CHAPTER 4

トラフィックの宛先変更の設定

この章では、Cisco Guard（Guard）でトラフィックの宛先変更を設定する方法について説明します。

（注） このドキュメントに記載されている Cisco ルータの設定に関する内容は、情報提供だけを目的としています。詳細については、適切なユーザ ガイドを参照してください。

トラフィックの宛先変更設定は、トポロジに依存しません。レイヤ 2 トポロジとレイヤ 3 トポロジの設定手順は同じです。

Guard のメモリへの設定変更をすべて保存するには、ルータ設定モードで **write memory** コマンドを使用します。

この章は、次の項で構成されています。

BGP 宛先変更方式について

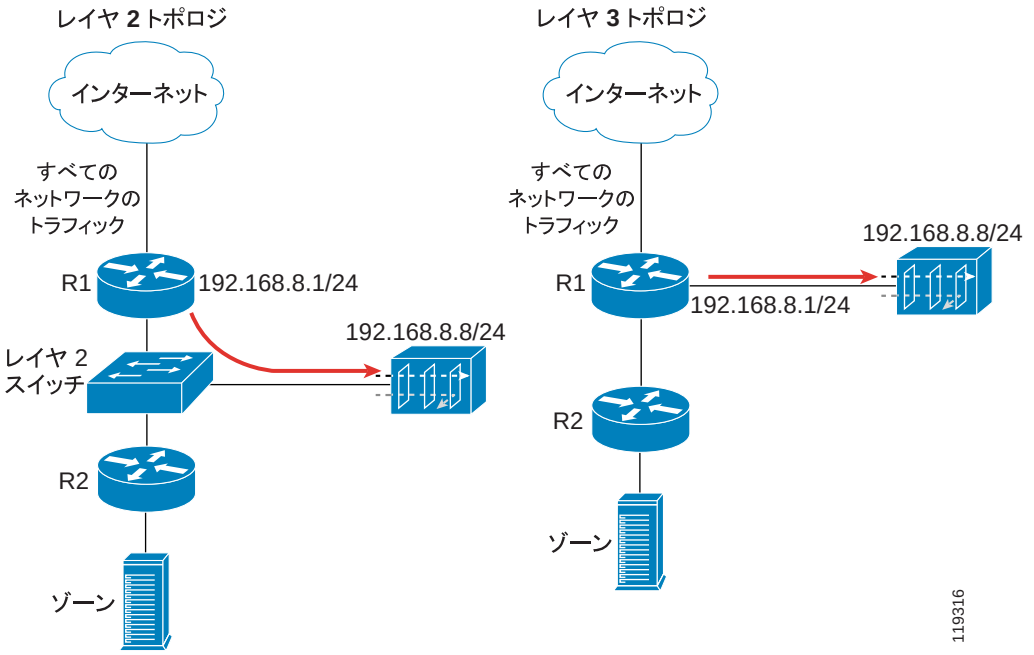
ルータは、標準の Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）ルーティング定義に従って、プレフィックスが最も長く一致する（「最も限定的」とも言われる）ルーティング パスを選択します。Guard は、ルータとの BGP セッションの確立後、Guard を保護対象ゾーンへの最良のパスとしてリストするルーティング アップデートを送信します。Guard が通知するネットワーク プレフィックスは、ルータのルーティング テーブルにすでにリストされているプレフィックスよりも長いため、ルータのルーティング テーブル定義が上書きされます。プレフィックス サブネットは、ゾーンのサブネット IP アドレスごとに設定されます。BGP はすべてのネットワークで同様に設定されます。

レイヤ 2 およびレイヤ 3 のネットワーク トポロジでトラフィックの宛先変更を設定するには、次の手順を実行します。

1. BGP　　を使用してトラフィック宛先変更を設定します（詳細については、「Guard の BGP 設定」の項を参照してください）。
2. 適切なトラフィック転送方式を設定します（詳細については、「トラフィック転送方式について」の項を参照してください）。

図 4-1 に、レイヤ 2 およびレイヤ 3 のネットワーク トポロジの例を示します。どちらのネットワーク トポロジでも、Guard はルータ R1 からトラフィックを宛先変更します。

図 4-1　BGP 設定



BGP 宛先変更が確立されると、ルータのルーティング テーブルがゾーンへの最良のルートとして Guard を指し、ルータがゾーンの IP アドレス宛てのすべてのトラフィックを Guard に転送するようになります。

この項では、次のトピックについて取り上げます。

- BGP 設定のガイドライン
- Guard の BGP 設定
- Cisco ルータの BGP 設定

BGP 設定のガイドライン

この項では、Guard 上および宛先変更元ルータ上の BGP 設定に関する一般的なガイドラインを示します。

（注） この項で示すガイドラインは、Guard がトラフィックを宛先変更する元となる任意のルータ上の BGP 設定に適用されます。この項および後続の項の BGP 設定例では、シスコ構文を使用しています。

（注） 次の例では、一般的な External Border Gateway Protocol（eBGP; 外部ボーダー ゲートウェイ プロトコル）を使用しています。ネットワーク設定を考慮して、eBGP と Internal Border Gateway Protocol（iBGP; 内部ボーダー ゲートウェイ プロトコル）のどちらをネットワークで実装するかを決める必要があります。

Guard と隣接ルータが一般的な eBGP を使用して動作する場合は、次のガイドラインに従います。

1. Guard に、簡単に認識できる Autonomous System（AS; 自律システム）番号を設定します。

   Guard は、トラフィックを宛先変更する場合にだけルーティング情報を送信します。このルートは、ルータのルーティング テーブルに表示されます。認識できる値を使用すると、ルータのルーティング テーブル内で Guard を簡単に識別できます。

2. Guard のルーティング情報が内部および外部の他の BGP 隣接デバイスに再配布されないようにするには、次の手順を実行します。

   - ルーティング情報を送信せず、かつ着信 BGP ルーティング情報をドロップするように Guard を設定します。
   - Guard の BGP コミュニティ アトリビュート値を **no-export** および **no-advertise** に設定します。

   コミュニティ アトリビュートにおける一致により、Guard はルータ上の BGP 通知をフィルタリングして、このポリシーを適用することができます。

3. セットアップ手順中に、**soft-reconfiguration inbound** コマンドを入力します。このコマンドはトラブルシューティングに役立ちます。このコマンドを使用すると、隣接デバイスに再接続せずにルーティング テーブルを復元できます。

BGP の詳細については、P.A-9 の「BGP 宛先変更方式」を参照してください。

Guard の BGP 設定

Zebra アプリケーションを使用して、Guard に BGP を設定できます（Zebra アプリケーションの詳細については、http://www.zebra.org を参照してください）。

（注） ゾーンがスタンバイ モードであるときにゾーンの宛先変更を設定することをお勧めします。

Guard に宛先変更設定を入力するには、次の手順を実行します。

ステップ 1　設定コマンド グループ レベルから、次のコマンドを入力します。

```
admin@GUARD-conf# router
```

システムが非特権モードで Zebra アプリケーションに入ったことを示す次のプロンプトが表示されます。

```
router>
```

ヒント このモードで使用できるコマンドのリストを表示するには、Zebra アプリケーションの各コマンド レベルで疑問符（?）のキーを押してください。

ステップ 2　次のコマンドを入力して、特権モードに切り替えます。

```
router> enable
```

システムが特権モードで Zebra アプリケーションに入ったことを示す次のプロンプトが表示されます。

```
router#
```

（注）　Zebra アプリケーションを終了するには、ルータ コマンド レベルから **exit** コマンドを入力します。現在のコマンド グループ レベルを終了して上位のグループ レベルに移るには、**exit** コマンドを入力します。

ステップ 3　次のコマンドを入力して、端末設定モードに切り替えます。

```
router# config terminal
```

システムが Zebra アプリケーション設定モードに入ったことを示す次のプロンプトが表示されます。

```
router(config)#
```

ステップ 4　次のコマンドのとおりに、Guard にルーティングを設定します。これらのコマンドは、次の表記法を順守します。

- 太字の項目はコマンドを表します。
- 太字の斜体の項目は名前を表します。これらの名前は置き換え可能です。
- 山カッコで囲まれた斜体の項目（< >）は、指定しなければならない値を示しています。斜体の用語は、記載されているとおりの、Guard およびルータ（宛先変更元ルータ）の値に置き換えてください。山カッコは含めないでください。

（注）　ルータの発信ルーティング情報をフィルタリングするには、いくつかの方式を使用できます。次の例は、「distribute-list」方式を示しています。ルーティング情報が Guard に送信されない限り、他のタイプのフィルタリング方式を使用できます。

次のコマンドを Guard に入力する必要があります。

```
router(config)# router bgp <Guard-AS-number>
router(config-router)# bgp router-id <Guard-IP-address>
router(config-router)# redistribute guard
router(config-router)# neighbor <Router-IP-address> remote-as
<Router-AS-number>
router(config-router)# neighbor <Router-IP-address> description
<description>
router(config-router)# neighbor <Router-IP-address>
soft-reconfiguration inbound
router(config-router)# neighbor <Router-IP-address> distribute-list
nothing-in in
router(config-router)# neighbor <Router-IP-address> route-map
Guard-out out
router(config-router)# exit
router(config)# access-list nothing-in deny any
router(config)# route-map Guard-out permit 10
router(config-route-map)# set community no-export no-advertise
```

この項では、次のトピックについて取り上げます。

- Guard の BGP 設定例
- Guard のルータ設定ファイルの表示

Guard の BGP 設定例

Guard のルータの設定を表示するには、ルータのコマンド レベルから **show running-config** コマンドを入力します。次の例では、ルータの AS 番号が 100 で、Guard の AS 番号が 64555 です。

次のような出力（部分的な例）が表示されます。

```
router# show running-config
... ... ...
router bgp 64555
bgp router-id 192.168.8.8
redistribute guard
neighbor 192.168.8.1 remote-as 100
neighbor 192.168.8.1 description divert-from router
neighbor 192.168.8.1 soft-reconfiguration inbound
neighbor 192.168.8.1 distribute-list nothing-in in
neighbor 192.168.8.1 route-map Guard-out out
!
access-list nothing-in deny any
!
route-map Guard-out permit 10
set community 100:64555 no-export no-advertise
... ... ...
```

Guard のルータ設定ファイルの表示

Guard から、ルータの設定ファイルを表示できます。

ルータの設定ファイルを表示するには、グローバル コマンド グループ レベルから次のコマンドを入力します。

```
show running-config router
```

Cisco ルータの BGP 設定

この項では、宛先変更を設定する場合に使用する、ルータの BGP 設定について説明します。このコマンドの構文は、Cisco ルータ上の BGP 設定から取得されるものです。

これらのコマンドは、次の表記法を順守します。

- 太字の項目はコマンドを表します。
- 太字の斜体の項目は名前を表します。これらの名前は置き換え可能です。
- 山カッコで囲まれた斜体の項目（< >）は、指定しなければならない値を示しています。斜体の用語は、記載されているとおりの、Guard およびルータ（宛先変更元ルータ）の値に置き換えてください。山カッコは含めないでください。

```
R7200(config)# router bgp <Router-AS>
R7200(config-router)# bgp log-neighbor-changes
R7200(config-router)# neighbor <Guard-IP-address> remote-as GuardAS
R7200(config-router)# neighbor <Guard-IP-address> description
<description>
R7200(config-router)# neighbor <Guard-IP-address> soft-reconfiguration
inbound
R7200(config-router)# neighbor <Guard-IP-address> distribute-list
routesToGuard out
R7200(config-router)# neighbor <Guard-IP-address> route-map Guard-in
in
R7200(config-router)# no synchronization
R7200(config-router)# exit
R7200(config)# ip bgp-community new-format
R7200(config)# ip community-list expanded <Guard-community-name>
permit no-export no-advertise
R7200(config)# route-map Guard-in permit 10
R7200(config-route-map)# match community <Guard-community-name> exact
match
R7200(config-route-map)# exit
R7200(config)# ip access-list standard routestoGuard
R7200(config-std-nacl)# deny any
```

no synchronization コマンドにより、Guard の BGP ルーティング アップデートが IGP に配布されなくなります。

Cisco ルータの BGP 設定例

ルータの設定を表示するには、ルータのグローバル コマンド レベルから **show running-config** コマンドを入力します。次の例では、ルータの AS 番号が 100 で、Guard の AS 番号が 64555 です。

次のような出力（部分的な例）が表示されます。

```
R7200# show running-config
... ... ...
router bgp 100
bgp log-neighbor-changes
neighbor 192.168.8.8 remote-as 64555
neighbor 192.168.8.8 description Guard
neighbor 192.168.8.8 soft-reconfiguration inbound
neighbor 192.168.8.8 distribute-list routesToGuard out
neighbor 192.168.8.8 route-map Guard-in in
no synchronization
!
ip bgp-community new-format
ip community-list expanded Guard permit 100:64555 no-export no-
advertise
!
route-map Guard-in permit 10
match community Guard exact match
ip access-list standard routesToGuard
 deny any
... ... ...
```

トラフィック転送方式について

この項では、トラフィック転送方式について詳しく説明します。トラフィック転送方式は、クリーンなトラフィックを Guard からネクストホップ ルータに転送するために使用されます。詳細については、P.A-10 の「トラフィック転送方式について」を参照してください。

この項では、次のトピックについて取り上げます。

- Layer 2 Forwarding 方式
- Policy-Based Routing Destination 転送方式
- VPN Routing Forwarding Destination 転送方式
- Policy-Based Routing VLAN 転送方式
- VPN Routing Forwarding VLAN 転送方式
- トンネル宛先変更の転送方式

Layer 2 Forwarding 方式

レイヤ 2 トポロジでは Layer 2 Forwarding（L2F）方式が使用されます。この場合、3 つすべてのデバイス（Cisco Guard、宛先変更元ルータ、およびネクストホップ ルータ）が 1 つの共有 IP ネットワーク内に置かれます（図 4-2）。

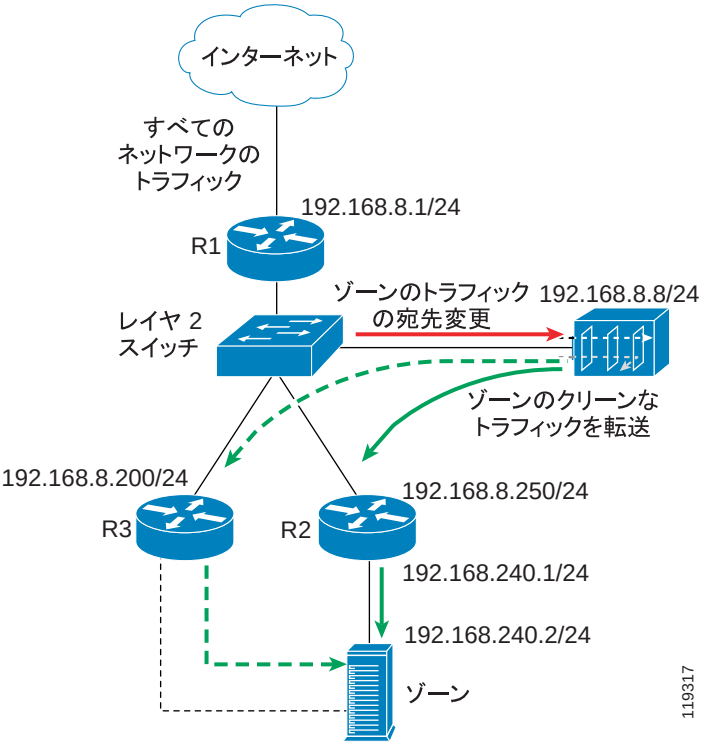
レイヤ 2 トポロジでは、宛先変更元ルータおよび注入先のルータが 2 つの別個のデバイスです。ネクストホップ ルータと注入先のルータは同じデバイスです。

Guard は、注入先 / ネクストホップ ルータの MAC アドレスを解決するために ARP クエリーを発行して、トラフィックを転送します。そのため、L2F 方式を使用する場合は、ルータの上の設定は不要です。

ゾーンは、次の方法で接続されます。

- レイヤ 2 スイッチに直接接続。この場合、ゾーンを Guard と同じ IP サブネットに接続し、ゾーンの IP アドレスを注入先ルータとして設定します。Guard は、トラフィックをゾーンに直接転送します。
- IP 転送機器を使用。この場合、IP 転送機器を Guard のネクストホップ ルータとして定義する必要があります。

図 4-2　Layer 2 Forwarding 方式



この項では、次のトピックについて取り上げます。

- Guard の L2F 設定
- ルータの L2F 設定

Guard の L2F 設定

この項では、Guard の L2F 設定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。

- インターフェイスに関する文
- BGP に関する文
- 注入の設定

インターフェイスに関する文

「物理インターフェイスの設定」の項に示すとおりに、Guard のアウトオブバンドインターフェイスを設定できます。

次の例は、アウトオブバンドインターフェイス giga1 を設定する方法を示しています。

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

BGP に関する文

「Guard の BGP 設定」の項に示すとおりに、Guard のルータ BGP 設定を入力できます。

次の例では、Guard の AS が 64555、ルータの AS が 100 で IP アドレスが 192.168.8.1 です。

```
router bgp 64555
 redistribute guard
 neighbor 192.168.8.1 remote-as 100
 neighbor 192.168.8.1 description C7513
 neighbor 192.168.8.1 distribute-list nothing-in in
 neighbor 192.168.8.1 soft-reconfiguration inbound
 neighbor 192.168.8.1 route-map filt-out out
!
route-map filt-out permit 10
 set community no-advertise no-export 100:64555
!
access-list nothing-in deny any
```

注入の設定

ネットワーク トポロジに応じてゾーンまたはネクストホップ ルータへのスタティック ルートを追加して、Guard からゾーンへのトラフィック注入を設定できます。このスタティック ルートは、Guard のルータ設定レベルで設定する必要があります。

次の例では、ネクストホップ ルータ（192.168.8.250）経由でゾーンのネットワーク（192.168.240.0/24）へのスタティック ルートを設定する方法を示しています。

```
router# configure terminal
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.8.250
```

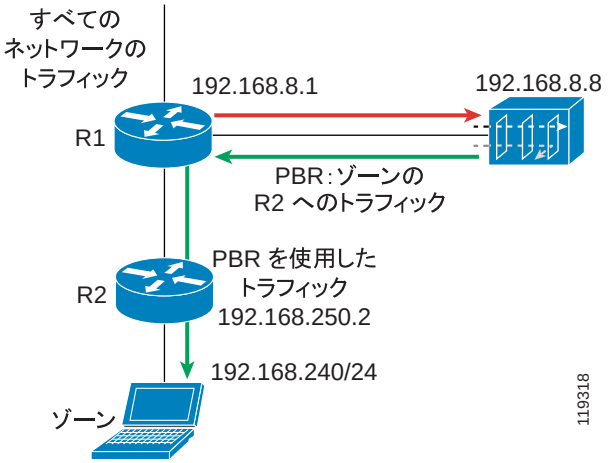
ルータの L2F 設定

ルータ上の設定は不要です。

Policy-Based Routing Destination 転送方式

Policy-Based Routing（PBR; ポリシーベース ルーティング）は、レイヤ 3 ネットワーク トポロジで展開されるスタティック転送方式です。この方式では、Guard が、フィルタ処理されたトラフィックをトラフィックの宛先変更元のルータに転送します（図 4-3）。

図 4-3　PBR 転送方式



Guard がゾーンのトラフィックをルータから宛先変更できるようにするために、ルータのルーティング テーブルでゾーンのルートが変更され、ゾーンへの最良のパスとして Guard がリストされます。

ルータのルーティング テーブルが変更されないと、無限ルーティング ループが発生する可能性があります。ルータのルーティング テーブル内でゾーン宛てのトラフィック用の唯一のエントリが Guard であるため、Guard からのフィルタ処理されたトラフィックが Guard に返送されます。

ルーティング ループが発生しないようにするために、注入先のルータにポリシーベース ルーティング（PBR）を設定できます。PBR では、ルータのルーティング テーブル内の規則を上書きして無限ルーティング ループを回避する規則を作成できます。PBR では、フィルタ処理されたトラフィックに適用される規則を追加できます。このような規則により、ルータは、ルーティング テーブルのエントリに関係なく、フィルタ処理されたトラフィックをゾーンに転送するよう指示されます。

このネットワーク トポロジで宛先変更を設定するために、BGP を使用するトラフィック宛先変更プロセスを設定できます（詳細については、「Guard の BGP 設定」の項を参照してください）。

この項では、次のトピックについて取り上げます。

PBR-DST 設定のガイドライン

この項で示すガイドラインは、任意の注入先ルータ上の PBR 設定に適用されます。

注入先のルータに PBR を設定するには、次のガイドラインに従います。

1. Guard に接続しているルータ インターフェイスに、PBR を適用する必要があります。

（注）　Guard からのトラフィックにのみ、PBR を適用できます。

2. PBR によって選択されたトラフィックを、ネクストホップ ルータに転送する必要があります。ネクストホップ ルータは、次の特性を持つ必要があります。
   - ネクストホップ ルータは、宛先変更元ルータに直接接続されている。レイヤ 3 トポロジでは、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。
   - 宛先変更元ルータは、ネクストホップ ルータの、ゾーンへのルートに含まれない（宛先変更元ルータがネクストホップ ルータのゾーンへのルートに含まれる設定では、宛先変更元ルータとネクストホップ ルータの間にルーティング ループが発生します）。

PBR は **route-map** コマンド、および **match** コマンドと **set** コマンドを使用して適用され、ポリシー ルーティング パケットの条件を定義します。PBR をイネーブルにするには、一致基準、および match 句のすべての基準が満たされた場合に実行されるアクションを指定するルート マップを作成する必要があります。ユーザは、特定のインターフェイス上の設定済みルート マップに対して PBR をイネーブルにする必要があります。指定したインターフェイスに到着するパケットで、match 句の基準を満たすものはすべて、PBR の対象となります。

PBR 設定は、次の 3 つの部分で構成されます。

- シーケンス : 新しいルート マップが、すでに同じ名前で設定されているルート マップのリスト内に置かれる位置を指定します。Cisco ルータは、シーケンス番号を昇順で処理します。

  ゾーンに転送される予定のトラフィックと、その他のトラフィックには、別のルート マップ エントリとシーケンス番号を定義できます。

  シーケンスは、**route-map** コマンドを使用して設定します。**route-map** コマンドを使用すると、ルータはルート マップ設定モードに入ります。
- 一致文 : ポリシー ルーティングが行われる条件を指定します。**match** コマンドを使用して、IP アドレスが一致する条件を指定する必要があります。一致するかどうかにより、ネクストホップが変更されるかどうかが決まります。
- 転送文 : **match** コマンドによって設定された基準が満たされた場合に実行されるルーティング アクションを指定します。**set ip next-hop route-map** 設定コマンドにより、ポリシー ルーティング用ルート マップの match 句の基準を満たすパケットをどこに送信するかが指定されます。

Guard の PBR-DST 設定

次の例の設定は、図 4-3 のネットワークを示しています。

BGP に関する文

「Guard の BGP 設定」の項に示すとおりに、Guard のルータ BGP 設定を入力できます。

ネクストホップ ルータへ注入設定

この例のネクストホップ ルータは R2 です（図 4-3 を参照してください）。Guard からゾーンへのトラフィック注入を設定するには、注入先のルータへのスタティック ルートを追加します。

このスタティック ルートは、Guard のルータ設定レベルで設定する必要があります。

次の例では、ゾーンのネットワーク（192.168.240.0/24）へのスタティック ルートを設定する方法を示しています。

```
router# configure terminal
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.8.1
```

Cisco ルータの PBR-DST 設定例

次の例は、宛先変更を設定する場合に使用する、ルータの PBR 設定を示しています。

```
R7200(config)# interface FastEthernet 0/2
R7200(config-if)# description <Interface connected to the Guard>
R7200(config-if)# ip address <Router interface IP address> <Router
interface IP mask>
R7200(config-if)# no ip directed-broadcast
R7200(config-if)# ip policy route-map <Guard-PBR-name>
R7200(config-if)# exit
R7200(config)# ip access-list extended <Zone-name>
R7200(config-ext-nacl)# permit ip any host <Zone IP address>
R7200(config-ext-nacl)# exit
R7200(config)# route-map <Guard-PBR-name> permit 10
R7200(config-route-map)# match ip address <Zone-name>
R7200(config-route-map)# set ip next-hop <next-hop router IP address>
R7200(config-route-map)# exit
R7200(config)# route-map < Guard-PBR-name > permit 100
R7200(config-route-map)# description let thru all other packets
without modifying next-hop
```

この例は、図 4-3 に示したサンプル ネットワークの PBR トラフィック転送設定について示しています。ルータ設定を表示するには、**show running-config** コマンドを入力します。

次のような画面（部分的な例）が表示されます。

```
R7200# show running-config
... ... ...
interface FastEthernet0/2
description Interface connected to the Guard
    ip address 192.168.8.1 255.255.255.0
    no ip directed-broadcast
    ip policy route-map GuardPbr
!
ip access-list extended zone-A
    permit ip any host 192.168.240.2
!
route-map GuardPbr permit 10
    match ip address zone-A
    set ip next-hop 192.168.250.2
!
route-map GuardPbr permit 100
description let thru all other packets without modifying next-hop
```

VPN Routing Forwarding Destination 転送方式

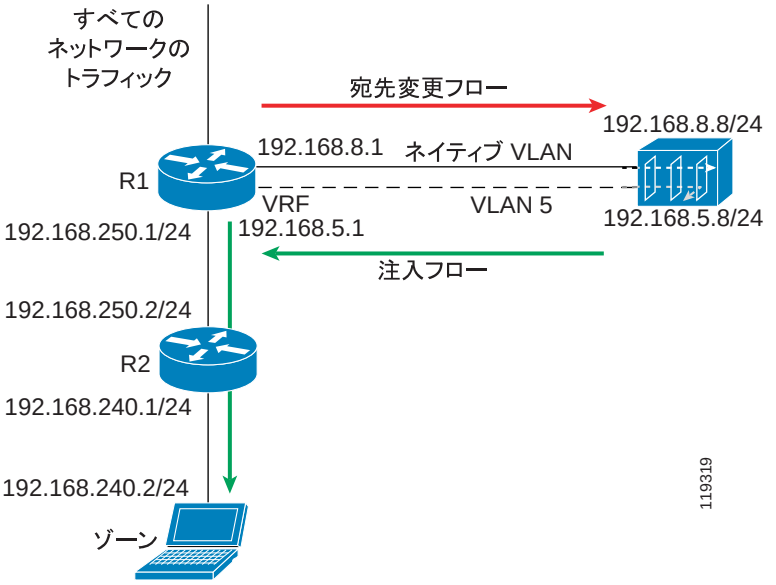
VPN Routing Forwarding Destination（VRF-DST）は、レイヤ 3 ネットワーク トポロジで展開されるスタティック転送方式です。この方式では、Guard が、フィルタ処理されたトラフィックをトラフィックの宛先変更元のルータに転送します（図 4-4）。

Guard がゾーンのトラフィックをルータから宛先変更できるようにするために、ルータのルーティング テーブルでゾーンのルートが変更され、ゾーンへの最良のパスとして Guard がリストされます。

ルータのルーティング テーブルが変更されないと、無限ルーティング ループが発生する可能性があります。ルータのルーティング テーブル内でゾーン宛てのトラフィック用の唯一のエントリが Guard であるため、Guard からのフィルタ処理されたトラフィックが Guard に返送されます。

VRF-DST では、メインのルーティング / 転送テーブルのほかに、もう 1 つルーティング / 転送テーブル（VRF テーブルと呼ばれる）を作成できます。追加のルーティング テーブルは、Guard 用のルータ インターフェイスによって処理されるトラフィックをルーティングするように設定されます。

図 4-4　VRF DST 転送方式



この項では、次のトピックについて取り上げます。

- VRF-DST 設定のガイドライン
- Guard の VRF-DST 設定

VRF-DST 設定のガイドライン

注入先のルータに VRF-DST を設定するには、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。

- ネイティブ VLAN インターフェイス : このインターフェイスは、トラフィックをルータから 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。Guard は、BGP 通知を送信して、このインターフェイス上のトラフィックを Guard に宛先変更します。

- もう 1 つの VLAN インターフェイス：このインターフェイスは、Guard から戻ってきたトラフィックをルータに宛先変更するために使用されます。このインターフェイスには VRF テーブルが設定されます。VRF 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スタティック ルートが含まれています。

（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使用してください。

Guard の VRF-DST 設定

この項では、Guard の VRF-DST 設定について説明します。次の例の設定は、図 4-4 のネットワークを示しています。

ネイティブ インターフェイスに関する文

次の例は、インバンド インターフェイスを設定する方法を示しています。

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

インターフェイス VLAN に関する文

次の例は、インバンド インターフェイスで VLAN 5 を設定する方法を示しています。

```
admin@GUARD-conf# interface giga1.5
admin@GUARD-conf-if-giga1.5# ip address 192.168.5.8 255.255.255.0
```

BGP に関する文

「Guard の BGP 設定」の項に示すとおりに、Guard のルータ BGP 設定を入力できます。

注入の設定

この例のネクストホップ ルータは R2 です（図 4-3 を参照してください）。Guard からゾーンへのトラフィック注入を設定するには、ネクストホップ ルータへのスタティック ルートを追加します。

このスタティック ルートは、Guard のルータ設定レベルで設定する必要があります。

次の例では、R1（192.168.5.1）上の VLAN インターフェイス経由でゾーンのネットワーク（192.168.240.0/24）へのスタティック ルートを設定する方法を示しています。

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.5.1
```

（注）　VRF は、Cisco IOS リリース 12.0(17) S/ST からサポートされています。

VRF テーブルの作成

次の例は、注入先のルータに VRF テーブルを作成する方法を示しています。

```
ip vrf Guard-vrf
 rd 100:1
 route-target export 100:1
 route-target import 100:1
```

インターフェイス ネイティブ VLAN に関する文

次の例は、宛先変更元ルータにネイティブ VLAN を設定する方法を示しています。

```
interface fastEthernet1/0.1
 encapsulation dot1Q 1 native
 description << VLAN TO GUARD-DIVERSION >>
 ip address 192.168.8.1 255.255.255.0
 no ip directed-broadcast
```

インターフェイス VLAN 5 に関する文

次の例は、注入先のルータに VLAN 5 インターフェイスを設定する方法を示しています。

```
interface fastEthernet 1/0.5
 encapsulation dot1Q 5
 description << VLAN TO GUARD-INJECTION >>
 ip vrf forwarding Guard-vrf
 ip address 192.168.5.1 255.255.255.0
```

ゾーンへのインターフェイスに関する文

次の例は、ゾーンにルータ インターフェイスを設定する方法を示しています。

```
interface fastEthernet 2/0
 description << LINK TO ZONE >>
 ip address 192.168.250.1 255.255.255.0
```

BGP に関する文

「Cisco ルータの BGP 設定」の項に示すとおりに、ルータ R1 の BGP 設定を入力できます。

スタティック VRF-DST に関する文

次の例は、注入先のルータにスタティック VRF を設定する方法を示しています。スタティック VRF は、ゾーンへのルートを指定します。パラメータ **global** は、ネクストホップへのルートがグローバル ルーティング テーブルからラーニングされることを示します。

```
R7200(config)# ip route vrf Guard-vrf 192.168.240.2 255.255.255.0
192.168.250.2 global
```

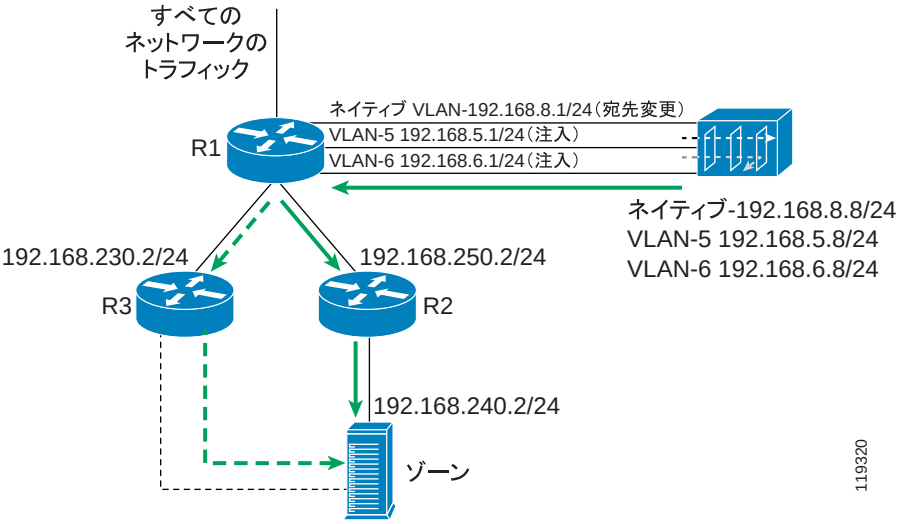
Policy-Based Routing VLAN 転送方式

ネクストホップになる可能性のあるルータが複数存在する場合に、Policy-Based Routing VLAN（PBR-VLAN）方式を使用できます（図 4-5）。Guard とルータ R1（宛先変更元かつ注入先のルータ）の間に複数の VLAN（Virtual LAN、802.1Q）トランクを設定します。トランクの各 VLAN は、異なるネクストホップ ルータに関連付けられます。さらに、各 VLAN 論理インターフェイスに PBR を設定し、VLAN 上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。

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。そのため、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。

トラフィックの宛先変更にはネイティブ VLAN が使用されます。このインターフェイスで、Guard は BGP 通知をルータに送信します。

図 4-5　PBR-VLAN 転送方式



この項では、次のトピックについて取り上げます。

- Guard の PBR-VLAN 設定
- Cisco ルータの PBR-VLAN 設定

Guard の PBR-VLAN 設定

この項では、Guard の PBR-VLAN 設定について説明します。次の例は、図 4-5 のネットワークを示しています。

R1 の Guard 用インターフェイスに PBR-VLAN が適用されます。VLAN-5 上のゾーン トラフィックは R2 に転送されます。VLAN-6 上のゾーン トラフィックは R3 に転送されます。

ネイティブ インターフェイスに関する文

次の例は、インバンド インターフェイスを設定する方法を示しています。

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

インターフェイス VLAN -5 に関する文

次の例は、インバンド インターフェイスに VLAN-5 を設定する方法を示しています。

```
admin@GUARD-conf# interface giga1.5
admin@GUARD-conf-if-giga1.5# ip address 192.168.5.8 255.255.255.0
```

インターフェイス VLAN -6 に関する文

次の例は、インバンド インターフェイスに VLAN-6 を設定する方法を示しています。

```
admin@GUARD-conf# interface giga1.6
admin@GUARD-conf-if-giga1.5# ip address 192.168.6.8 255.255.255.0
```

BGP に関する文

「Guard の BGP 設定」の項に示すとおりに、Guard のルータ BGP 設定を入力できます。

R2 への注入設定

Guard からゾーンへのトラフィック注入を設定するには、ネクストホップ ルータ R2 へのスタティック ルートを追加します。

このスタティック ルートは、Guard のルータ設定レベルで設定する必要があります。

次の例では、R1（192.168.5.1）上の VLAN インターフェイス経由でゾーンのネットワーク（192.168.240.0/24）へのスタティック ルートを設定する方法を示しています。

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.5.1
```

R3 への注入設定

ネクストホップ ルータ R3 へのスタティック ルートを追加して、Guard からゾーンへのトラフィック注入を設定できます。

このスタティック ルートは、Guard のルータ設定レベルで設定する必要があります。

次の例では、R1（192.168.6.1）上の VLAN インターフェイス経由でゾーンのネットワーク（192.168.240.0/24）へのスタティック ルートを設定する方法を示しています。

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.6.1
```

Cisco ルータの PBR-VLAN 設定

この項では、Cisco ルータの PBR-VLAN 設定について説明します。

インターフェイス ネイティブ VLAN に関する文

次の例は、トラフィックの宛先変更にネイティブ VLAN を設定する方法を示しています。

```
interface fastEthernet 1/0
 description << NATIVE VLAN TO GUARD-DIVERSION >>
 ip address 192.168.8.1 255.255.255.0
 no ip directed-broadcast
```

VLAN-5 の作成

次の例は、ルータ R1 に VLAN-5 を作成する方法を示しています。

```
interface fastEthernet 1/0.1
 encapsulation dot1Q 5
 description << VLAN-5 TO GUARD-INJECTION >>
 ip address 192.168.5.1 255.255.255.0
 ip policy route-map next-hop_R2
 no ip directed-broadcast
```

VLAN-6 の作成

次の例は、ルータ R1 に VLAN-6 を作成する方法を示しています。

```
interface fastEthernet 1/0.2
 encapsulation dot1Q 6
 description << VLAN-6 TO GUARD-INJECTION >>
 ip address 192.168.6.1 255.255.255.0
 ip policy route-map next-hop_R3
 no ip directed-broadcast
```

ネクストホップ インターフェイスの設定

次の例は、ネクストホップ ルータへのインターフェイスを設定する方法を示しています。

```
interface fastEthernet 2/0
 ip address 192.168.250.1 255.255.255.0
 Description << LINK TO NEXT-HOP R2 >>
 exit
interface fastEthernet 3/0
 ip address 192.168.230.1 255.255.255.0
 description << LINK TO NEXT-HOP R3 >>
```

BGP に関する文

「Cisco ルータの BGP 設定」の項に示すとおりに、ルータ R1 の BGP 設定を入力できます。

ルート マップに関する文（PBR）

次の例は、ネクストホップ ルータへの PBR を設定する方法を示しています。

```
route-map next-hop_R2 permit 10
 set ip next-hop 192.168.250.2

route-map next-hop_R3 permit 10
 set ip next-hop 192.168.230.2
```

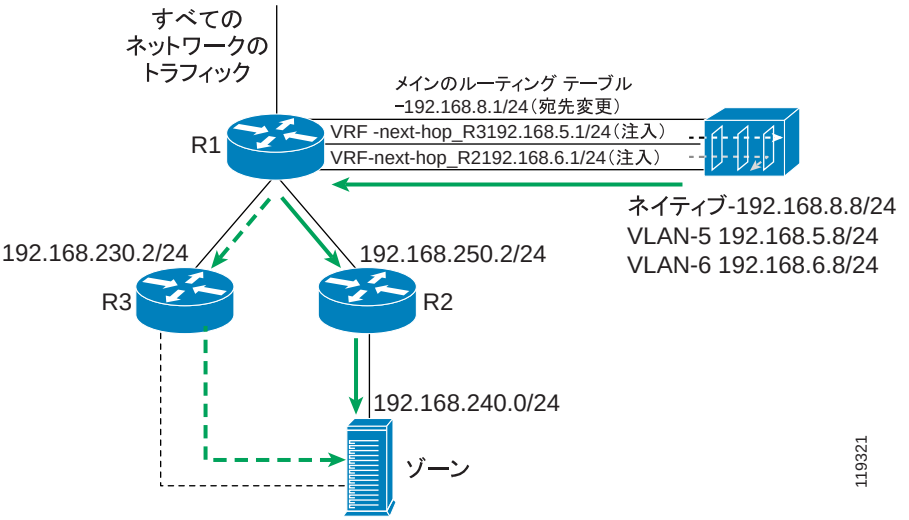
VPN Routing Forwarding VLAN 転送方式

VPN Routing Forwarding VLAN（VRF-VLAN）方式は、PBR-VLAN 方式に似ています。PBR テーブルではなく VRF テーブルが、注入先のルータ上の各 VLAN に関連付けられます。各 VRF テーブルは、VLAN 上のトラフィックを、対応するネクストホップ ルータに誘導します（図 4-6）。

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。そのため、Guard は、パケットが転送される VLAN を変更することにより、ゾーンへのネクストホップ ルータを変更できます。

トラフィックの宛先変更にはネイティブ VLAN が使用されます。このインターフェイスで、Guard は BGP 通知をルータに送信します。

図 4-6　VRF-VLAN 転送方式



この項では、次のトピックについて取り上げます。

- Guard の VRF-VLAN 設定
- Cisco ルータの VRF-VLAN 設定

Guard の VRF-VLAN 設定

この項では、Guard の VRF-VLAN 設定について説明します。次の例は、図 4-6 のネットワークを示しています。

R1 の Guard 用インターフェイスに VRF-VLAN が適用されます。VLAN-5 上のゾーン トラフィックは R2 に転送されます。VLAN-6 上のゾーン トラフィックは R3 に転送されます。

ネイティブ インターフェイスに関する文

次の例は、インバンド インターフェイスを設定する方法を示しています。

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

インターフェイス VLAN -5 に関する文

次の例は、インバンド インターフェイスに VLAN-5 を設定する方法を示しています。

```
admin@GUARD-conf# interface giga1.5
admin@GUARD-conf-if-giga1.5# ip address 192.168.5.8 255.255.255.0
```

インターフェイス VLAN -6 に関する文

次の例は、インバンド インターフェイスに VLAN-6 を設定する方法を示しています。

```
admin@GUARD-conf# interface giga1.6
admin@GUARD-conf-if-giga1.5# ip address 192.168.6.8 255.255.255.0
```

BGP に関する文

「Guard の BGP 設定」の項に示すとおりに、Guard のルータ BGP 設定を入力できます。

隣接 IP アドレスを 192.168.8.1 に設定します。

R2 への注入設定

ネクストホップ ルータ R2 へのスタティック ルートを追加して、Guard からゾーンへのトラフィック注入を設定できます。

このスタティック ルートは、Guard のルータ設定レベルで設定する必要があります。

次の例では、R1（192.168.5.1）上の VLAN インターフェイス経由でゾーンのネットワーク（192.168.240.0/24）へのスタティック ルートを設定する方法を示しています。

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.5.1
```

R3 への注入設定

ネクストホップ ルータ R3 へのスタティック ルートを追加して、Guard からゾーンへのトラフィック注入を設定できます。

このスタティック ルートは、Guard のルータ設定レベルで設定する必要があります。

次の例では、R1（192.168.6.1）上の VLAN インターフェイス経由でゾーンのネットワーク（192.168.240.0/24）へのスタティック ルートを設定する方法を示しています。

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.6.1
```

Cisco ルータの VRF-VLAN 設定

この項では、Cisco ルータの VRF-VLAN 設定について説明します。

最初の VRF テーブルの作成

次の例は、ルータ R2 に関連付けられた VRF テーブルを作成する方法を示しています。

```
ip vrf next-hop_R2
 rd 100:1
 route-target export 100:1
 route-target import 100:1
Second VRF Table Production
Create the VRF table associated with router R3:
ip vrf next-hop_R3
 rd 100:1
 route-target export 100:1
 route-target import 100:1
```

ネイティブ VLAN の作成

次の例は、ルータ R1 にネイティブ VLAN を設定する方法を示しています。

```
interface fastEthernet 1/0
 description <<NATIVE VLAN TO GUARD-DIVERSION>>
 ip address 192.168.8.1 255.255.255.0
 no ip directed-broadcast
```

VLAN-5 の作成

次の例は、ルータ R1 に VLAN-5 を作成する方法を示しています。

```
interface fastEthernet 1/0.1
 encapsulation dot1Q 5
 description << VLAN-5 TO GUARD-INJECTION >>
 ip address 192.168.5.1 255.255.255.0
 ip vrf forwarding next-hop_R2
 no ip directed-broadcast
```

VLAN-6 の作成

次の例は、ルータ R1 に、別の VRF 関連付けを持つ VLAN-6 を作成する方法を示しています。

```
interface fastEthernet 1/0.2
 encapsulation dot1Q 6
 description << VLAN-6 TO GUARD-INJECTION >>
 ip address 192.168.6.1 255.255.255.0
 ip vrf forwarding next-hop_R3
 no ip directed-broadcast
```

ネクストホップ インターフェイス

次の例は、ネクストホップ ルータへのインターフェイスを設定する方法を示しています。

```
interface fastEthernet 2/0
 ip address 192.168.250.1 255.255.255.0
 Description << LINK TO NEXT-HOP R2 >>
!
interface fastEthernet 3/0
 ip address 192.168.230.1 255.255.255.0
 description << LINK TO NEXT-HOP R3 >>
```

BGP に関する文

「Cisco ルータの BGP 設定」の項に示すとおりに、ルータ R1 の BGP 設定を入力できます。

スタティック VRF ルート

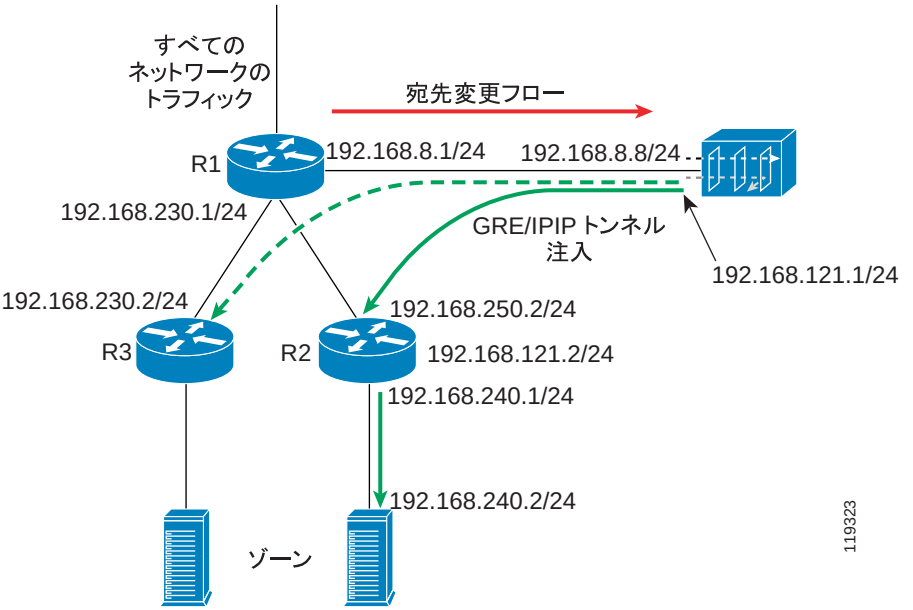
次の例は、注入先のルータにスタティック VRF を設定する方法を示しています。スタティック VRF は、ゾーンへのルートを指定します。パラメータ global は、ネクストホップへのルートがグローバル ルーティング テーブルからラーニングされることを示します。

```
R7200(config)# ip route vrf next-hop_R3 192.168.240.2 255.255.255.255
192.168.230.2 global
R7200(config)# ip route vrf next-hop_R2 192.168.240.2 255.255.255.255
192.168.250.2 global
```

トンネル宛先変更の転送方式

トンネル宛先変更方式では、Guard と各ネクストホップ ルータの間にトンネル（GRE または IPIP）が作成されます（図 4-7）。Guard は、ゾーン宛てのトラフィックを、トンネルを介して適切なネクストホップ ルータに送信します。そのため、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、指定されているゾーンへのネクストホップ ルータを変更できます。Guard からゾーンへのクリーンなトラフィックがトンネルにカプセル化されるため、注入先のルータは、ゾーンのアドレスに関してではなく、トンネル インターフェイス エンド ポイントに関してルーティング決定を行います。

図 4-7　トンネル宛先変更の転送方式



この項では、次のトピックについて取り上げます。

- Guard のトンネル宛先変更の設定
- Cisco ルータのトンネル宛先変更の設定

Guard のトンネル宛先変更の設定

この項では、Guard のトンネル宛先変更の設定について説明します。次の例は、図 4-7 のネットワークを示しています。

ネイティブ インターフェイスに関する文

次の例は、インバンド インターフェイスを設定する方法を示しています。

```
admin@GUARD-conf# interface giga1
admin@GUARD-conf-if-giga1# ip address 192.168.8.8 255.255.255.0
```

トンネル インターフェイスに関する文

次の例は、Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）トンネルを設定する方法を示しています。

```
admin@GUARD-conf# interface gre1
admin@GUARD-conf-if-gre1# ip address 192.168.121.1 255.255.255.0
admin@GUARD-conf-if-gre1# tunnel source 192.168.8.8
admin@GUARD-conf-if-gre1# tunnel destination 192.168.250.2
```

次の例は、IP-in-IP（IPIP）トンネルを設定する方法を示しています。

```
admin@GUARD-conf# interface ipip1
admin@GUARD-conf-if-ipip1# ip address 192.168.121.1 255.255.255.0
admin@GUARD-conf-if-ipip1# tunnel source 192.168.8.8
admin@GUARD-conf-if-ipip1# tunnel destination 192.168.250.2
```

BGP に関する文

「Guard の BGP 設定」の項に示すとおりに、Guard のルータ BGP 設定を入力できます。

隣接 IP アドレスを 192.168.8.1 に設定します。

注入の設定

この例のネクストホップ ルータは R2 です。Guard からゾーンへのトラフィック注入を設定するには、ネクストホップ ルータへのスタティック ルートを追加します。

このスタティック ルートは、Guard のルータ設定レベルで設定する必要があります。

次の例では、R1（192.168.121.2）上のトンネル インターフェイス経由でゾーンのネットワーク（192.168.240.0/24）へのスタティック ルートを設定する方法を示しています。

```
router(config)# ip route 192.168.240.0 255.255.255.0 192.168.121.2
```

Cisco ルータのトンネル宛先変更の設定

トンネル転送では、トンネルの端にあるルータ（図 4-7 の R2）の設定が必要です。宛先変更プロセスでは、宛先変更元ルータ（図 4-7 の R1）の設定が必要です。

R1 の宛先変更設定：BGP に関する文

「Cisco ルータの BGP 設定」の項に示すとおりに、ルータ R1 の BGP 設定を入力できます。

R2 の転送設定：R2 上のトンネル インターフェイス

次の例は、ルータ R2 にトンネルを設定する方法を示しています。

```
interface tunnel 1
 description << GRE tunnel to Guard  >>
 ip address 192.168.121.2 255.255.255.252
 load-interval 30
 tunnel source 192.168.250.2
 tunnel destination 192.168.8.8
```

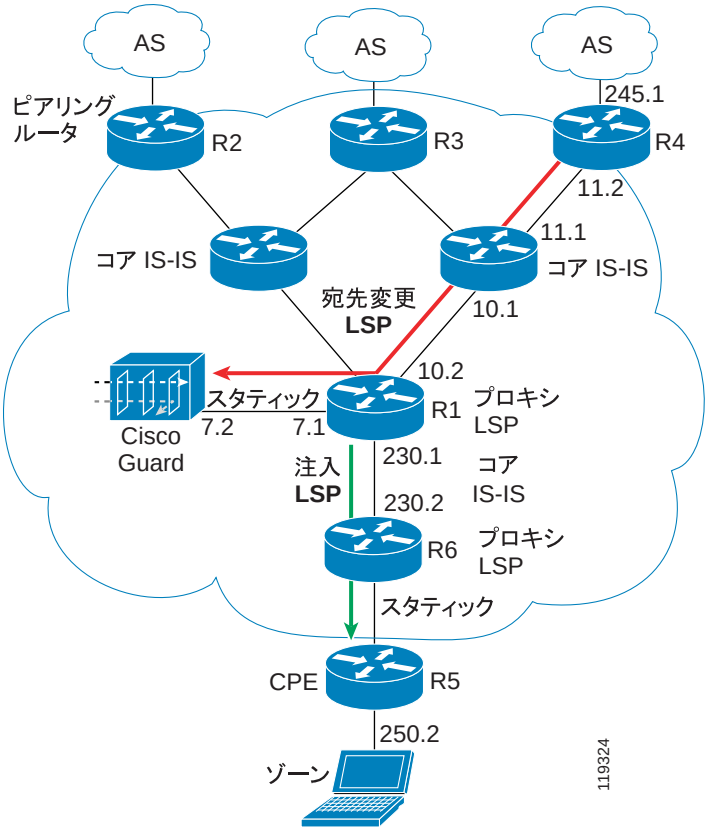
遠隔宛先変更方式

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。

図 4-8 には、次のネットワーク要素が含まれます。

- ピアリング ルータ（R4）
- Guard の隣接ルータ（R1）
- ゾーンのエッジ ルータ（R6）
- Cisco Guard

図 4-8　遠隔宛先変更の設定



この項では、次のトピックについて取り上げます。

- パケット フローの例
- 遠隔宛先変更の設定

パケット フローの例

（Label Switched Path（LSP; ラベル スイッチド パス）を保持するループバック アドレスに基づいて）トラフィックがゾーンの IP アドレスに流れます。

攻撃が識別されると、ネットワーク オペレータは Guard をアクティブにし、攻撃対象のゾーンを保護します。次の手順が自動的に実行されます。

1. Guard がピアリング ルータ（R2、R3、R4）にゾーンへの新しいルートを通知します。ネクストホップは Guard のループバック インターフェイスと定義されます。
2. ゾーンのトラフィックが、ピアリング ルータにより、宛先変更 LSP 経由でゾーンにルーティングされます。
3. Guard がクリーンなトラフィックを R1 に転送します。
4. R1 が IP ルックアップを実行し、適切な LSP 上のパケットをゾーンにルーティングします。

遠隔宛先変更の設定

次の例の設定は、図 4-8 のネットワークを示しています。

Guard の遠隔宛先変更の設定

この項では、Guard の遠隔宛先変更の設定について説明します。

Guard の CLI ループバック設定

次の例は、Guard にループバック インターフェイスを追加する方法を示しています。

```
admin@GUARD# configure
admin@GUARD-conf# interface lo:2
admin@GUARD-conf-if-lo:2# ip address 1.1.1.1 255.255.255.255
admin@GUARD-conf-if-lo:2# no shutdown
admin@GUARD-conf-if-lo:2# exit
For changes to take effect you need to reload the software.
Type 'yes' to reload now, or any other key to reload manually later
yes
reloading...
```

Zebra の CLI ループバック設定

次の例は、Zebra アプリケーションを使用して、ルータの設定にループバック インターフェイスを追加する方法を示しています。

（注）　Zebra アプリケーションの詳細については、http://www.zebra.org を参照してください。

```
router(config)# router bgp 100
router(config-router)# redistribute Guard
router(config-router)# bgp router-id 192.168.8.16
router(config-router)# neighbor 192.168.8.1 remote-as 100
router(config-router)# neighbor 192.168.8.1 description << iBGP
session to peering Router >>
router(config-router)# neighbor 192.168.8.1 soft-reconfiguration
inbound
router(config-router)# neighbor 192.168.8.1 route-map _new_next-hop
out
router(config-router)# exit
router(config)# route-map _new_next-hop permit 10
router(config-route-map)# set ip next-hop 1.1.1.1
router(config)# ip route 0.0.0.0 0.0.0.0 192.168.7.1
```

Cisco ルータの遠隔宛先変更の設定

この項では、Cisco ルータの遠隔宛先変更の設定について説明します。

ピアリング ルータの設定（R2、R3、および R4）

この項の設定例は、ピアリング ルータ R2、R3、および R4 に適用されます（図 4-8 を参照してください）。この項では、遠隔宛先変更の設定に関連するコマンドだけを示します。

次の例は、ピアリング ルータに Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）を設定する方法を示しています。

```
mpls ip
ip cef
```

次の例は、ループバック 0 インターフェイスを設定する方法を示しています。このインターフェイスは、Intermediate System-to-Intermediate System（IS-IS）経由の LSP を作成するために使用されます。

```
interface Loopback 0
 ip address 3.3.3.3 255.255.255.255
 no ip directed-broadcast
 load-interval 30
```

次の例は、ネットワーク接続インターフェイスを設定する方法を示しています。

```
interface fastEthernet 5/0
 ip address 192.168.11.2 255.255.255.0
 no ip directed-broadcast
 load-interval 30
 tag-switching ip (enable MPLS)
 no cdp enable
```

次の例は、IS-IS を設定する方法を示しています。

```
router isis
 redistribute static ip
 net 49.0001.0000.0000.0003.00
```

次の例は、Guard への iBGP を設定する方法を示しています。

```
router(config)# router bgp 100
R7200(config-router)# no synchronization
R7200(config-router)# bgp log-neighbor-changes
R7200(config-router)# neighbor 192.168.8.16 remote-as 100
R7200(config-router)# neighbor 192.168.8.16 description << iBGP to the
Guard >>
R7200(config-router)# neighbor 192.168.8.16 soft-reconfiguration
inbound
```

隣接ルータの設定（R1）

この項の設定例は、隣接ルータ R1 に適用されます（図 4-8 を参照してください）。この項では、遠隔宛先変更の設定に関連するコマンドだけを示します。

次の例は、ループバック 0 インターフェイスを設定する方法を示しています。このインターフェイスは、IS-IS 経由の LSP を作成するために使用されます。

```
interface Loopback 0
 ip address 2.2.2.2 255.255.255.255
 no ip directed-broadcast
```

次の例は、ネットワーク接続インターフェイスを設定する方法を示しています。

```
interface fastEthernet 5/0
 ip address 192.168.10.2 255.255.255.0
 no ip directed-broadcast
 load-interval 30
 tag-switching ip (enable MPLS)
 no cdp enable
```

次の例は、Guard へのインターフェイスを設定する方法を示しています。

（注）　このインターフェイスには、MPLS は設定されません。

```
interface FastEthernet1/0
 ip address 192.168.7.1 255.255.255.0
 no ip directed-broadcast
```

次の例は、Guard へのインターフェイスを設定する方法を示しています。

（注）　このインターフェイスには MPLS が設定されます。

```
interface fastEthernet 0/1/1
 ip address 192.168.230.1 255.255.255.0
 tag-switching ip (enable MPLS)
 no cdp enable
```

次の例は、IS-IS を設定する方法を示しています。

```
router isis
 redistribute static ip
 net 49.0001.0000.0000.0002.00
```

次の例は、Guard のループバック IP アドレスへの、出力プロキシ LSR 上のスタティック ルートを設定する方法を示しています（IP アドレス 1.1.1.1 は、Guard に設定されているループバック アドレスです）。

```
ip classless
ip route 1.1.1.1 255.255.255.255 192.168.7.2
```