APPENDIX A

ゾーン トラフィックの宛先変更について

この章では、トラフィックの宛先変更について説明し、Guard がレイヤ 2 およびレイヤ 3 トポロジで使用するトラフィックの宛先変更方式の詳細を示します。遠隔宛先変更方式およびネクストホップ ディスカバリ方式についても説明します。

この付録は、次の項で構成されています。

トラフィックの宛先変更におけるルータ機能について

ネットワークで、主要なルータの隣に Guard を配置します。また、Guard をアクティブにするときは、ゾーンに宛てられたトラフィックをルータから Guard に宛先変更します。Guard はゾーン トラフィックの分析とフィルタ処理を行い、宛先変更されたストリームから悪意のあるパケットを削除し、クリーンなトラフィックをメインのデータ パスに転送（注入）してゾーンに配信します。このサイクル全体をトラフィックの宛先変更プロセスと呼びます。この付録では、次の用語を使用します。

- 宛先変更元ルータ：Guard が宛先ゾーン トラフィックの宛先変更を行う元のルータ。
- 注入先ルータ：Guard がクリーンな宛先ゾーン トラフィックを転送する先のルータ。
- ネクストホップ ルータ：Guard がトラフィックの宛先変更をアクティブにする前に、宛先変更元ルータのルーティング テーブルでゾーンのネクストホップにあるルータ。
- ネクストホップ ルータの候補：ルータのグループ（このグループを構成する各ルータはすべて正当なネクストホップ ルータです）。ネットワーク内のルーティングの変更により、ネクストホップ ルータが変更される場合があります。

（注） トラフィックの宛先変更プロセスにおいて、1 台のルータが複数の機能を実行することがあります。

IP トラフィックの宛先変更について

IP トラフィックの宛先変更は、次の 2 つのタスクで構成されています。

1. ネットワークのトラフィック フローを妨げずに、Guard が 1 つ以上のゾーンから自分自身にトラフィックの宛先を変更する。
2. クリーンなトラフィックを元のデータ パスおよびゾーンに戻す。

Guard のフィルタリング アレイは、クリティカル パスに常駐しません。Guard は、影響を受けているゾーン トラフィックだけを処理およびフィルタリングの目的でリダイレクトします。Guard の攻撃フィルタリング機能を使用すると、ゾーン内で攻撃を受けているサイトだけがフィルタリングされ、正当なトラフィックは直接ゾーンを流れることができます。

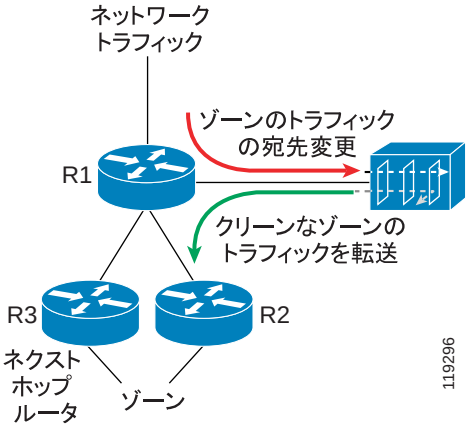
この項では、次のトピックについて取り上げます。

トラフィックの宛先変更プロセス

トラフィックの宛先変更（図 A-1 を参照）は、次の 2 つのタスクで構成されています。

1. ゾーンのトラフィックをネットワークから Guard に宛先変更する：通常、この処理は Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）を使用して実行されます。指定のゾーンに対する Guard の保護がアクティブになっている場合、Guard は宛先変更元ルータに対して BGP アナウンスメントを発行します。BGP アナウンスメントに基づいて、宛先変更元ルータはそのルーティング テーブルを変更します。ルーティング テーブルには、Guard が指定されたゾーンへの最適なネクストホップとしてリストされています。BGP アナウンスメントは宛先変更元ルータのルーティング テーブルに提示され、ゾーンのトラフィックが Guard に宛先変更されます。

図 A-1　　宛先変更プロセス



2. ゾーンのトラフィックを Guard からゾーンに転送する：Guard は宛先変更元ルータのインターフェイスを介して、クリーンなトラフィックをネクストホップ ルータに戻します（レイヤ 2 トポロジでは方式が異なります。「レイヤ 2 トポロジ」の項を参照してください）。

（注） Guard は、宛先変更元ルータの通常のルーティング テーブルを使用したクリーンなトラフィックの転送は行いません。ルータは、その IP アドレスへの最適なネクストホップ（宛先変更 BGP アナウンスメントによる）である Guard に、クリーンなトラフィックを戻します。次に、Guard はトラフィックをルータに送信し、ループを作成します。

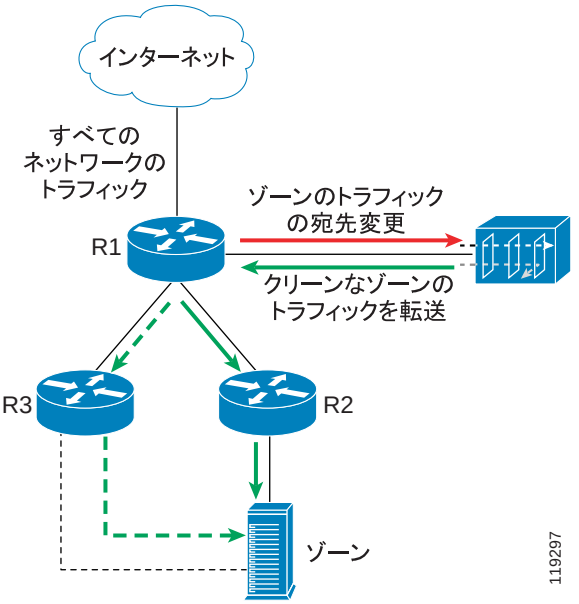
複数のネクストホップ ルータがトラフィックを転送する場合、Guard は、ネクストホップ ディスカバリと呼ばれるプロセスで、ゾーンにトラフィックを転送するために使用するネクストホップ ルータを判断します。図 A-1 で、トラフィックの宛先変更プロセスについて示します。R2 または R3 がゾーンへのネクストホップ ルータである可能性があります。Guard はネクストホップ ディスカバリ プロセスを実行し、使用するルータをラーニングします（この図では R2）。

ネクストホップ ルータが 1 つしか存在しない場合、Guard はそのルータをネクストホップ ルータとして選択します。ルーティングの変更により、ゾーンへの現在のネクストホップ ルータが動的に変更される場合があります。この場合、Guard は R1 のネクストホップ ルータのセレクションを複製することによってネクストホップ ルータを選択します。Guard は、ネクストホップ ディスカバリ プロセスを通じて、R1 のネクストホップ ルータのセレクションを取得します。

レイヤ 3 トポロジ

レイヤ 3 トポロジでは、Guard は宛先変更元ルータの R1 に直接接続されます（図 A-2 を参照）。Guard は、宛先変更されたトラフィックを R1 から受信し、それをクリーンにした後、トラフィックを R1 に戻してクリーンなトラフィックをゾーンに転送しようとします。この時点では、R1 が Guard をゾーン トラフィックの宛先にしているため、R1 と Guard の間にクローズド ループが発生する危険があります。このようなループを防止するには、Policy Based Routing（PBR; ポリシーベース ルーティング）や VPN Routing Forwarding（VRF）などのルーティング ポリシー技術を使用して、R1 が Guard からトラフィックを受信するときにトラフィックが R1 のメイン ルーティング テーブルをバイパスするようにします。これらのルーティング ポリシー技術はレイヤ 3 トポロジ環境で機能するので、Layer 3 Forwarding（L3F）方式と呼ばれます。

図 A-2　　レイヤ 3 トポロジ

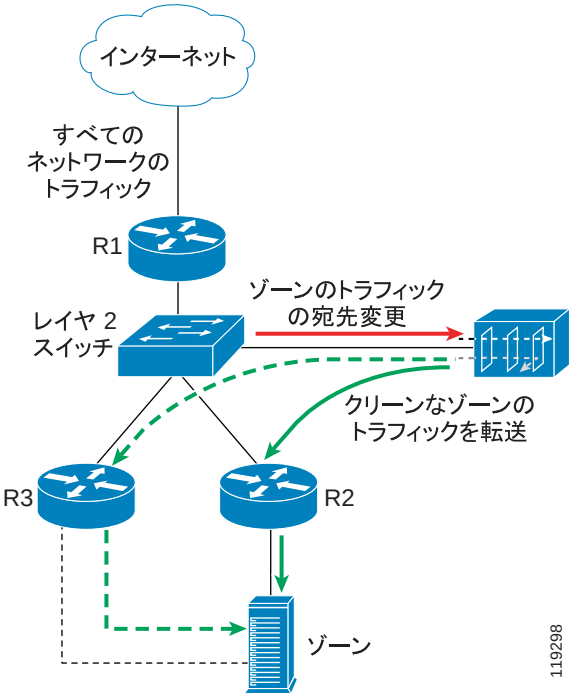


実線は、R2 がゾーンへの最適なネクストホップであることを示しています。ただし、R3 を介した場合でもゾーンに到達できます。R1 は宛先変更元と注入先の両方のルータとして機能します。R2 はネクストホップ ルータとして機能し、R3 もネクストホップ ルータの候補として機能します。

レイヤ 2 トポロジ

レイヤ 2 トポロジでは、Guard はレイヤ 2 スイッチに接続されるため、宛先変更元ルータ（R1）、ゾーンへのネクストホップ ルータ（R2）、および Guard は同一の LAN 上に配置されています（図 A-3 を参照）。Guard は Address Resolution Protocol（ARP; アドレス解決プロトコル）クエリーを R2 の IP アドレスに送信することによりネクストホップ ルータ（R2）を配置し、クリーンなゾーンのトラフィックを直接そこに転送します。ルータは、トラフィックをゾーンに転送します。

図 A-3　　レイヤ 2 トポロジ



実線は、R2 がゾーンへの最適なネクストホップであることを示しています。ただし、R3 を介した場合でもゾーンに到達できます。

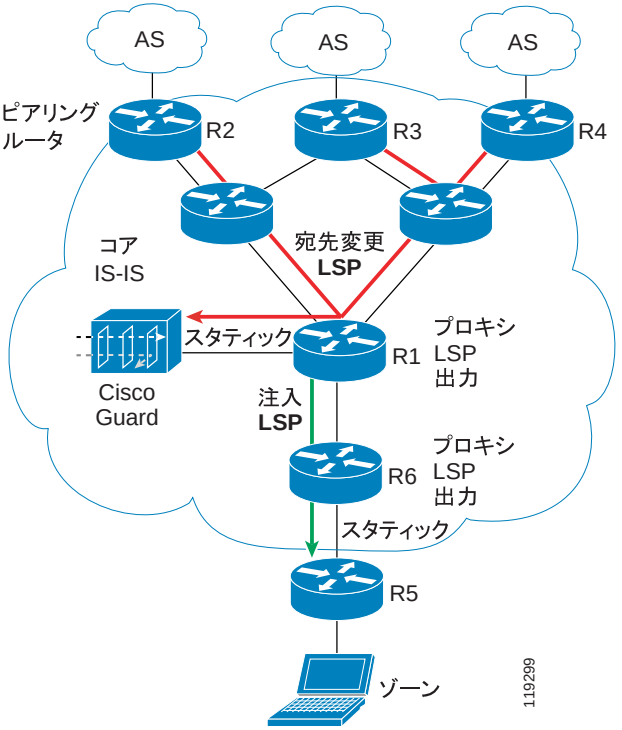
レイヤ 2 トポロジでは、注入先ルータはネクストホップ ルータと同じです。また、レイヤ 2 トポロジでは、宛先変更元ルータ、ネクストホップ ルータ、および Guard は同一の LAN 上にあります。

（注）　ネットワークによっては、ゾーンがレイヤ 2 スイッチに直接接続される場合もあります。ゾーンは Guard と同じ IP サブネットに接続される可能性があります。この場合、注入先ルータがゾーン（R2 = ゾーン）として設定されます。

遠隔宛先変更

標準の宛先変更技術では、Guard は隣接ルータからのトラフィックだけを宛先変更します。これに対して、遠隔宛先変更方式では、リモートに配置されたピアリング ルータ（Guard から数ホップ離れているようなルータ）からのトラフィックを宛先変更します。図 A-4 に、Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）ネットワークにおける遠隔宛先変更の概要を示します。

図 A-4　　Guard の使用（遠隔宛先変更の場合）



BGP 宛先変更方式

Guard は宛先変更元ルータに BGP アナウンスメントを送信して、ゾーンへのネクストホップ ルータが Guard であることを通知します。BGP アナウンスメントは、external Boarder Gateway Protocol（eBGP; 外部ボーダー ゲートウェイ プロトコル）アナウンスメントの場合も、internal Boarder Gateway Protocol（iBGP; 内部ボーダー ゲートウェイ プロトコル）アナウンスメントの場合もあります。ゾーンに関して以前に行われたルーティングの決定よりもアナウンスメントが優先されるようにするために、アナウンスメントは、宛先変更元ルータのルーティング テーブル内のゾーンを表すプレフィックスよりも長く正確なプレフィックスとともに送信されます。

アナウンスメントが Guard の隣接ルータだけに到達できるようにするために、BGP アナウンスメントは no-advertise および no-export の BGP コミュニティ ストリングとともに送信されます。この処理によって、Guard の隣接ルータだけがアナウンスメントを受信します。ゾーンを宛先とするパケットがネクストホップ ルータに到達すると、ルータはそのパケットをゾーンに転送します（Guard には戻しません）。

また、Guard は BGP アナウンスメントに特別なストリングを追加して、アナウンスメントの送信元が Guard であることを通知します。Guard は、2 つの Autonomous System（AS; 自律システム）番号、AS-number-ISP と AS-number-guard で構成されるコミュニティを使用します。AS-number-guard は専用の AS 番号です。

Guard のルーティング アナウンスメントに BGP を使用する利点として、ルータと Guard の間の通信が失われたときに、Guard へのトラフィックの宛先変更が自動的に停止する点が挙げられます。これは BGP キープアライブ プロセスによる処理です。BGP キープアライブ プロセスでは、ピア（Guard）が複数のキープアライブ メッセージに対して一定時間応答しなかった場合に、ルータからのプレフィックスが自動的に除去されます。

トラフィック転送方式について

この項では、Guard からネクストホップ ルータにクリーンなトラフィックを転送する方法について説明します。2 つの主要なネットワーク トポロジのシナリオ（レイヤ 2 トポロジおよびレイヤ 3 トポロジ）によって方式が異なります。

この項では、次のトピックについて取り上げます。

トラフィックを転送するレイヤ 2 トポロジ

レイヤ 2 トポロジでは、Guard、宛先変更元ルータ、およびネクストホップ ルータは同一の VLAN 上にあります。レイヤ 2 トポロジでは、宛先変更元ルータと注入先ルータは 2 つの別個のデバイスです。ネクストホップ ルータと注入先のルータは同じデバイスです。

トラフィックを転送するレイヤ 3 トポロジ

レイヤ 3 トポロジでは、宛先変更元ルータと注入先ルータは同じルータです（この章では、単にルータと記述します）。Guard は、ゾーン トラフィックを Guard に宛先変更するようにルータのルーティング テーブルを変更する BGP アナウンスメントを送信します。Guard はトラフィックをクリーンにした後、クリーンなトラフィックを同じルータに戻します。次に、宛先変更元ルータはそのトラフィックを、ゾーンへの最適なパスとして提示されるルータに送信します。このプロセスは、有害なルーティング ループになる可能性があります。このようなループを防止するために、ルータのルーティング テーブルを無効にするルーティング規則を Guard から戻るトラフィックに関連付けます。ルーティング テーブルを使用せずにパケットを転送する次の技術を使用して、トラフィック ループを防ぎます。

- ポリシーベース ルーティング（PBR）：以前に行われたルーティング テーブルの決定を無効にする規則を記述します。

- VPN Routing Forwarding（VRF）/ ルーティング インスタンスの使用：Guard がルータに戻すパケットをルーティングする別の転送テーブルをルータに作成します。この転送テーブルには、パケットを正確なネクストホップに転送するための情報だけが含まれます。トラフィックを Guard に宛先変更する Guard の BGP アナウンスメントは含まれません。
- トンネル：Guard とネクストホップ ルータの間に設定されたトンネルを使用して、クリーンなトラフィックを転送します。注入先ルータは、ゾーンのアドレスに対応するルーティングの決定を実行せずに、パケットをネクストホップ ルータに転送します。

（注） 遠隔宛先変更の場合は、ゾーン トラフィックがトンネルを通過して Guard に転送されるように、ピアリング ルータのメイン ルーティング テーブルが調整されます。Guard はクリーンなトラフィックを隣接ルータに転送します。隣接ルータのメイン ルーティング テーブルは、宛先変更プロセスによって変更されません。

次の 3 つの宛先変更方式は、ネクストホップ ルータの設定に依存します。ただし、ネクストホップ ルータは、各ゾーンで静的でも、動的に変更されても構いません。

- 静的ネクストホップ宛先変更方式：ネクストホップ ルータが注入先ルータに設定されます。このような宛先変更方式は、ネクストホップ ルータが各ゾーンで静的である場合に限り適用できます。
- 動的ネクストホップ宛先変更方式：このカテゴリの宛先変更方式は、ネクストホップ ルータが動的に変更される場合に適用できます。動的宛先変更方式は、静的宛先変更方式としても使用できます。ほとんどの転送技術では、Guard が現在のネクストホップ ルータをラーニングする必要があります。「ネクストホップ ディスカバリ」の項で説明しているように、Guard はネクストホップ ルータの変更についてラーニングします。表 A-1 に、宛先変更方式とその特徴をまとめます。

表 A-1　トラフィックの宛先変更方式の要約

方式	トポロジ	静的 / 動的
Layer 2 Forwarding（L2F）	レイヤ 2	動的（ネクストホップ ディスカバリを使用）
Policy-Based Routing Destination（PBR-DST）	レイヤ 3	静的
Virtual Private Network（VPN; バーチャル プライベート ネットワーク）Routing Forwarding Destination（VRF-DST）	レイヤ 3	静的
Policy-Based Routing VLAN（PBR-VLAN）	レイヤ 3	動的（ネクストホップ ディスカバリを使用）
VPN Routing Forwarding VLAN（VRF-VLAN）	レイヤ 3	動的（ネクストホップ ディスカバリを使用）
TUNNELS	レイヤ 3	動的（ネクストホップ ディスカバリを使用）

Layer 2 Forwarding 方式について

L2F 方式は、Guard、宛先変更元ルータ、およびネクストホップ ルータが同一の VLAN 上にあるネットワーク トポロジで使用されます（図 A-3 を参照）。レイヤ 2 トポロジでは、宛先変更元ルータと注入先ルータは 2 つの別個のデバイスです。ネクストホップ ルータと注入先のルータは同じデバイスです。

L2F 方式では、Guard は注入先 / ネクストホップ ルータの MAC アドレスを解決した後、そのアドレスにトラフィックを転送します。MAC アドレスを解決するために、Guard は注入先 / ネクストホップ ルータの IP アドレスに対して標準の ARP クエリーを発行します。L2F 方式を使用する場合、ルータの設定は必要ありません。

特定のネットワーク設定によっては、ゾーンがレイヤ 2 スイッチに直接接続される可能性があります。これは、ゾーンが Guard と同じ LAN に接続されることを意味します。ゾーン IP アドレスが注入先ルータとして設定されているため、Guard はトラフィックをゾーンに直接転送します。保護されているゾーンに IP 転送デバイスを介してトラフィックが送信される場合、この IP 転送デバイスは Guard のネクストホップ デバイスとして定義する必要があります。詳細については、P.4-11 の「Layer 2 Forwarding 方式」を参照してください。

Layer 3 Forwarding 方式について

この項では、レイヤ 3 ネットワーク トポロジで Guard が使用するトラフィック転送方式について説明します。

この項では、次のトピックについて取り上げます。

- Policy-Based Routing-Destination
- VPN Routing Forwarding-Destination
- Policy-Based Routing VLAN
- VPN Routing Forwarding VLAN
- トンネル宛先変更を使用したトラフィックの転送
- 遠隔宛先変更方式
- Guard へのトラフィックの宛先変更
- BGP アナウンスメント
- MPLS LSP

Policy-Based Routing-Destination

Policy-Based Routing-Destination（PBR-DST）方式を使用して、ルータのルーティング テーブルで設定されている規則と異なるルーティング規則を設定できます。PBR-DST 規則は、Guard に相対するルータのインターフェイスにだけ設定します。ユーザは設定を 1 度実行します。設定される規則では、Guard からゾーンへのトラフィックは対応するネクストホップ ルータに転送されるように指定されます。このプロセスは静的ネクストホップ ディスカバリ方式です。詳細については、P.4-16 の「PBR-DST 設定のガイドライン」を参照してください。

図 A-5　　PBR 転送方式

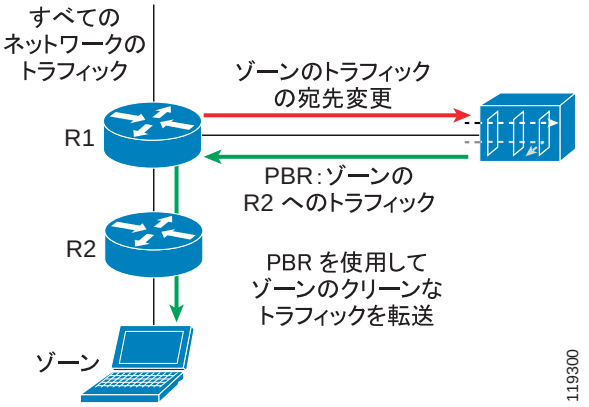


図 A-5 では、Guard から流れるゾーン トラフィックをすべて R2 に転送する規則を定義するために、Guard に相対する R1 のインターフェイスに PBR-DST 方式が適用されています。

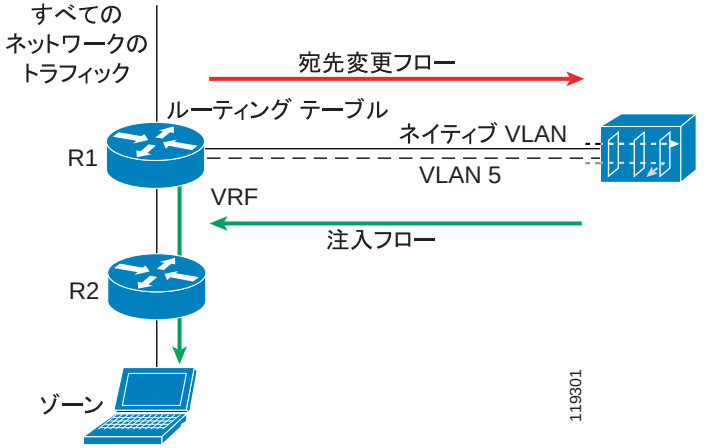
VPN Routing Forwarding-Destination

VPN Routing Forwarding-Destination（VRF-DST）方式（図 A-6 を参照）を使用して、メインのルーティング テーブルおよび転送テーブル（VRF テーブル）のほかに、別のルーティング テーブルおよび転送テーブルを設定できます。

追加のルーティング テーブルは、Guard に相対するルータのインターフェイスに流れるトラフィックをルーティングするためだけに使用されます。Guard 用の物理的なルータ インターフェイス上に次の 2 つのインターフェイスを設定します。最初のインターフェイス（ネイティブ VLAN）は、トラフィックをルータから Guard に宛先変更します。この VLAN 上のトラフィックは、グローバル ルーティング テーブルに従って転送されます。この VLAN 上で、Guard はトラフィックの宛先を Guard に変更する BGP アナウンスメントを送信します。

2 番目の VLAN は、戻されるトラフィックを Guard からルータに宛先変更します。2 番目の VLAN 上で、VRF テーブルを設定します。このテーブルには、すべてのゾーン トラフィックを特定のネクストホップ ルータに転送するための静的ルーティング規則が含まれています。VRF-DST 方式は、静的ネクストホップ宛先変更方式でもあります。VRF と PBR を使用した動的ネクストホップ宛先変更方式については、P.A-28 の「ネクストホップ ディスカバリ」で説明します。詳細については、P.4-14 の「Policy-Based Routing Destination 転送方式」を参照してください。

図 A-6　　VRF-DST 転送方式



VRF-DST 方式は、Guard に相対するルータのインターフェイスに適用されます。このインターフェイス上の VRF テーブルは、Guard から流れるゾーンのトラフィックをすべて R2 にルーティングする規則を含めるように定義します。

（注）　VRF-DST 方式は、ネクストホップ ルータが各ゾーンで静的である場合に限り適用できます。

Policy-Based Routing VLAN

PBR VLAN 方式では、Guard とルータ R1 の間に複数の VLAN（Virtual LAN, 802.1Q）トランクを設定できます（図 A-7 を参照）。トランク内の各 VLAN は別のネクストホップ ルータの候補に関連付けます。また、PBR はルータ側の各 VLAN 論理インターフェイスに設定します。各 PBR は、特定の VLAN からのすべてのトラフィックを対応するネクストホップ ルータに転送します。次に、Guard は適切な VLAN 経由でパケットを送信することにより、特定のネクストホップ ルータにパケットを転送します。Guard は、パケットを転送する VLAN を変更することにより、ゾーンのネクストホップ ルータを変更できます。この図で、ネイティブ VLAN はトラフィックの宛先変更に使用されます（このインターフェイスで Guard が BGP アナウンスメントをルータに送信します）。

図 A-7　　PBR VLAN 転送方式

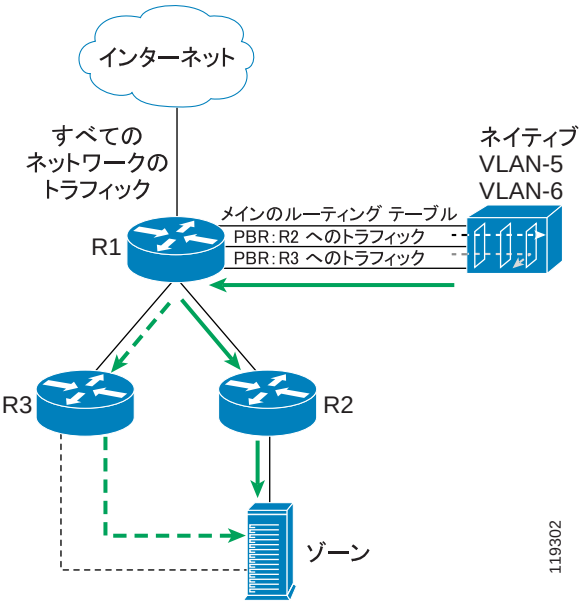


図 A-7 では、Guard に相対する R1 のインターフェイスに PBR VLAN 方式が適用されています。VLAN-5 を介して流れるトラフィックは R2 に転送され、Guard から VLAN-6 を介して流れるゾーンのトラフィックは R3 に転送されます。詳細については、P.4-23 の「Policy-Based Routing VLAN 転送方式」を参照してください。

VPN Routing Forwarding VLAN

VPN Routing Forwarding（VRF）VLAN 方式は、PBR VLAN（P.A-17 の「Policy-Based Routing VLAN」を参照）方式と同じですが、PBR テーブルの代わりに VRF テーブルを注入先ルータの各 VLAN に関連付けることができます。各 VRF テーブルには、着信するすべてのトラフィックを対応するネクストホップ ルータに転送する規則が含まれています。次に、Guard は適切な VLAN 経由でパケットを送信することにより、特定のネクストホップ ルータにパケットを転送します。Guard は、パケットを転送する VLAN を変更することにより、ゾーンのネクストホップ ルータを変更できます。図 A-8 で、ネイティブ VLAN はトラフィックの宛先変更に使用されます（このインターフェイスで Guard が BGP アナウンスメントを送信します）。詳細については、第 4 章「トラフィックの宛先変更の設定」を参照してください。

図 A-8　　VRF-VLAN 転送方式

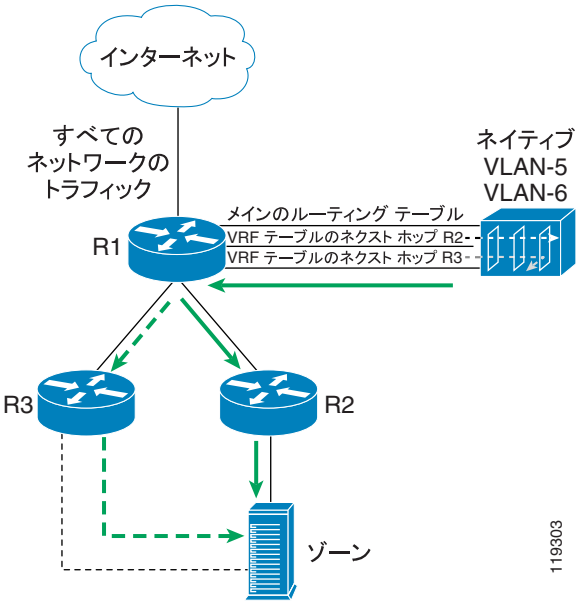
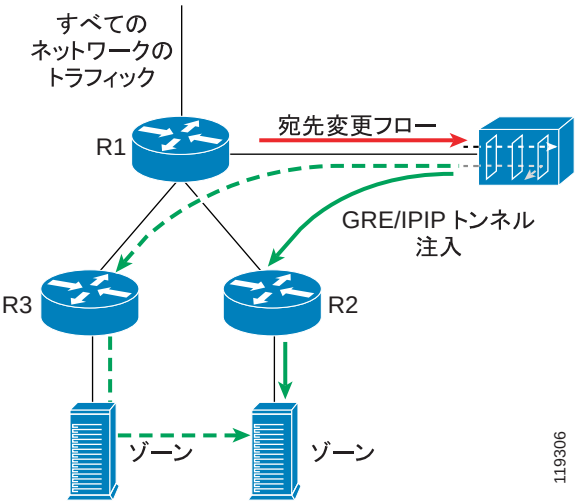


図 A-8 では、Guard に相対する R1 のインターフェイスに VRF-VLAN 方式が適用されています。VLAN-2 を経由するトラフィックは R2 に転送され、VLAN-3 を経由するトラフィックは R3 に転送されます。

トンネル宛先変更を使用したトラフィックの転送

トンネル宛先変更方式では、ユーザが Guard と各ネクストホップ ルータの間にトンネルを設定します（図 A-9 を参照）。Guard は、宛先となるゾーンのネクストホップ ルータを終端とするトンネルを介してトラフィックを送信します。戻されたトラフィックはトンネルを通過するので、注入先ルータは、トンネル インターフェイスのエンド ポイントに対してのみルーティングの決定を実行します。ゾーンのアドレスに対しては実行しません。

図 A-9　　トンネル宛先変更



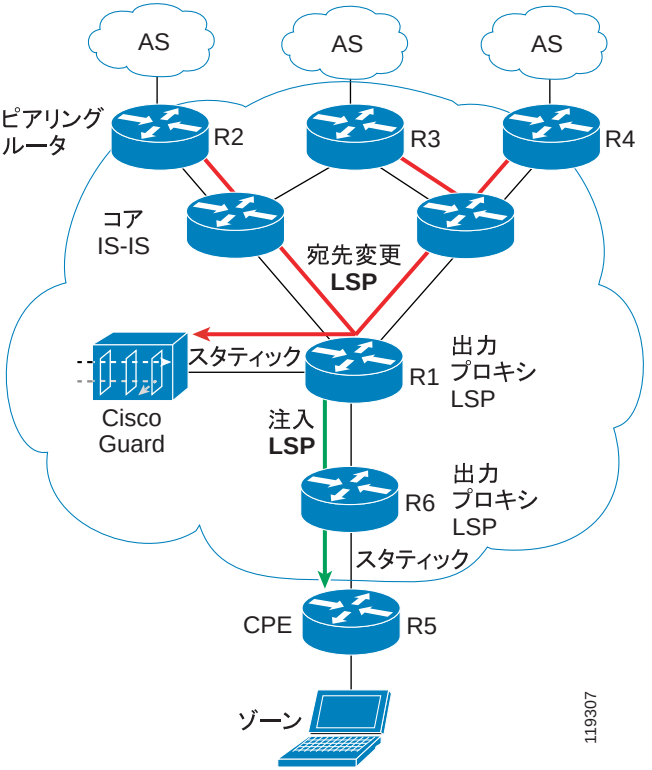
詳細については、P.4-33 の「トンネル宛先変更の転送方式」を参照してください。

遠隔宛先変更方式

標準の宛先変更技術では、Guard に直接接続されている隣接ルータからトラフィックが宛先変更されるだけですが、遠隔宛先変更方式では、Guard から何ホップも離れたところに位置するリモートのピアリング ルータからトラフィックが宛先変更されます。ゾーンへのトラフィックがピアリング ポイントからトンネル（GRE/IPIP、MPLS LSP など）を介して Guard に宛先変更されます。通常の転送方式では、R1（Guard に接続される）と他のバックボーン ルータの各転送テーブルは影響を受けないので、ネットワークにクリーンなトラフィックを注入し直すことができます。

図 A-10 で、MPLS を実装する ISP バックボーンに宛先変更がどのように実装されているかを示します。この図で、R2、R3、および R4 はピアリング ルータであり、R1 は Guard に隣接するルータです。

図 A-10　Guard の遠隔宛先変更



遠隔宛先変更は、次の 3 つの要素に分類されます。

- 宛先変更：ゾーンのトラフィックをピアリング ルータ（R2、R3、R4）から Guard に宛先変更します。
- クリーニング：悪意のあるパケットを削除し、クリーンなパケットを転送します。
- 注入：クリーンなトラフィックをネットワークに戻します。

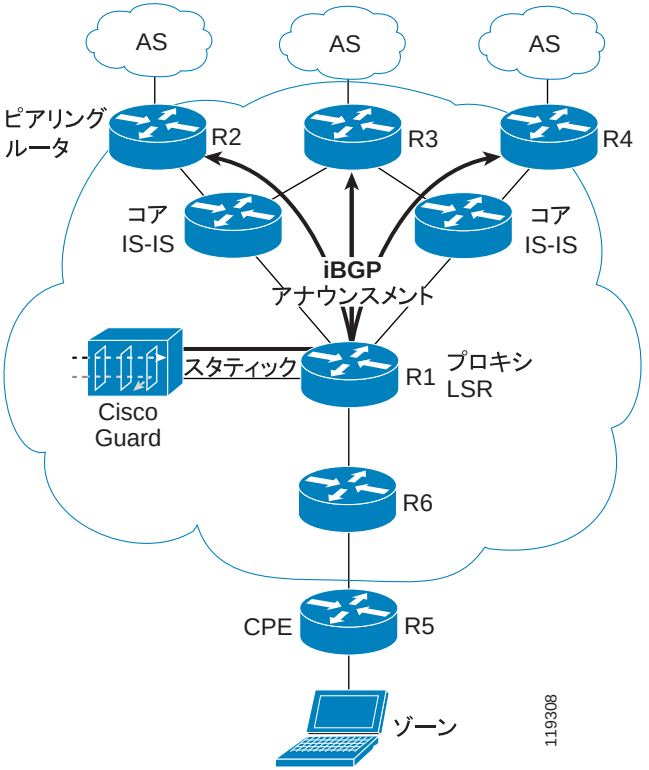
Guard へのトラフィックの宛先変更

特定のゾーンに対して攻撃が開始されると、Guard は iBGP アナウンスメントを送信します。このアナウンスメントは、トラフィックがゾーンに到達できるように、Guard のループ バック アドレス / インターフェイスを終端とする Layered Service Provider（LSP）にトラフィックをルーティングすることを通知するものです。すべてのバックボーン ルータのルーティング テーブルに BGP アナウンスメントが伝搬しないようにするために、**no-advertise** および **no-export** の BGP コミュニティ ストリングが BGP アナウンスメントに付加されます。R2、R3、および R4 だけが、Guard のループバック インターフェイスに対応するゾーンの（より長いプレフィックスを持つ）ネクストホップに関する BGP アナウンスメントを取得します。

BGP アナウンスメント

BGP アナウンスメント方式では、Guard は（**no-advertise** および **no-export** とともに）iBGP アナウンスメントを R2、R3、および R4 に送信して、ゾーンへのネクストホップが Guard のループバック インターフェイスであることを通知します。BGP アナウンスメントのネクストホップ アトリビュートを設定します（Cisco IOS ソフトウェアの **route-map** コマンドを使用）。アナウンスメントはゾーンの元のアナウンスメントよりも長いプレフィックスを使用するので、元の BGP アナウンスメントよりも優先順位が高くなります。

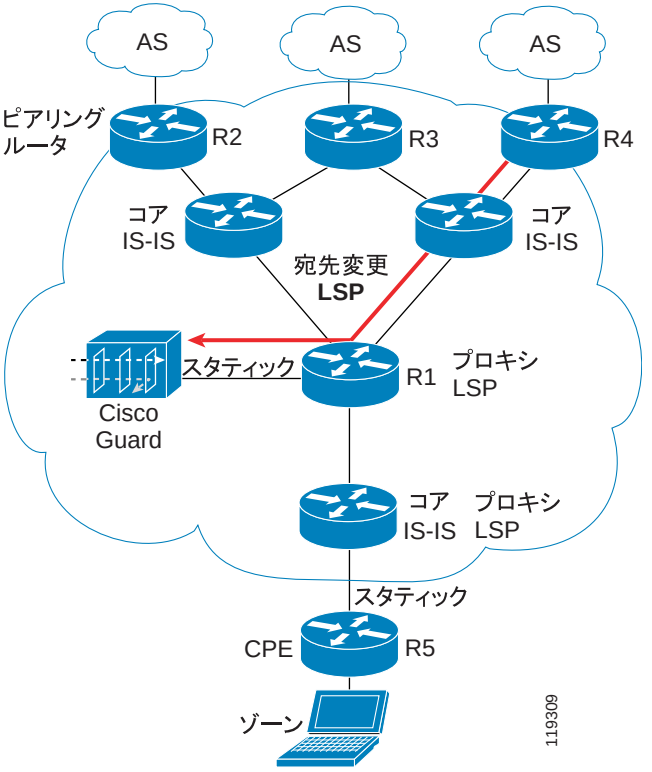
図 A-11　ピアリング ルータに対する iBGP アナウンスメント



MPLS LSP

MPLS LSP 方式では、iBGP アナウンスメントがピアリング ルータに到達した後、それらのルータが、ピアリング ポイントから Guard のループバック インターフェイスに延びる LSP にゾーン トラフィックを再ルーティングします（図 A-12 を参照）。

図 A-12　ピアリング ルータ（R2、R3、R4）から Guard への MPLS LSP



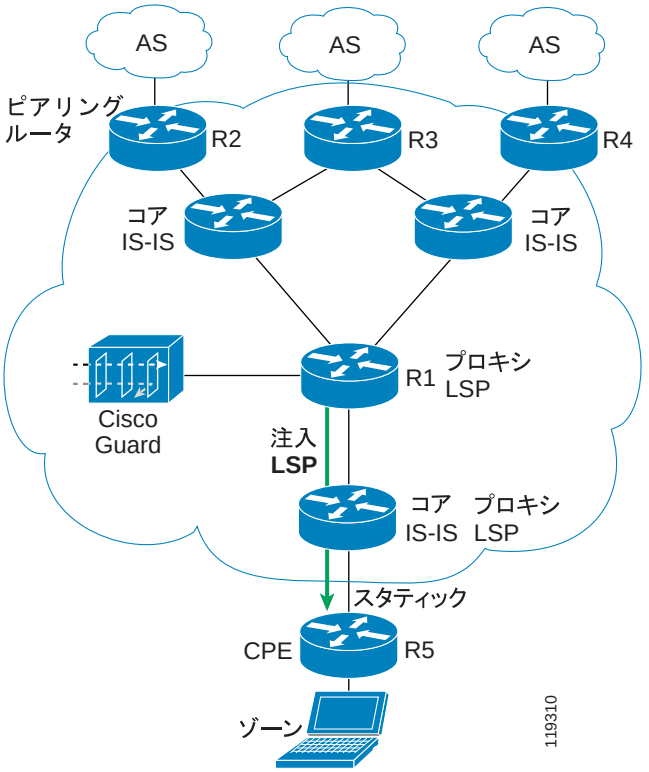
Guard は LSP の最後に位置しますが、MPLS をサポートする必要はありません。R1 は Guard に対応する出力プロキシ LSP であるため、Guard は純粋な IP（MPLS ラベルのない IP パケット）を受信するだけです。つまり、Guard のループバック インターフェイスに着信する MPLS パケットで、R1 は最終ホップの 1 つ前のホップのポッピング（MPLS ラベルの削除）を実行し、それらの MPLS パケットをスタティック ルートで Guard に直接配信します。

R1 に Guard のループバック アドレスへのスタティック ルートを設定して、IGP を介して Guard のループバック アドレスをネットワーク全体にルーティングする必要があります。このプロセスによって、スタティック ルートが IGP プロトコル（この例では IS-IS）で再配布されます。Guard は IS-IS を実行しません。

ゾーンへのトラフィックの注入

Guard はトラフィックをクリーンにした後、このトラフィックを R1 に注入します（図 A-13 を参照）。次のシナリオでは、R1 はピアリング ルータとまったく同じように動作して、候補となるすべてのゾーンへのすべてのルートを格納します。R1 は適切な LSP を使用してトラフィックをゾーンに転送します。

図 A-13　　ゾーンへのトラフィックの注入



遠隔宛先変更の注意事項と制限事項は次のとおりです。

- Guard に接続されたルータ（R1）：クリーンなトラフィックをネットワークに注入するとき、Guard はトラフィックを R1 に転送した後に IP ルックアップを実行します。R1 は、候補となるすべてのゾーンへのルートを格納する必要があります。R1 は、ピアリング ルータであってはいけません（R1 がピアリング ルータや宛先変更元ルータの場合は、別の方式でクリーンなトラフィックを注入する必要があります）。通常のコア ルータは、候補となるゾーンへのルートをすべて格納する必要はありません。コア ルータの場合は、ネットワーク内にあるルータのすべてのループバック インターフェイスへのルートを格納するだけで十分です。
- バックボーン キャパシティ：ISP バックボーン インフラストラクチャには、攻撃されたトラフィックを大量に処理する能力が必要です。
- MPLS のイネーブル化：MPLS は、バックボーン インフラストラクチャに実装する必要があります。実装できるトンネル技術は他にもいくつかあります（たとえば GRE）。
- トポロジの条件：R1 からゾーンへの LSP がエッジ ルータ（たとえば R6）で終端し、R6 が出力プロキシ LSP を実装していない場合、Guard はそのルータからのトラフィックを宛先変更できません（つまり、R6 をピアリング ルータにすることもできません）。R1 からゾーンへの LSP が Customer Premises Equipment（CPE; 宅内装置）で終端する場合は、Guard は R6 からのトラフィックを宛先変更できます（R6 をピアリング ルータにすることもできます）。CPE が MPLS をサポートしていない場合でも、出力プロキシ LSP として R6 を使用することにより、LSP が CPE で終端する場合があります。詳細については、P.4-36 の「遠隔宛先変更方式」を参照してください。

ネクストホップ ディスカバリ

トラフィックをゾーンに転送する際に、Guard は、宛先変更元ルータによる決定に従ってネクストホップ ルータとなるルータを認識する必要があります。ネクストホップ ディスカバリは、ネクストホップ ルータとなるルータをラーニングするために Guard が実行するプロセスです。ネクストホップ ルータはゾーンへのネクストホップなので（宛先変更前の宛先変更元ルータによる）、Guard は宛先変更元ルータと同じルーティング情報を参照している必要があります。ルーティング情報には、IGP と BGP の両方またはいずれか一方の情報が含まれている場合があります。Guard の隣接ルータは宛先変更元ルータの隣接ルータと同じでなければなりません。ゾーンへのルートを見つけるために宛先変更元ルータが実行するすべてのルーティング プロトコルを Guard が受信する必要があります。IGP ルーティング プロトコルだけを実行すればよい場合もあれば、IGP と BGP のプロトコルを受信しなければならない場合もあります。このソリューションが適用できるのは、宛先変更元ルータがゾーンにルーティングする方法について決定するために、ゾーンへのスタティック ルートではなくルーティング プロトコルを使用する場合だけです。スタティック ルートが使用される場合は、ルーティング プロトコルからネクストホップ ルータを判断できません（この場合は、Telnet によるディスカバリ ソリューションの使用を検討してください）。

宛先変更元ルータと同じ IGP 情報を受信するために、トンネル（GRE/IPIP）を介して宛先変更元ルータのネクストホップ ルータの候補に Guard を接続する必要があります。

BGP 情報を受信するには、Guard が宛先変更元ルータの iBGP 隣接であれば十分です。iBGP によって、宛先変更元がルーティング情報を Guard にアナウンスします。

注意　ゾーン トラフィック以外のトラフィックを受信するため、Guard はネットワークで参照可能になっている必要があります。

この項では、次のトピックについて取り上げます。

- IGP を使用したネクストホップ ルータの判定
- IGP と BGP を使用したネクストホップ ルータの判定

IGP を使用したネクストホップ ルータの判定

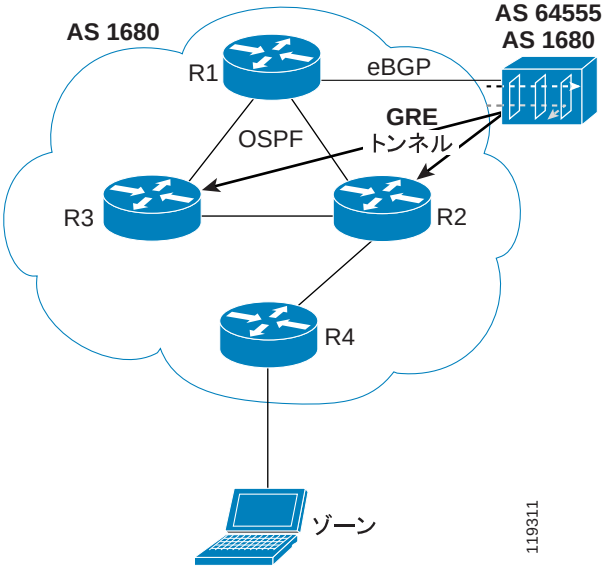
Guard は、次の場合にのみ、IGP ルーティング情報を受信してネクストホップ ルータをラーニングします。

- ゾーンが宛先変更元ルータと同じ Autonomous System（AS; 自律システム）に属する場合。ルーティングは IGP 情報プロトコル（OSPF/IS-IS/EIGRP）を使用して実行されます。
- ゾーンと宛先変更元ルータが同じ AS に属していない場合。ゾーンへのルートが BGP によってラーニングされ、ルートが IGP プロトコルに再配布されます。

Guard は OSPF と RIP だけをサポートしています。Guard が使用している Zebra ルーティング プロトコル ソフトウェアが、これらの IGP プロトコルだけをサポートしているためです。

図 A-14 に、IGP 情報を受信する方法を示します。

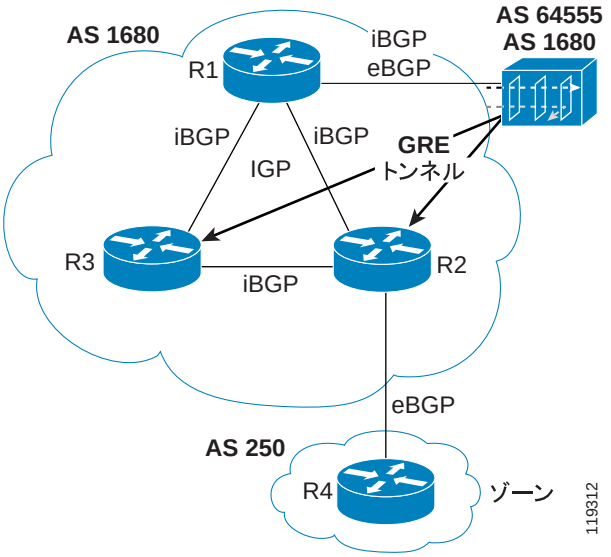
図 A-14　IGP によるネクストホップ ディスカバリ ラーニング



IGP と BGP を使用したネクストホップ ルータの判定

ゾーンが宛先変更元ルータと別の AS に存在し、BGP 情報が IGP に再配布されないときは、そのゾーンへのネクストホップ情報は IGP と BGP の両方のルーティング情報から判断されます。宛先変更元ルータは 2 つのフェーズでネクストホップを決定します。最初に、BGP を使用してゾーンへのネクスト BGP ホップをラーニングします。次に、IGP からそのネクスト BGP ピアに誘導する実際のネクストホップ ルータ（インターフェイス）をラーニングします（図 A-15 を参照）。

図 A-15　IGP+BGP によるネクストホップ ディスカバリ ラーニング



宛先変更元ルータの BGP 情報を受信するために、Guard は宛先変更元ルータから iBGP アナウンスメントを受信します。ネクストホップのアトリビュートは iBGP では変更されません（元のネクストホップが保存されます）。

この方式では、2 つの BGP デーモンが宛先変更元ルータとのピアとして機能します。最初の eBGP デーモンは宛先変更に使用され、2 番目の iBGP デーモンはネクストホップ ディスカバリ プロセスに使用されます。

宛先変更元ルータと同じ IGP 情報を受信するには、3 番目のデーモン（IGP デーモン）を、トンネルを介して宛先変更元ルータのネクストホップ ルータの候補に接続します。

Guard は、宛先変更元ルータと同じ 2 フェーズのプロセスを実行して、ゾーンへのネクストホップを確立します。最初に、Guard は BGP からゾーンへのネクスト BGP ホップ ルータをラーニングします。次に、IGP を使用してネクストホップ BGP ルータへのルートを検出します。この図で、Guard は、ゾーンへのネクストホップが R4 であることをラーニングし、このインターフェイスへの IGP ルートをラーニングします。

Guard によるトラフィック / アップデートのアナウンスのブロック

ネクストホップ ルータをラーニングする場合に限り、Guard は IGP と IBGP に関与します。Guard は、ルーティング情報をアナウンスすることも、トンネルを介してルーティング アップデート以外のトラフィックを受信することもできません。Guard によるトラフィック アップデートのアナウンスをブロックするには、次の手順に従います。

ステップ 1　IBGP によってラーニングされる情報を再配布しないように Guard を設定します。

ステップ 2　通常のトラフィックがトンネルを介してネットワークから Guard にルーティングされないようにトンネルを設定します。**ip ospf cost 65535** コマンドを使用して、Guard への OSPF トンネル リンクを最も重く設定できます。

ステップ 3　**ip ospf priority 0** コマンドを使用して、Guard が DR/BDR として選択されないことを確認します。