックは流れません。
- トラフィックを許可する明示的なポリシーがゾーン Z1 とゾーン Z2 間で設定されている場合だけ、E0 または E1 と E2 間でトラフィックが流れます。
- デフォルトゾーンが有効になっていないかぎり、E3 と E0、E1、または E2 の間でトラフィックは流れません。

（注） Cisco ASR 1000 シリーズ アグリゲーション サービス ルータでは、ファイアウォールは最大 4000 のゾーンをサポートします。

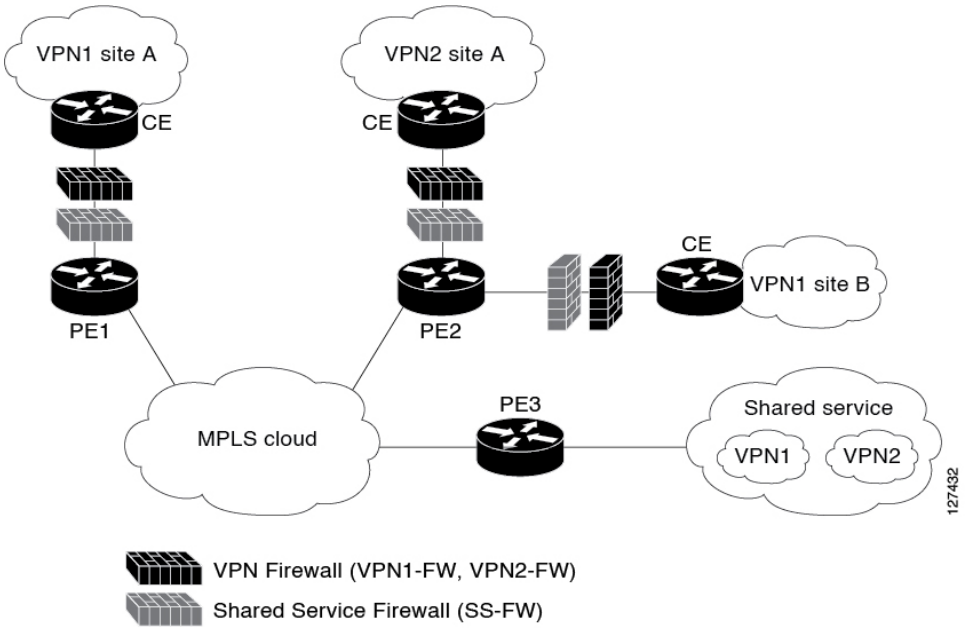
VRF 対応シスコ ファイアウォールの展開

ファイアウォールをネットワーク内の複数のポイントに展開することで、VPN サイトと共有サービス（またはインターネット）を双方向で保護できます。ここでは、次のファイアウォール展開シナリオについて説明します。

VRF 対応のシスコ ファイアウォールを擁する分散ネットワーク

次の図は、サービス プロバイダー（SP）がファイアウォール サービスを VPN カスタマーの VPN1 および VPN2 に提供し、VPN サイトと外部ネットワーク（共有サービスやインターネットなど）を双方向で保護するという一般的な状況について示します。

図 *4:* 分散ネットワーク



この例では、VPN1 には、マルチプロトコル ラベル スイッチング（MPLS）コア全体を対象とする Site A と Site B という 2 つのサイトがあります。Site A は PE1 に接続され、Site B は PE2 に接続されています。VPN2 には、PE2 に接続している 1 つのサイトのみがあります。各 VPN には、PE3 上の対応する VLAN サブインターフェイスに接続されている共有サービス内の VLAN セグメントがあります。

各 VPN（VPN1 および VPN2）には 2 つのファイアウォール ルールがあります。1 つは VPN サイトを共有サービスから保護するためのもので、もう 1 つは共有サービスを VPN サイトから保護するためのものです。VPN サイトを共有サービスから保護するファイアウォールは VPN ファイアウォールと呼ばれ、共有サービスを VPN サイトから保護するファイアウォールは共

有サービス ファイアウォールと呼ばれます。両方のファイアウォール ルールが、VPN サイトに接続された各入力プロバイダー エッジ（PE）デバイスの VPN ルーティングおよび転送（VRF）インターフェイスに適用されます。VPN ファイアウォール ルールは、VRF インターフェイスが VPN サイトへの入力であるため、入力方向に適用されます。共有サービス ファイアウォール ルールは、VRF インターフェイスが共有サービスへの出力であるため、出力方向に適用されます。

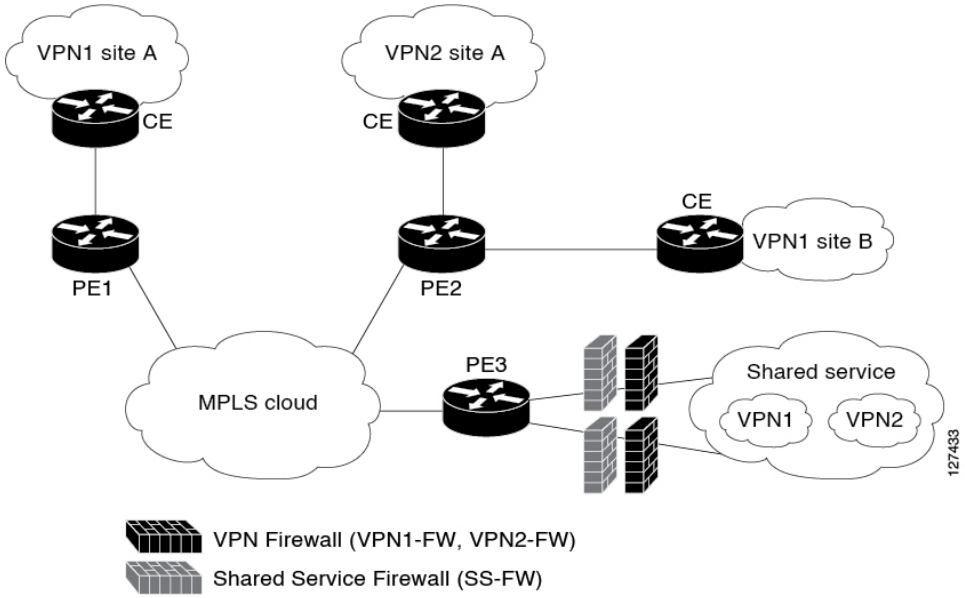
分散ネットワークを使用する利点は次のとおりです。

- ファイアウォールの導入はマルチプロトコル ラベル スイッチング（MPLS）クラウドで分散されるため、ファイアウォールの処理負荷はすべての入力PEデバイスに分散されます。
- 共有サービスは、入力 PE デバイスの VPN サイトから保護されるため、VPN サイトから送信された悪意のあるパケットは、MPLS クラウドに入る前に、入力 PE デバイスでフィルタリングされます。
- VPN ファイアウォール機能はインバウンド方向に導入できます。

VRF 対応のシスコ ファイアウォールを擁するハブアンドスポーク ネットワーク

次の図に、すべての VPN サイトのファイアウォールが、共有サービスに接続されている出力 PE デバイス PE3 に適用されるハブアンドスポーク ネットワークを示します。

図 *5:* ハブアンドスポーク ネットワーク



一般的に、個々の VPN には、共有サービスに接続されている VLAN と VPN ルーティングおよび転送（VRF）サブインターフェイスの両方または一方があります。パケットがマルチプロトコル ラベル スイッチング（MPLS）インターフェイスに到着すると、MPLS はそのパケットを、共有サービスに接続されている対応するサブインターフェイスにルーティングします。各 VPN 上のファイアウォール ポリシーが、対応するサブインターフェイス（VRF インターフェイス）に適用されます（上記の図を参照）。VPNサイトにとってはサブインターフェイスは出

力インターフェイスであるため、VPN ファイアウォール ルールは出力方向で適用されます。共有サービスにとってはサブインターフェイスは入力インターフェイスであるため、共有サービス ファイアウォールは入力方向で適用されます。

ハブアンドスポーク ネットワークの利点は次のとおりです。

- ファイアウォールは出力プロバイダーエッジ（PE）デバイス（PE3）に集中的に導入されるため、ファイアウォールの導入および管理が容易になります。
- 共有サービス ファイアウォール機能は、入力方向で適用できます。
- VPN サイトは出力 PE デバイスで共有サービスから保護されるため、パケットが MPLS クラウドに入る前に、共有サービスからの悪意のあるパケットが PE デバイスでフィルタリングされます。

VRF 対応 Cisco IOS XE ファイアウォールの設定方法

VRF、クラスマップ、およびポリシーマップの定義

手順の概要

1. **enable**
2. **configure terminal**
3. **ip vrf** *vrf-name*
4. **rd** *route-distinguisher*
5. **route-target export** *route-target-ext-community*
6. **route-target import** *route-target-ext-community*
7. **exit**
8. **class-map type inspect match-any** *class-map-name*
9. **match protocol tcp**
10. **match protocol h323**
11. **exit**
12. **policy-map type inspect** *policy-map-name*
13. **class type inspect** *class-map-name*
14. **inspect** [*parameter-map-name*]
15. **exit**
16. **class class-default**
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：	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）。

	コマンドまたはアクション	目的
	`Router> enable`	
ステップ 2	**configure terminal** 例： `Router# 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	**ip vrf** *vrf-name* 例： `Router(config)# ip vrf vrf1`	VRFインスタンスを定義し、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	**rd** *route-distinguisher* 例： `Router(config-vrf)# rd 10:1`	VRFインスタンスのルート識別子（RD）を指定します。
ステップ 5	**route-target export** *route-target-ext-community* 例： `Router(config-vrf)# route-target export 10:1`	VRF インスタンスのルート ターゲット拡張コミュニティを作成し、ターゲットVPN拡張コミュニティへのルーティング情報をエクスポートします。
ステップ 6	**route-target import** *route-target-ext-community* 例： `Router(config-vrf)# route-target import 10:1`	VRF インスタンスのルート ターゲット拡張コミュニティを作成し、ターゲットVPN拡張コミュニティへルーティング情報をインポートします。
ステップ 7	**exit** 例： `Router(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 8	**class-map type inspect match-any** *class-map-name* 例： `Router(config)# class-map type inspect match-any class-map1`	レイヤ 3 およびレイヤ 4（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、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 9	**match protocol tcp** 例： `Router(config-cmap)# match protocol tcp`	指定されたプロトコルに基づいて、クラス マップの一致基準を設定します。
ステップ 10	**match protocol h323** 例： `Router(config-cmap)# match protocol h323`	指定されたプロトコルに基づいて、クラス マップの一致基準を設定します。
ステップ 11	**exit** 例： `Router(config-cmap)# exit`	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 12	**policy-map type inspect** *policy-map-name* 例： `Router(config)# policy-map type inspect global-vpn1-pmap`	レイヤ 3 およびレイヤ 4（プロトコル固有）検査タイプ ポリシーマップを作成し、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 13	**class type inspect** *class-map-name* 例： `Router(config-pmap)# class type inspect class-map1`	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、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 14	**inspect** [*parameter-map-name*] 例： `Router(config-pmap-c)# inspect class-map1`	Cisco IOS XE 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 15	**exit** 例： `Router(config-pmap-c)# exit`	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、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 16	**class class-default** 例： `Router(config-pmap)# class class-default`	ポリシーを設定または変更できるようデフォルト クラスを指定します。 • class-default クラスはデフォルトで定義されます。**class class-default** コマンドを設定して、class-default に関連付けられるデフォルトのドロップ属性を変更します。
ステップ 17	**end** 例： `Router(config-pmap)# end`	ポリシーマップ 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。

ゾーンとゾーン ペアの定義

手順の概要

1. **enable**
2. **configure terminal**
3. **zone security** *security-zone-name*
4. **exit**
5. **zone security** *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. **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： `Router> 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： `Router# 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** *security-zone-name* 例： `Router(config)# zone security vpn1-zone`	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： `Router(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** *security-zone-name* 例： `Router(config)# zone security global-zone`	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： `Router(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： `Router(config)# zone-pair security vpn1-global-zone-pair source vpn1-zone destination global-zone`	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。 • *zone-pair-name*：インターフェイスに付加されているゾーンの名前。 • **source** *source-zone*：トラフィックの送信元ルータの名前を指定します。 • **destination** *destination-zone*：トラフィックの宛先ルータの名前を指定します。
ステップ 8	**service-policy type inspect** *policy-map-name* 例： `Router(config-sec-zone-pair)# service-policy type inspect global-vpn1-pmap`	レイヤ 7 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	**end** 例：	ゾーン ペア 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。

	コマンドまたはアクション	目的
	`Router(config-sec-zone-pair)# end`	

インターフェイスへのゾーンの適用とルートの定義

手順の概要

1. **enable**
2. **configure terminal**
3. **interface** *type number*
4. **ip vrf forwarding** *name*
5. **ip address** *ip-address mask*
6. **zone-member security** *zone-name*
7. **negotiation auto**
8. **exit**
9. **interface** *type number*
10. **ip address** *ip-address mask*
11. **zone-member security** *zone-name*
12. **negotiation auto**
13. **exit**
14. **ip route vrf** *vrf-name destination-ip-address destination-prefix interface-type number* [**global**]
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： `Router> 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： `Router# 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： `Router(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 4	**ip vrf forwarding** *name* 例： `Router(config-if)# ip vrf forwarding vrf1`	VRF をインターフェイスまたはサブインターフェイスと関連付けます。

	コマンドまたはアクション	目的
ステップ 5	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.1.1.1 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 6	**zone-member security** *zone-name* 例： `Router(config-if)# zone-member security vpn1-zone`	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 7	**negotiation auto** 例： `Router(config-if)# negotiation auto`	ギガビットイーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 8	**exit** 例： `Router(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 9	**interface** *type number* 例： `Router(config)# interface gigabitethernet 1/1/1`	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 10	**ip address** *ip-address mask* 例： `Router(config-if)# ip address 10.111.111.111 255.255.255.0`	インターフェイスに対するプライマリ IP アドレスまたはセカンダリ IP アドレスを設定します。
ステップ 11	**zone-member security** *zone-name* 例： `Router(config-if)# zone-member security global-zone`	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	**negotiation auto** 例： `Router(config-if)# negotiation auto`	ギガビットイーサネットインターフェイスの速度、デュプレックス、および自動フロー制御を自動ネゴシエーション プロトコルで設定できるようにします。
ステップ 13	**exit** 例： `Router(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 14	**ip route vrf** *vrf-name destination-ip-address destination-prefix interface-type number* [**global**] 例：	VRF インスタンス用のスタティック ルートを確立します。

	コマンドまたはアクション	目的
	`Router(config)# ip route vrf vpn1 10.111.111.0 255.255.255.0 gigabitethernet 1/1/1 global`	
ステップ 15	**end** 例： `Router(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。

VRF 対応 Cisco IOS XE ファイアウォールの設定例

例：VRF、クラス マップ、およびポリシー マップの定義

```
Router# configure terminal
Router(config)# ip vrf vrf1
Router(config-vrf)# rd 10:1
Router(config-vrf)# route-target export 10:1
Router(config-vrf)# route-target import 10:1
Router(config-vrf)# exit
Router(config)# class-map type inspect match-any class-map1
Router(config-cmap)# match protocol tcp
Router(config-cmap)# match protocol h323
Router(config-cmap)# exit
Router(config)# policy-map type inspect global-vpn1-pmap
Router(config-pmap)# class type inspect match-acl-111
Router(config-pmap-c)# inspect match-acl-111
Router(config-pmap-c)# exit
Router(config-pmap)# class class-default
Router(config-pmap)# end
```

例：ポリシー マップ、ゾーン、およびゾーン ペアの定義

```
Router# configure terminal
Router(config)# zone security vpn1-zone
Router(config-sec-zone)# exit
Router(config)# zone security global-zone
Router(config-sec-zone)# exit
Router(config)# zone-pair security vpn1-global-zone-pair source vpn1-zone destination
global-zone
Router(config-sec-zone-pair)# service-policy type inspect vpn1-global-pmap
Router(config-sec-zone-pair)# end
```

例：インターフェイスへのゾーンの適用とルートの定義

```
Router# configure terminal
Router(config)# interface gigabitethernet 0/0/0
Router(config-if)# ip vrf forwarding vrf1
Router(config-if)# ip address 10.1.1.1 255.255.255.0
```

```
Router(config-if)# zone-member security vpn1-zone
Router(config-if)# negotiation auto
Router(config-if)# exit
Router(config)# interface gigabitethernet 1/1/1
Router(config-if)# ip address 10.111.111.111 255.255.255.0
Router(config-if)# zone-member security global-zone
Router(config-if)# negotiation auto
Router(config-if)# exit
Router(config)# ip route vrf vpn1 10.111.111.0 255.255.255.0 gigabitethernet 1/1/1 global
Router(config)# end
```

VRF 対応 Cisco IOS XE ファイアウォールに関する追加情報

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』
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』
NAT	『Configuring Network Address Translation: Getting Started』
MPLS VPN	『*onfiguring a Basic MPLS VPN*』
ゾーンベース ポリシー ファイアウォール	『*Zone-based Policy Firewall*』

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

VRF 対応 Cisco IOS XE ファイアウォールに関する機能情報

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 : VRF* 対応 *Cisco IOS XE* ファイアウォールに関する機能情報

機能名	リリース	機能情報
VRF 対応 Cisco IOS XE ファイアウォール	Cisco IOS XE リリース 2.5	SP または大企業のエッジルータで VRF 対応 Cisco IOS XE ファイアウォールが設定されている場合は、Cisco IOS XE ファイアウォール機能が VRF インターフェイスに適用されます。
ファイアウォール - VRF 対応 ALG サポート	Cisco IOS XE リリース 2.5	ファイアウォール - VRF 対応 ALG サポート機能を使用すれば、正しい IP アドレス VRF ID ペアが必要な ALG トークンを作成するときに、ALG で、キャッシュされた情報から正しい IP アドレスと VRF ID を抽出することができます。

用語集

C3PL：Cisco Common Classification Policy Language。ポリシー マップとクラス マップを使用してイベント、条件、アクションに基づくトラフィック ポリシーを作成する、構造化された機能固有の設定コマンドです。

EHLO：機能のネゴシエーションを開始するための拡張 HELO 代替コマンド。このコマンドは、ESMTP プロトコルを使用してリモート SMTP サーバに接続する送信者（クライアント）を識別します。

ESMTP：Extended Simple Mail Transfer Protocol（拡張 Simple Mail Transfer Protocol）。送達通知やセッション配信などの追加機能が含まれる、Simple Mail Transfer Protocol（SMTP）の拡張バージョンです。ESMTP は、RFC 1869「SMTP Service Extensions」で定義されています。

HELO：SMTP 機能のネゴシエーションを開始するコマンド。このコマンドは、完全修飾 DNS ホスト名を使用してリモート SMTP サーバに接続する送信者（クライアント）を識別します。

MAIL FROM：電子メールメッセージの開始部分。送信者の電子メールアドレス（および使用されている場合は名前）をメッセージの From: フィールドに示して識別します。

MIME：Multipurpose Internet Mail Extension。電子メールで、テキスト以外のデータ（つまり、プレーン ASCII コードでは表現できないデータ）を転送するための規格。たとえば、バイナリ、外国語テキスト（ロシア語や中国語など）、オーディオ、ビデオなどのデータです。MIME は RFC 2045 で定義されています。

RCPT TO：受信者の電子メールアドレス（および使用されている場合は名前）。単一のメッセージを複数の受信者に配信するようなメッセージでは、複数回繰り返すことができます。

SMTP：Simple Mail Transfer Protocol。電子メール サービスを提供するインターネット プロトコル。

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。