CHAPTER 4

ゾーン トラフィックの宛先変更

この章では、宛先変更プロセスの概要、および L2 と L3 のトポロジにおける宛先変更方式の詳細について説明します。また、章の最後に、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説明します。

Cisco と Juniper の両方のルータで構成される Guard 宛先変更メカニズム設定については、付録 A「宛先変更の設定」に記載されています。

この章には、次の主要な項があります。

概要

Cisco は、Guard という「クリーニング ボックス」をネットワーク内の主要なルータに隣接して配置しています。あるゾーンが攻撃を受ける可能性があるという警告を受信すると、そのゾーンを宛先とするトラフィックはルータから Guard に宛先変更されます。次に、Guard はゾーンのトラフィックを分析およびフィルタリングします。その結果、悪意のあるパケットは、宛先変更されたストリームから削除されます。最後に、クリーンなトラフィックがメイン データ パスに戻されてゾーンに転送されます。このサイクル全体を宛先変更プロセスと呼びます。このマニュアルでは、宛先変更に関連する次の用語を使用しています。

- **宛先変更元ルータ**：Guard で、ゾーンが送信先になっているトラフィックの元の宛先となっていたルータ。
- **注入先ルータ**：Guard で、ゾーンが送信先になっているクリーンなトラフィックの転送先となるルータ。
- **ネクストホップ ルータ**：宛先変更がアクティブになる前に、*宛先変更元*ルータに従ってゾーンへのネクストホップとなるルータ。
- **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）　ルータは複数の機能を受け持つ場合があるので、複数の用語で呼ばれることがあります。

IP トラフィックの宛先変更とは

IP トラフィックの宛先変更には 2 つのタスクがあります。最初のタスクは、1 つ以上のゾーンのトラフィックをそれらのフローを妨げることなく Guard に宛先変更します。2 番目のタスクは、正当でクリーンなトラフィックを Guard から元のデータ パスおよびゾーンに戻します。

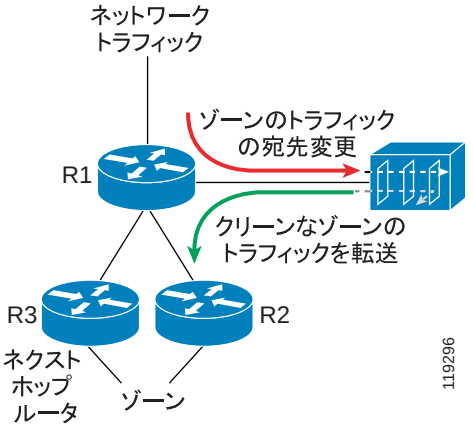
Guard の IP トラフィック宛先変更テクノロジーの主な利点は、そのフィルタリング アレイがクリティカル パスに常駐しないことです。Guard の宛先変更システムでは、非常に有効なプロセスとフィルタリングにより、ゾーンのトラフィックが異常通路にリダイレクトされます。したがって、フィルタは攻撃されたサイトのフィルタリングにすべての能力を集中できると同時に、残りのトラフィックはゾーンに直接流れるようになります。

宛先変更プロセス

宛先変更プロセスは、次の 2 つの処理で構成されています。

- **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。この 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。このアナウンスメントにより、指定のゾーンへの最適なネクストホップとして Guard がリストされます。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 4-1　　宛先変更プロセス



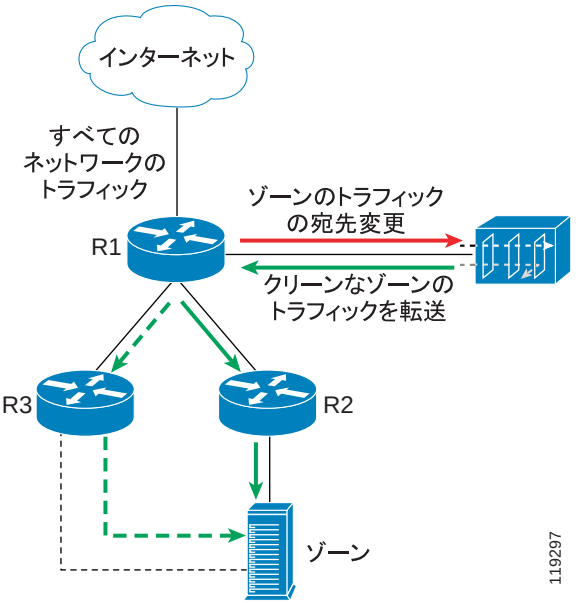
- **ゾーンのトラフィックを Guard からゾーンに転送する**：Guard は宛先変更元ルータのインターフェイスを介して、クリーンなトラフィックをネクストホップ ルータに戻します（レイヤ 2 トポロジでは方式が異なります。後述の「レイヤ 2 トポロジ」の項を参照してください）。宛先変更元ルータにある通常のルーティング テーブルを使用してクリーンなトラフィックは転送できないことに注意してください。これは、宛先変更元ルータがクリーンなトラフィックを Guard に戻しているためです。その後、Guard はループを形成するルータ（宛先変更の BGP アナウンスメントにより、その IP アドレスの最適なネクストホップは Guard になります）にトラフィックを返送します。

ネクストホップ ルータの候補が複数存在する場合、トラフィックを転送するには、ラーニングを実行してゾーンへのネクストホップ ルータを見つける必要もあります。このような場合、Guard は、ネクストホップ ディスカバリ メカニズムと呼ばれる特別なプロセスを実行します。図 4-1 に、宛先変更プロセスを示します。R2 と R3 の両方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。そのため、Guard はネクストホップ ディスカバリ プロセスを実行し、最適な候補（上記の図の R2）をラーニングします。ネクストホップ ルータが 1 つしか存在しない場合は、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。R1 のセレクションはネクストホップ ディスカバリ プロセスを介して取得されます。

レイヤ 3 トポロジ

L3 トポロジのシナリオ（図 4-2 を参照）では、Guard は宛先変更元ルータの R1 に直接接続されます。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 の間に悪意のある閉じたループが発生する危険があります。このような悪意のあるループを防止するには、ユーザがルーティング ポリシー技術（Policy Based Routing（PBR）、VPN Routing Forwarding（VRF）など）を利用します。これらの技術の主要な機能は、R1 が Guard からトラフィックを受信する際に R1 のメイン ルーティング テーブルをバイパスすることです。これらの技術は L3 トポロジ環境で機能するので、Layer 3 Forwarding 方式（L3F）と呼ばれます。

図 4-2　　レイヤ 3 トポロジ



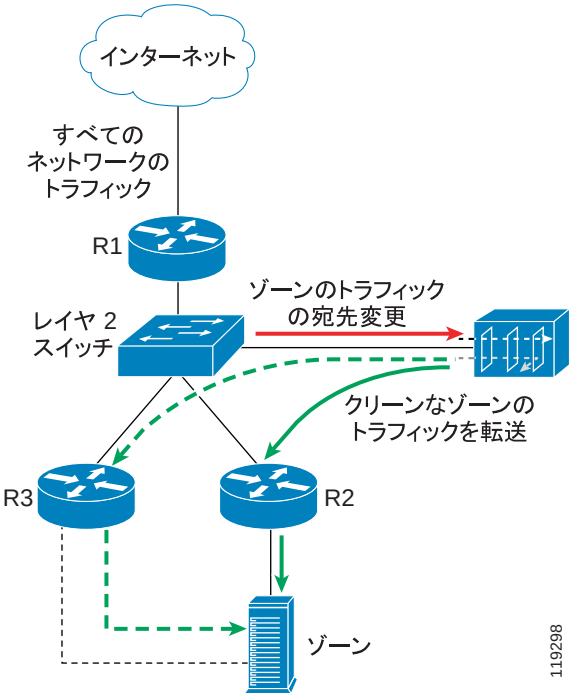
実線は、R2 がゾーンへの最適なネクストホップであることを示しています。ただし、R3 を介した場合でもゾーンに到達できます。

（注）　上記の例では、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

L2 トポロジのシナリオ（図 4-3 を参照）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。Guard は ARP 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。この処理によって、トラフィックがゾーンに転送されます。

図 4-3　　レイヤ 2 トポロジ



ルータ R2 への実直線は、R2 が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。

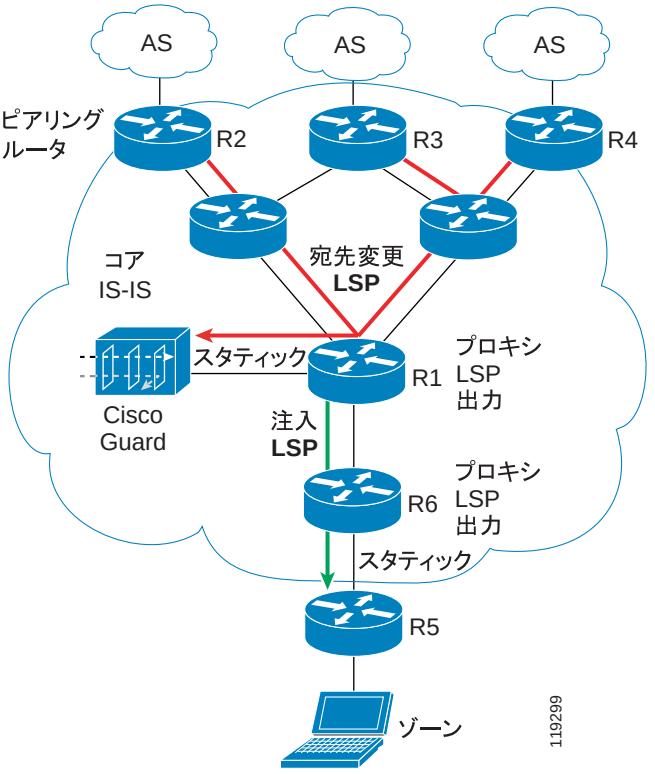
（注）　L2 トポロジでは、注入先ルータはネクストホップ ルータと同じです。また、L2 トポロジでは、宛先変更元ルータ、ネクストホップ ルータ、および Guard は同一の LAN 上にあります。

（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。したがって、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、Cisco 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 4-4 に、MPLS 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 4-4　　Guard の使用（遠隔宛先変更の場合）



トラフィック（BGP）宛先変更方式

Guard は宛先変更元ルータに EBGP（または IBGP）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が Guard 自身であることを通知します。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クスよりも長い（正確な）プレフィクスとともに送信されます。

アナウンスメントだけが Guard の隣接ルータ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 の隣接ルータはアナウンスメントを認識します。したがって、ゾーンを送信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。2 つの AS 番号（AS-number-ISP:AS-number-guard）で構成されるコミュニティが使用されます。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 を使用する利点の 1 つは、Guard の障害が発生した場合に Guard への宛先変更が自動的に停止することです。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クスが自動的に除去されます。

トラフィック転送方式

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際に使用される各方式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。

レイヤ 2 トポロジ

このトポロジでは、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 LAN 上にあります。L2 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 ルータと注入先ルータは同じデバイスです。

レイヤ 3 トポロジ

このトポロジでは、宛先変更元ルータと注入先ルータは同じルータです（単にルータと記述します）。トラフィックを宛先変更する際に、Guard は BGP アナウンスメントを送信することにより、ルータのルーティング テーブルを変更してゾーンのトラフィックを Guard に宛先変更します。Guard はトラフィックをクリーンにした後、それ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。これは悪意のあるルーティング 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が、Guard から戻るトラフィックに関連付けられています。ルータのルーティング テーブルを使用せずに、ループを防止しながらパケットを転送するには、3 つの主要な技術があります。それらの技術は次のとおりです。

- Policy Based Routing（PBR）の使用：この技術は、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に関するものです。
- VRF（VPN Routing Forwarding）/Routing Instance の使用：ルータに別の転送テーブルを作成します。これは、Guard から戻されるパケットをルーティングするために他の転送テーブルを使用するという考え方です。このテーブルには、パケットを正しいネクストホップ ルータに転送する方法に関する情報だけが含まれ、Guard（トラフィックを Guard に宛先変更する機能）からの BGP アナウンスメントは含まれません。

- トンネルの使用：トンネルは Guard とネクストホップ ルータの間に設定されます。Guard はトンネルを介してクリーンなトラフィックを転送します。したがって、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、ゾーンの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 はトラフィックをクリーンにした後、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。

上記の各宛先変更方式は、ネクストホップ ルータの設定に依存します。だたし、ネクストホップ ルータは、各ゾーンで静的である場合と動的に変更される場合があります。そのため、宛先変更方式は次のカテゴリに分類されます。

- **静的ネクストホップ宛先変更方式**：このカテゴリの方式では、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も適用できます。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ることに注意してください。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 ディスカバリの概要」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。次の表は、宛先変更方式とその特徴を要約しています。

方式	トポロジ	静的 / 動的
L2F	L2	動的（ネクストホップ ディスカバリを使用）
PBR-DST（Destination）	L3	静的
VRF-DST	L3	静的
PBR-VLAN	L3	動的（ネクストホップ ディスカバリを使用）
VRF-VLAN	L3	動的（ネクストホップ ディスカバリを使用）
ROUTING –INSTANCE Juniper ルータだけに適用できます。	L3	動的
TUNNELS	L3	動的（ネクストホップ ディスカバリを使用）
遠隔宛先変更	L3	動的

省略形

- PBR：Policy Based Routing（Juniper ルータでは Filter Based Forwarding（FBF）と呼ばれています）
- L2F：Layer 2 Forwarding
- DST：Destination
- VRF：VPN（Virtual Private Network）Routing Forwarding
- VLAN：Virtual LAN

次の各項で、Guard のさまざまな転送方法について詳細に説明します。

Layer 2 Forwarding 方式（L2F）

レイヤ 2 トラフィック転送方式は、3 つのデバイス（Guard、宛先変更元ルータ、およびネクストホップ ルータ）がすべて同一の VLAN 上にある場合に L2 トポロジのシナリオ（図 4-3 を参照）で使用されます。L2 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。この 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 転送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 Cisco Guard と同じ LAN に接続されることを意味します。この場合、Guard はトラフィックをゾーンに直接転送します。つまり、ゾーンの IP アドレスは注入先ルータとして設定されています。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 Cisco Guard のネクストホップとして定義する必要があります。詳細については、付録 A「宛先変更の設定」の「Layer-2-Forwarding（L2F）方式」の項を参照してください。

Layer 3 Forwarding 方式

Policy Based Routing（PBR）- DST（Destination）

この方式では、ルータのルーティング テーブルに設定されているものとは異なるルーティング規則の設定が可能です。PBR 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されます。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。したがって、これ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、付録 A「宛先変更の設定」の「PBR-DST 設定のガイドライン」の項を参照してください。

図 4-5　　PBR 転送方式

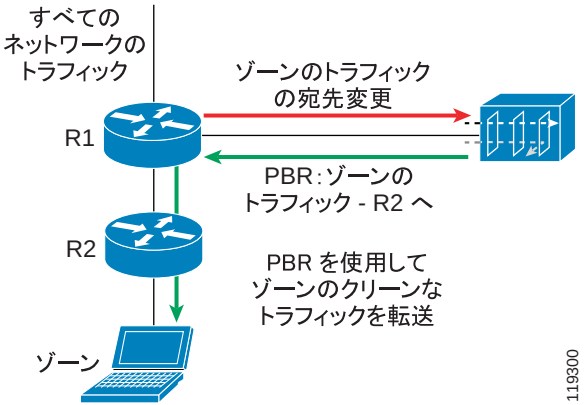


図 4-5 では、Guard から流れるゾーンのトラフィックをすべて R2 に転送する規則を定義するために、Guard に相対する R1 のインターフェイスに PBR 方式が適用されています。

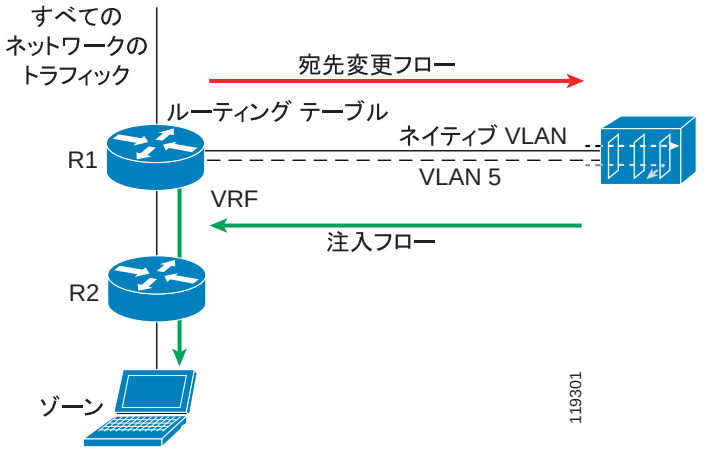
（注）　Juniper で PBR に相当するものは FBF（Filter Based Forwarding）です。

VRF（VPN Routing Forwarding）*VRF- DST*（*Destination*）

この機能では、メイン ルーティング テーブルおよび転送テーブルに加え、別のルーティングおよび転送テーブル（VRF テーブル）の設定が可能です。追加のルーティング テーブルの設定は、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。したがって、2 つの別個のインターフェイスが Guard に相対するルータの物理インターフェイスに設定されます。最初のインターフェイス（ネイティブ VLAN）は、ルータから Guard に宛先変更するために使用されます。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。また、この VLAN では、Guard はトラフィックを Guard に宛先変更するための 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するために使用されます。VRF テーブルは、この 2 番目の VLAN に設定されます。また、VRF テーブルには、特定のネクストホップ ルータにゾーン トラフィックをすべて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。したがって、これも静的ネクストホップ宛先変更方式です。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、次に説明します。詳細については、付録 A「宛先変更の設定」の「Policy-Based Routing Destination（PBR-DST）トラフィック転送方式」の項を参照してください。

（注）　Juniper で VRF に相当するものは「ルーティング インスタンス」と呼ばれています。これは、1 つのルータで複数のルーティング テーブルと転送テーブルをサポートしています。この機能により、動的宛先変更も容易に実現できます。このため、Juniper ルータでは、VRF-DST 宛先変更方式の代わりにルーティング インスタンス宛先変更方式を使用することを推奨します。詳細については、「Juniper ルーティング インスタンス」の項を参照してください。

図 4-6　VRF 転送方式



VRF 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されます。

（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。

ネクストホップが動的に変更されるトポロジでは、次のメカニズムが適用されます。

VLAN Policy Based Routing（PBR VLAN）

この方式では、Guard とルータ R1 の間に複数の VLAN（Virtual LAN, 802.1Q）トランクが設定されます（図 4-7 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られます。また、PBR はルータ側の各 VLAN 論理インターフェイスに設定されます。各 PBR は、特定の VLAN 上を流れるすべてのトラフィックを対応するネクストホップ ルータに転送するように設定されます。その結果、Guard は該当の VLAN を介してパケットを伝送することにより、特定のネクストホップ ルータにパケットを転送します。このため、Guard は、パケットが転送される 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。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 4-7　　PBR VLAN 転送方式

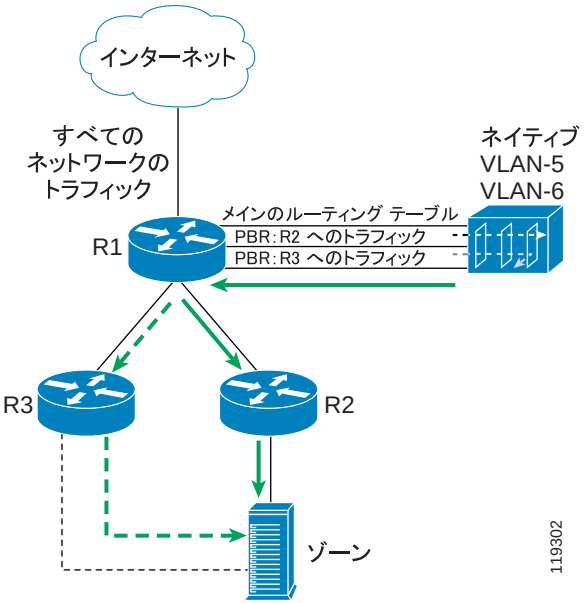


図 4-7 では、Guard に相対する R1 のインターフェイスに PBR VLAN 方式が適用されています。この例では、VLAN5 を介して流れるトラフィックは R2 に転送され、Guard から VLAN6 を介して流れるゾーンのトラフィックは R3 に転送されます。詳細については、付録 A「宛先変更の設定」の「PBR-VLAN 設定」の項を参照してください。

VLAN VRF

この方式は前述の PBR VLAN と同じです（ただし、PBR テーブルの代わりに VRF テーブルが注入先ルータの各 VLAN に関連付けられています）。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るだけです。その結果、Guard は該当の VLAN を介してパケットを伝送することにより、特定のネクストホップ ルータにパケットを転送します。このため、Guard は、パケットが転送される 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。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、付録 A「宛先変更の設定」を参照してください。

図 4-8　VRF-VLAN 転送方式

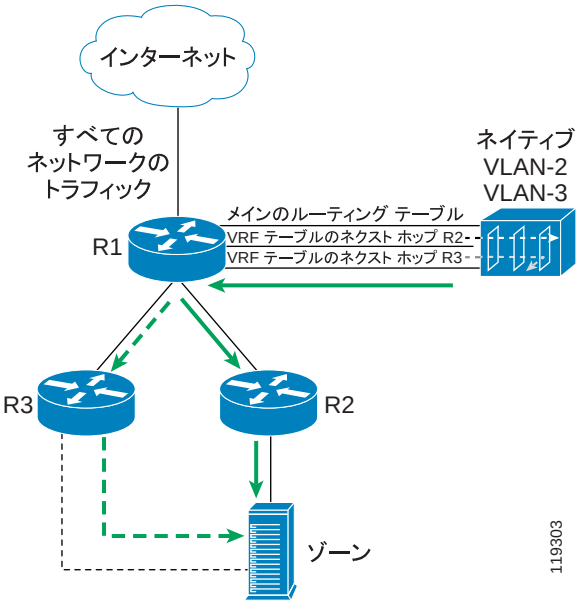
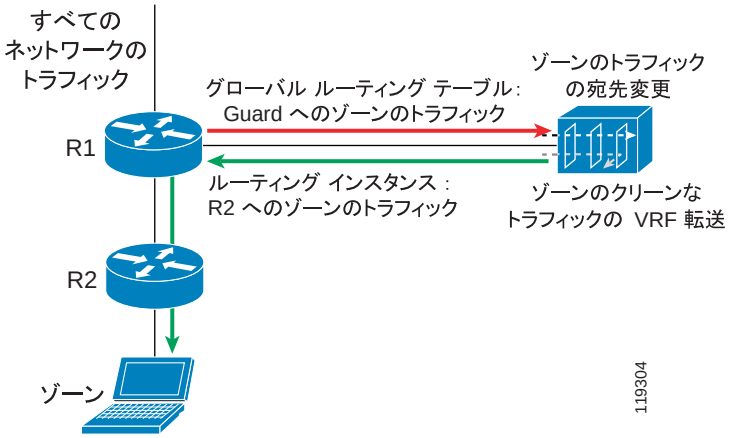


図 4-8 では、Guard に相対する R1 のインターフェイスに VRF-VLAN 方式が適用されています。VLAN5 を介して流れるトラフィックは R2 に転送され、VLAN6 を介して流れるトラフィックは R3 に転送されます。

Juniper ルーティング インスタンス

図 4-9　Juniper ルーティング インスタンス



ルーティング インスタンスは、Guard に相対する R1 の（Juniper ルータ）インターフェイスに実装されます。このルーティング インスタンスのルーティング テーブルはメイン ルーティング テーブルとは異なります。このルーティング テーブルには、メイン ルーティング テーブルに提示されるすべてのルートが含まれます（ただし、Guard アナウンスメントの結果としてのルートは除きます）。

ルーティング インスタンス方式では、Guard から戻るトラフィックをルーティングするために、別のルーティング テーブルをユーザが設定します（Guard インターフェイス ルーティング テーブル）。ユーザは、Guard に相対するルータのインターフェイスに設定する Filter Based-Forwarding（FBF）規則による方式を使用します。FBF 規則は、Guard から着信するトラフィックを Guard インターフェイス ルーティング テーブルを使用して転送するように指示します。Guard インターフェイス ルーティング テーブルには、グローバル ルーティング テーブルのすべてのルートが入力されます（ただし、Guard からのルートであることを示す Cisco の特別なコミュニティ ストリングのタグが付いているルートは除きます）。巨大なグローバル ルーティング テーブルが存在するときは、候補となるゾーンだけ

にルートの伝搬を制限することにより、Guard インターフェイス ルーティング テーブルのザイズを縮小できる場合もあります。この方式は動的ネクストホップ宛先変更方式であることに注意してください。詳細については、付録 A「宛先変更の設定」の「Juniper ルータのルーティング インスタンス」の項を参照してください。

図 4-10　Juniper ルータ内部の図

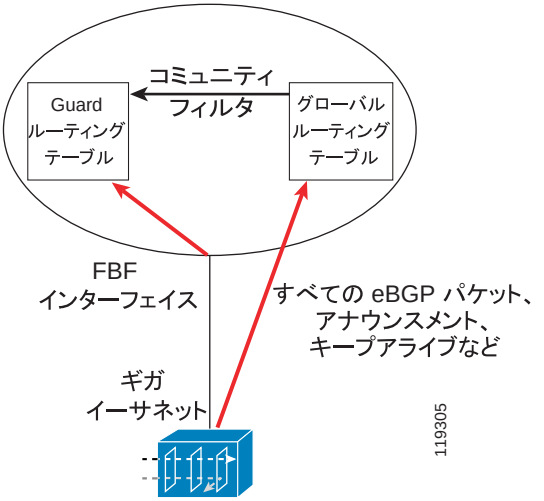
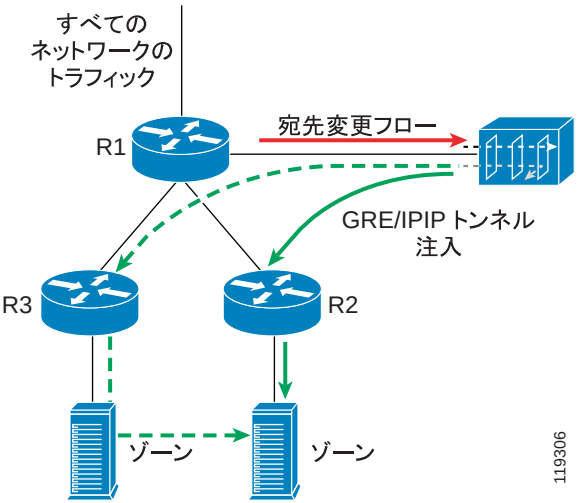


図 4-10 は、この宛先変更方式に対応するルータ内部の情報とトラフィックのフローを示しています。これに対して、図 4-8（VRF-VLAN 転送方式）はトラフィックの外部フローを示しています。

トンネルを介した転送

この方式では、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。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 4-11　　トンネル宛先変更



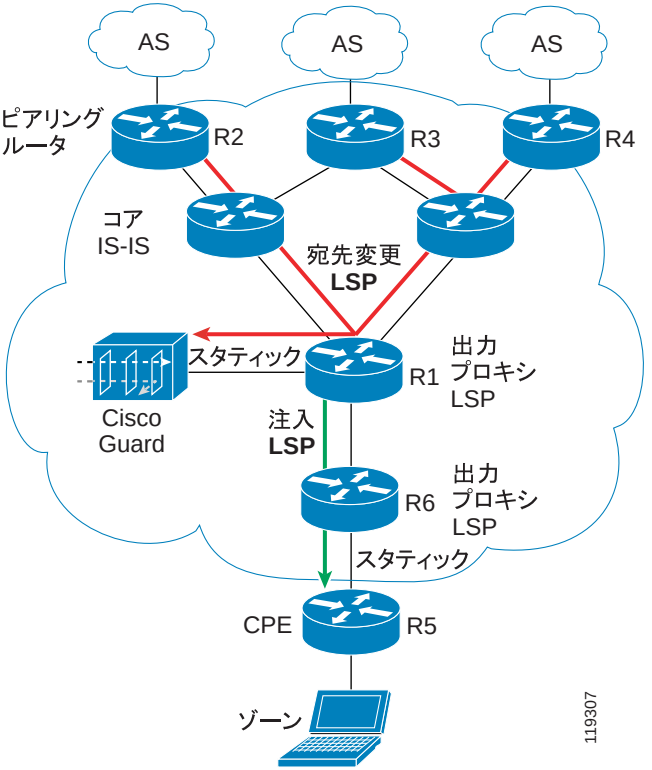
トンネル宛先変更方式では、ユーザが Guard と候補となる各ネクストホップ ルータの間にトンネルを設定します。Guard は、ネクストホップ ルータを終端とするトンネルを介してトラフィックを送信します。このため、Guard は、パケットが転送されるトンネルを変更することにより、指定のゾーンへのネクストホップ ルータを変更できます。詳細については、付録 A「宛先変更の設定」の「トンネル宛先変更」の項を参照してください。

遠隔宛先変更方式

標準の宛先変更技術では、Cisco Guard は直接接続された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。基本的には、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 に宛先変更されるという考え方です。通常の転送方式では、R1（Guard によって接続される）と他のバックボーン ルータの各転送テーブルは両方とも影響を受けないので、クリーンなトラフィックを注入し直すことができます。これはトンネル技術によるものです。下記の例で、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。

図 4-12 は遠隔宛先変更の概要を示しています。この中で、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 4-12　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 Guard によって削除し、「クリーン」なパケットを転送します。
- **注入**：ルート上の「クリーン」なトラフィックをゾーンに戻します。

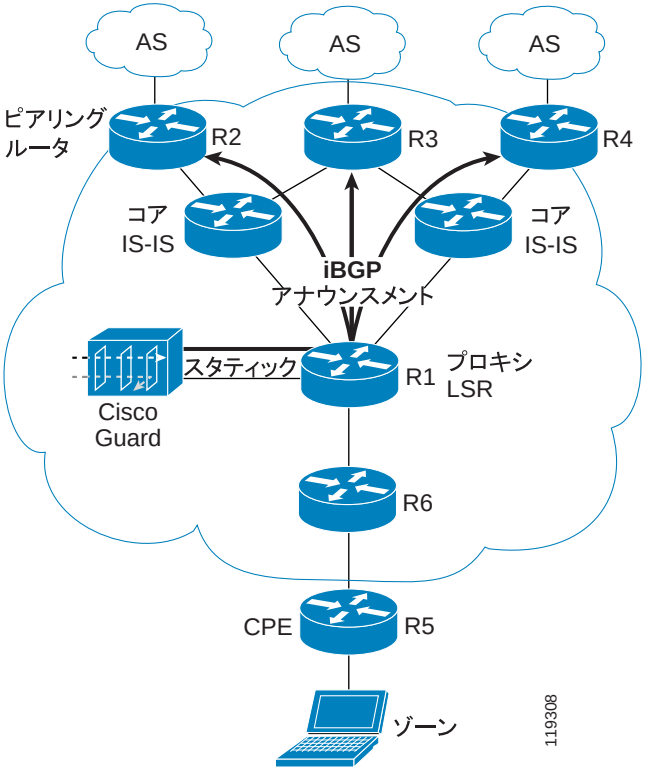
Cisco Guard へのトラフィックの宛先変更

特定のゾーンに対して攻撃が開始されると、Guard が iBGP アナウンスメントを送信することによって宛先変更が実現されます。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 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。そのため、R2、R3、および R4 だけが、対応する Guard のループ バック インターフェイスへのゾーンの（より長いプレフィクスを持つ）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

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。このプロセスは、（Cisco IOS のコマンド ルートマップを使用して）BGP アナウンスメントにネクストホップの属性を適切に設定することによって実現されます。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。

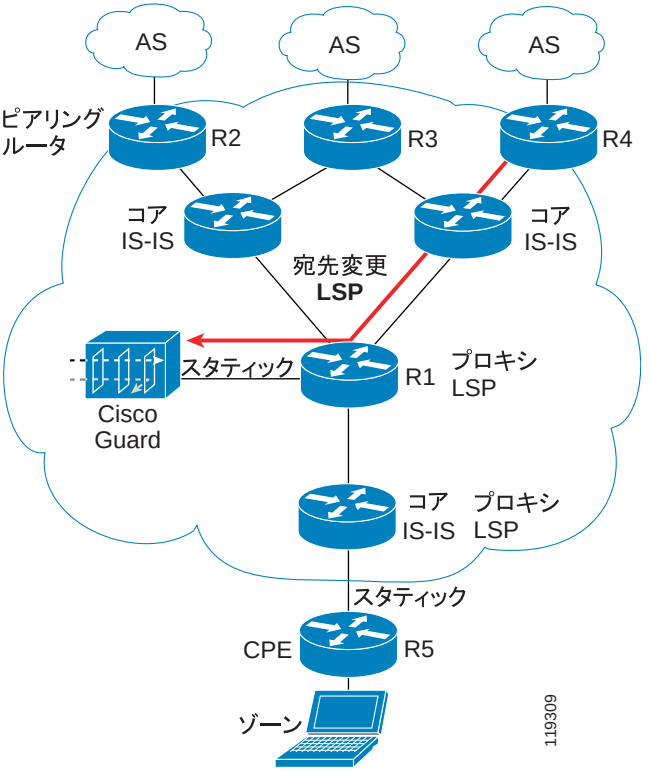
図 4-13　ピアリング ルータに対する iBGP アナウンスメント



MPLS LSP

iBGP アナウンスメントがピアリング ルータに到達した後、それらのルータはゾーンのトラフィックを LSP に再ルーティングして、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誘導します。

図 4-14　　ピアリング ルータ（R2、R3、R4）から Guard への MPLS LSP



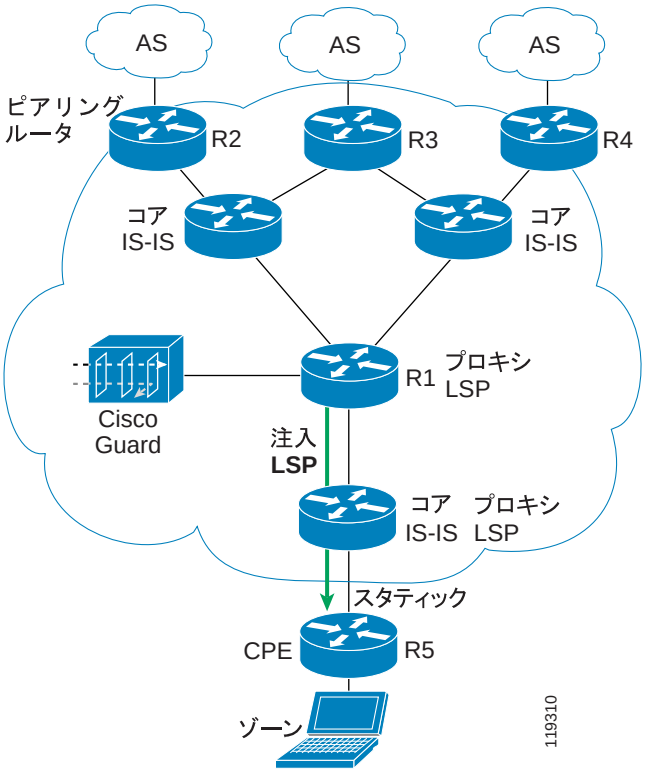
Guard は LSP の最後に位置し、MPLS のサポートには必要ありません。R1 は Guard に対応する出力プロキシ LSP であるため、Guard は純粋な IP を受信するだけです。つまり、Guard のループ バックに着信する MPLS パケットに現れる最後のホップより以前に、R1 は出力プロキシ LSP を実行し、それらの MPLS パケットをスタティック ルートで Guard に直接配信します。

Guard のループ バック アドレスは、ネットワーク全体で IGP を介してルーティング可能でなければなりません。これを実現するために、R1 には Guard のループ バック アドレスへのスタティック ルートが設定されています。このため、IGP プロトコル（上記の例の IS-IS）を使用して、このスタティック ルートが再配布されます。Guard は IS-IS を実行しないことに注意してください。

Guard からゾーンへのトラフィックの注入

Cisco Guard は、トラフィックをクリーンにした後、R1 に注入し直します。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。したがって、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 4-15　　ゾーンへのトラフィックの注入



注意事項と制限事項

計画した遠隔宛先変更方式が正しく機能するためには、次のようないくつかの点を考慮に入れる必要があります。

- Guard に接続されたルータ（R1）：トラフィックをゾーンに転送し直す場合、トラフィックが R1 に注入された後に IP ルックアップを実行します。ルータ 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。この方式ではルータ R1 をピアリング ルータにしないように注意してください（ルータ R1 をピアリング ルータおよび宛先変更元ルータにする場合は、クリーンなトラフィックを注入するために別の方式を使用する必要があります）。また、通常のコア ルータは、候補となるゾーンへのルートを必ずしもすべて格納する必要がないことにも注意してください。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 の有効化：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）。これに対して、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（つまり、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ることに注意してください。詳細については、付録 A「宛先変更の設定」の「遠隔宛先変更」の項を参照してください。

ネクストホップ ディスカバリの概要

トラフィックをゾーンに戻す際に、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 ルータの情報を取得するには、次の 2 つの技術があります。

- ルーティング プロトコル ネクストホップ ディスカバリ
- Router Management Protocol（RMP）ネクストホップ ディスカバリ

ルーティング プロトコル ネクストホップ ディスカバリ

ルーティング プロトコルによるネクストホップ ルータのラーニングは、Guard が持っているルーティング情報の評価は宛先変更元ルータの評価と一致している必要があるという考え方に基づいています。これらの評価が一致している必要があるのは、（宛先変更以前の宛先変更元ルータに応じて）ネクストホップ ルータがゾーンへのネクストホップとなるためです。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ることに注意してください。つまり、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 プロトコルを通常どおり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、ネクストホップ ルータはルーティング プロトコルから推論できません。したがって、ユーザは「Telnet によるディスカバリ」のソリューションを考慮する必要があります。

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

BGP 情報を受信するための十分な条件は、Guard が宛先変更元ルータの IBGP 隣接ルータになっていることです。その場合、IBGP では、宛先変更元ルータがそのルーティング情報を Guard にアナウンスします。

ルーティング情報の受信中に Guard がネットワークに対して「可視」になっているために、ゾーン トラフィック以外のトラフィックを取得しようとする状況が発生しないように十分注意してください。

次の項では、Guard がネクストホップ ルータをラーニングする方法について説明します。考えられるシナリオは次のとおりです。

- IGP 情報からネクストホップ ルータが導かれる（Guard は IGP 情報だけを受信すればよい）。
- IGP+BGP 情報からネクストホップ ルータが導かれる（Guard は IGP+BGP 情報を受信する必要がある）。

IGP 情報からネクストホップ ルータが導かれる

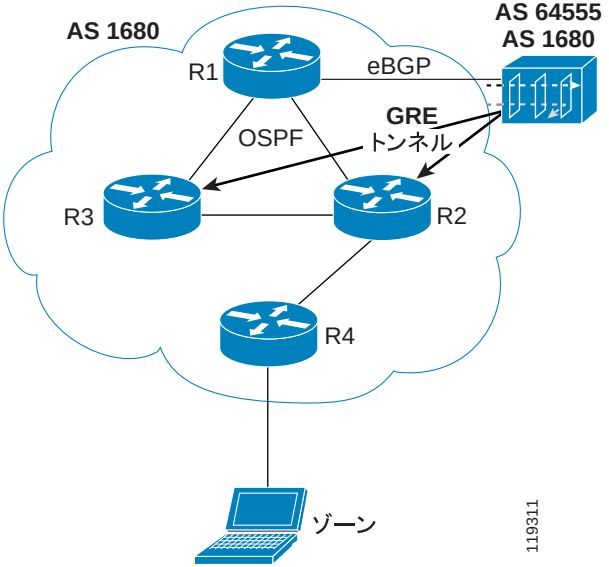
IGP ルーティング情報だけを受信することによってネクストホップ ルータをラーニングできるのは、次の 2 つの場合です。

- 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。したがって、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別の AS に属する場合。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。

現在、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 4-16 は、IGP 情報だけを受信すればよい場合を示しています。

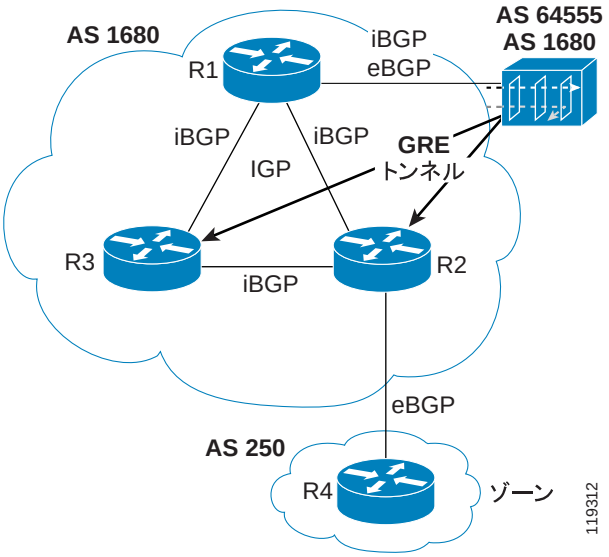
図 4-16　IGP によるネクストホップ ディスカバリ ラーニング



IGP+BGP からネクストホップ ルータが導かれる

ゾーンが宛先変更元ルータと別の AS に存在している場合、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導かれる必要があります。このような場合、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することに注意してください。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 4-17　　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。ネクストホップの属性は 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）。

この方式には、宛先変更元ルータに相当する 2 つの BGP デーモン（Guard 上に必要）が存在することに注意してください。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（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される IGP デーモン）が Guard 上に必要になります。

Guard は、宛先変更元ルータと同じ 2 フェーズの再帰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、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見つけます。上記の図で、Guard は、ゾーンへのネクストホップが R4 であることを IBGP からラーニングし、このインターフェイスへの IGP ルートを IGP からラーニングします。

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。そのため、次のステップを実行する必要があります。

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。
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るようにトンネルを設定します。これは、Guard への OSPF トンネル リンクに最高の重み付けを設定することによって実現されます。この設定には、**ip ospf cost 65535** コマンドを使用します。
3. ユーザは、Guard が DR/BDR として選択されていないことを確認する必要があります。この確認には、**ip ospf priority 0** コマンドを使用します。

Router Management Protocol（RMP）を使用したネクストホップ ディスカバリ

Guard は「Telnet」接続または「SSH」接続を使用して、宛先変更元ルータからルーティング情報を直接取得できます。これは、標準のルーティング プロトコル（前項を参照）を使用したネクストホップ ディスカバリの他に使用できるネクストホップ ディスカバリです。最初に Telnet が試行され、それが失敗した場合は、代わりに Secured Shell（SSH）が使用されます。Guard は Cisco と Juniper のルータをサポートしています。Guard がルータで使用するコマンドは、**show ip route .... longer**（Cisco の場合）または **show route.... best**（Juniper の場合）だけです。ルータから取得されたルートは、アドミニストレーティブ ディスタンス 10 を使用して Zebra ルーティング テーブルに挿入され、Zebra の **show ip route** コマンド内部で「M」という文字で表現されます。