トラフィックの宛先変更の設定

この章では、次のトピックについて取り上げます。

（注） このドキュメントに記載されている Cisco ルータおよび Juniper 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。

BGP 宛先変更方式

ルータは、標準の BGP 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。そのため、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。

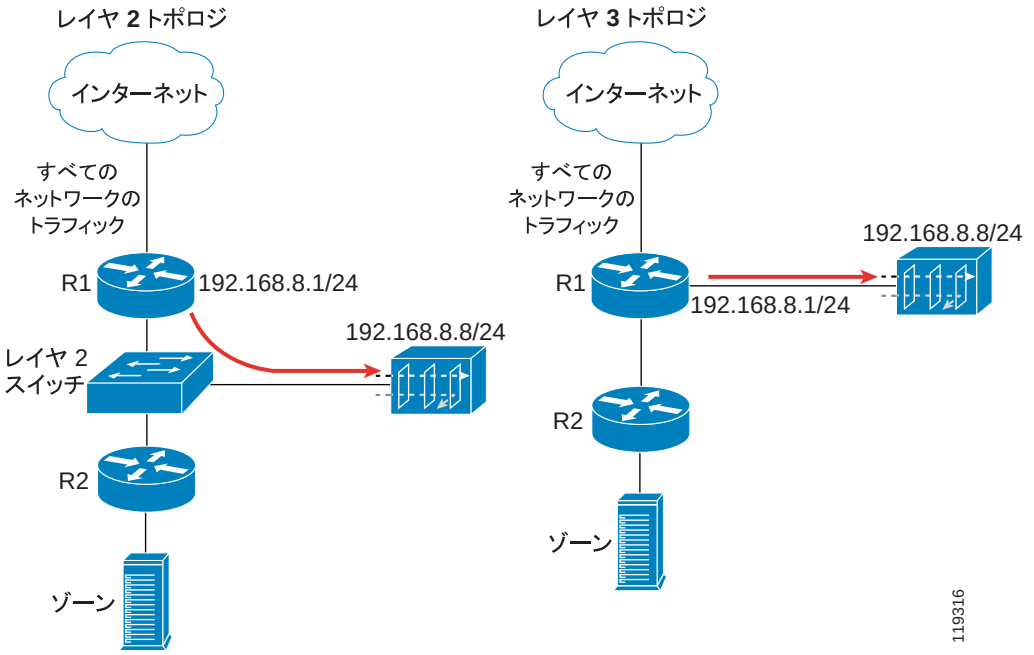
BGP はすべてのネットワークで同様に設定されます。

レイヤ 2 およびレイヤ 3 のネットワーク トポロジで Guard 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、この章の「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、この章の「トラフィック転送方式」の項を参照してください）。

図 4-1 に、L2 および L3 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 を指すようになります。そのため、ゾーンの IP アドレス宛てのすべてのトラフィックが Guard に転送されます。

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 設定に適用できます。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 eBGP を使用しています。

ユーザは、ネットワーク設定を考慮して、eBGP と iBGP のどちらを実装するかを決める必要があります。ユーザは、設定中にこれらの相違点に注意する必要があります。

Guard と隣接ルータは、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）を使用して動作します。推奨ガイドラインは、次のとおりです。

1. Guard に、簡単に認識できる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。その場合だけ、そのルートが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、ネットワーク オペレータが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、ルータ上の BGP 通知をフィルタリングできるため、このポリシーが適用されます。

3. セットアップ手順中に soft-reconfiguration inbound コマンドを発行することをお勧めします。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「トラフィック（BGP）宛先変更方式」を参照してください。

Guard の BGP 設定

BGP は、Zebra アプリケーションを使用して Guard に設定されます（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）。

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。

1. 設定コマンド グループ レベルから、次のように入力します。

```
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。

2. 次のように入力して、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** と入力します。
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** と入力します。

3. 次のように入力して、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)#
```

4. Guard のルーティングを設定します。詳細については、後述のガイドラインおよび例を参照してください。

   次のコマンドを Guard に設定する必要があります。

（注）
- 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。
- 記号 < > は、適切なパラメータ値に置き換えてください。
- 太字の斜体の項目は名前を表します。ユーザは、これらの名前を置き換えることができます。
- 次の各行はコマンドを表します。太字の項目はコマンドを表します。

（注）ルータ上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。

```
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
```

Guard の BGP 設定例

この例では、ルータの Autonomous System Number（AS; 自律システム番号）が 100 で、Guard の AS が 64555 です。

Guard のルータ設定を表示するには、次の手順を実行します。

ルータ コマンド レベルから、次のように入力します。

```
router# show running-config
```

次のような画面（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

ユーザは、所定のルータの設定ファイルを表示できます。

所定の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 レベルから次のように入力します。

```
show running-config router
```

Cisco ルータの BGP 設定

この項では、シスコの宛先変更技術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。次の構文は、Cisco ルータ上の BGP 設定から取得されるものです。

（注）
- 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。
- 記号 < > は、適切なパラメータ値に置き換えてください。
- 太字の斜体の項目は名前を表します。ユーザは、これらの名前を置き換えることができます。
- 次の各行はコマンドを表します。太字の項目はコマンドを表します。

```
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

この例では、ルータの Autonomous System Number（AS; 自律システム番号）が 100 で、Guard の AS が 64555 です。

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 レベルから次のコマンドを入力します。

```
R7200# show running-config
```

次のような画面（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
... ... ...
```

Juniper ルータの BGP 設定例

この例では、ルータの Autonomous System Number（AS; 自律システム番号）が 100 で、Guard の AS が 64555 です。

bgp コマンドにより、ローカル AS 番号、使用する BGP のタイプ（EBGP）、説明、リモート AS 番号、隣接 IP（Guard の AS 番号と IP アドレス）など、基本的な BGP パラメータが定義されます。

policy コマンドにより、特定のコミュニティ（次の例では「riverhead」）から受信した BGP アップデートだけが受け入れられ、その他のアップデートが拒否されるように定義されます。

```
   bgp {
       local-as 100;
            group test {
            type external;
            description "BGP with the Guard";
     passive;
            import bgp-in;
            peer-as 64555;
            neighbor 192.168.8.8;
        }
    }
}
policy-options {

    policy-statement bgp-in {
        term 10 {
            from {
                protocol bgp;
                community riverhead;
            }
            then accept;
        }
        term 20 {
            then reject;
        }
    }
    community riverhead members [ no-export no-advertise 100:64555 ];
```

トラフィック転送方式

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」を参照してください。

Layer-2-Forwarding（L2F）方式

L2 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。

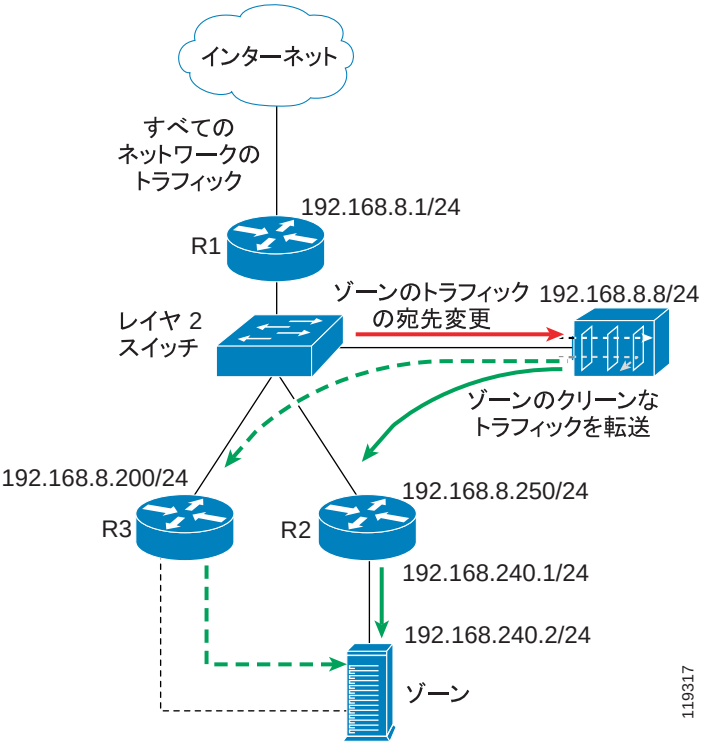
L2 トポロジでは、宛先変更元ルータおよび注入先のルータが 2 つの別個のデバイスです。ネクストホップ ルータと注入先のルータは同じデバイスです。

Guard は、注入先 / ネクストホップ ルータの MAC アドレスを解決して、トラフィックを転送します。MAC アドレスは、ARP クエリーを発行することによって解決されます。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、次のいずれかの方法で接続されます。

- ゾーンがレイヤ 2 スイッチに直接接続される。このような場合、ゾーンは Guard と同じ IP サブネットに接続されます。ゾーンの IP アドレスは注入先のルータとして設定され、Guard はトラフィックをゾーンに直接転送します。
- ゾーンが IP 転送機器を使用して接続される。このような場合、IP 転送機器が Guard のネクストホップ ルータとして定義される必要があります。

図 4-2　BGP 設定



Guard の L2F 設定

この項では、Guard の L2F 設定について詳しく説明します。

インターフェイスに関する文

Guard のアウトオブバンド インターフェイスを設定します（詳細については、「物理インターフェイスの設定」を参照してください）。

次の例では、アウトオブバンド インターフェイス giga1 が設定されています。

```
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

この章の「Guard の BGP 設定」の項の説明に従って、Guard のルータ BGP 設定を入力します。

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

Guard からゾーンへのトラフィック注入を設定するには、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 ルートが入力されています。

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

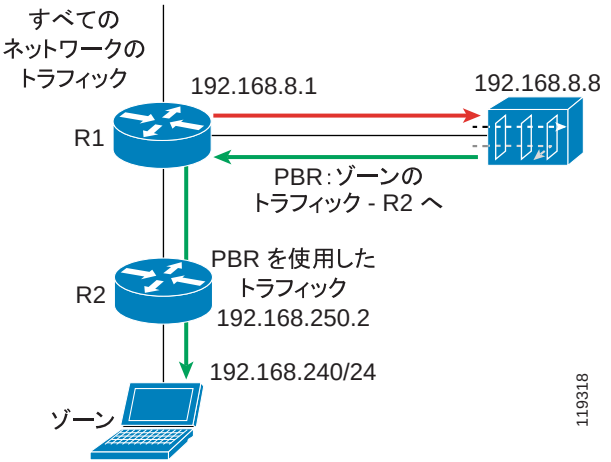
ルータの L2F 設定

ルータ上の設定は不要です。

Policy-Based Routing Destination（PBR-DST）トラフィック転送方式

Policy-Based Routing（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　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ます。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 Policy Based Routing（PBR; ポリシーベース ルーティング）が設定されます。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 ループのような状況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には、BGP を使用するトラフィック宛先変更プロセスを設定します（詳細については、この章の「Guard の BGP 設定」の項を参照してください）。

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 設定に適用できます。この項および後続の PBR 設定例では、シスコ構文を使用しています。

注入先のルータにポリシーベース ルーティングを設定するには、次のガイドラインに従います。

1. Guard に接続されているルータ インターフェイスでポリシーベース ルーティングが適用される必要があります。Guard からのトラフィックだけが PBR の対象となるため、これは重要です。
2. ポリシーベース ルーティングによって選択されたトラフィックは、ネクストホップ ルータに転送される必要があります。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。

このような設定により、宛先変更元ルータとネクストホップ ルータの間でルーティング ループが発生します。

ポリシーベース ルーティングは 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します。

  シーケンスは、route-map コマンドを使用して設定します。route-map コマンドにより、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。ユーザは、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 ルート マップ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

この章の「Guard の BGP 設定」の項の説明に従って、Guard のルータ BGP 設定を入力します。

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。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 ルートが入力されています。

```
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

この項では、シスコの宛先変更技術を設定する場合に使用する、ルータの PBR 設定について説明します。次の構文は、Cisco ルータ上の PBR 設定から取得されるものです。

```
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
```

PBR トラフィック転送の例

この項では、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の例を示します。

ルータの設定を表示するには、次の手順を実行します。

ルータのグローバル コマンド レベルから、次のように入力します。

```
R7200# show running-config
```

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
```

Juniper ルータの Filter Based Forwarding（FBF）の設定例

Juniper で PBR に相当するものは FBF（フィルタベース転送）です。

次の例の設定は、図 4-3 のネットワークを示しています。

この項では、Juniper ルータ上の Filter Based Forwarding（FBF）設定について説明します。

このルータ設定は、次の部分で構成されます。

- **フィルタの設定**：フィルタは、パケット フィルタリング基準を指定します。指定した宛先 IP アドレスを持つすべてのパケットと一致するようにフィルタを設定します。
- **ルーティング インスタンスの設定**：ルーティング インスタンスは、フィルタに一致するパケットの転送先のルーティング テーブル、およびフィルタに一致するパケットが転送される宛先を指定します。
- **インターフェイス ルートの設定**：インターフェイス ルートは、ルーティング インスタンスによって定義されているルートを、そのインターフェイスに直接接続されているネクストホップに解決する方法を指定します。

JUNOS のバージョン

DST-PBR は、5.1R1.4 JUNOS からサポートされています。

Guard へのインターフェイス

Guard 用のルータ インターフェイスを設定します。

```
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                filter {
                    input DST;
                }
                address 192.168.8.1/24;
            }
        }
    }
}
```

フィルタの設定

ファイアウォール フィルタでは、コンポーネントに基づいてパケットをフィルタリングできます。また、フィルタに一致するパケットに対してアクションを実行できます。フィルタの構成は、次のとおりです。

- **一致条件**：パケットに含まれる必要がある値またはフィールド。次の例で使用されている一致条件は、**destination-address** です。
- **アクション**：パケットが一致条件を満たした場合に実行されるアクションを指定します。次の例では、2 つのアクションがあります。最初のアクションでは、一致するパケットをルーティング インスタンス「next-hop_1」に割り当てます。2 番目のアクションでは、一致条件を満たさないすべてのパケットを受け入れます。

次の例では、フィルタ名が DST です。

```
firewall {
      filter DST {
        term 10 {
            from {
                destination-address {
                    192.168.240.2/32;
                }
            }
            then routing-instance next-hop_1;
        }
        term 20 {
            then accept;
        }
    }
```

ルーティング インスタンスの設定

各ルーティング インスタンスは、ルーティング テーブルのセット、そのルーティング テーブルに属するインターフェイスのセット、およびルーティング オプション設定のセットで構成されます。転送インスタンスは、Common Access Layer アプリケーションのフィルタベース転送の実装に使用されます。前の項で定義したフィルタごとに、ルーティング インスタンスを設定します。

次の例のルーティング インスタンス next-hop_1 は、一致するすべてのパケットをネクストホップ ルータ R2（192.168.250.2）に誘導します。

```
routing-instances {
    next-hop_1 {
        instance-type forwarding;
        routing-options {
            static {
                route 0.0.0.0/0 next-hop 192.168.250.2;
            }
        }
    }
}
```

インターフェイス ルートの設定

この例では、ネクストホップ ルータへのスタティック ルートが追加されています。**next-hop_1** ルーティング インスタンスを定義した後（上記の「ルーティング インスタンスの設定」の項を参照）、最後にルーティング インターフェイスを、接続されているインターフェイスに関連付ける必要があります。

ルーティング テーブル グループは、ルータのインターフェイスおよびルーティング テーブル グループのインターフェイス ルートに関連付けられます。これらは、**interface-routes** 文を使用して、指定の場所にインポートされます。

ルーティング テーブル グループは、**rib-groups** 文を使用して作成されます。

```
routing-options {
    interface-routes {
        rib-group inet dest;
        }
 rib-groups {
        dest {
            import-rib [ inet.0 next-hop_1.inet.0 ];
        }
 }
}
```

VPN Routing Forwarding - Destination（VRF-DST）

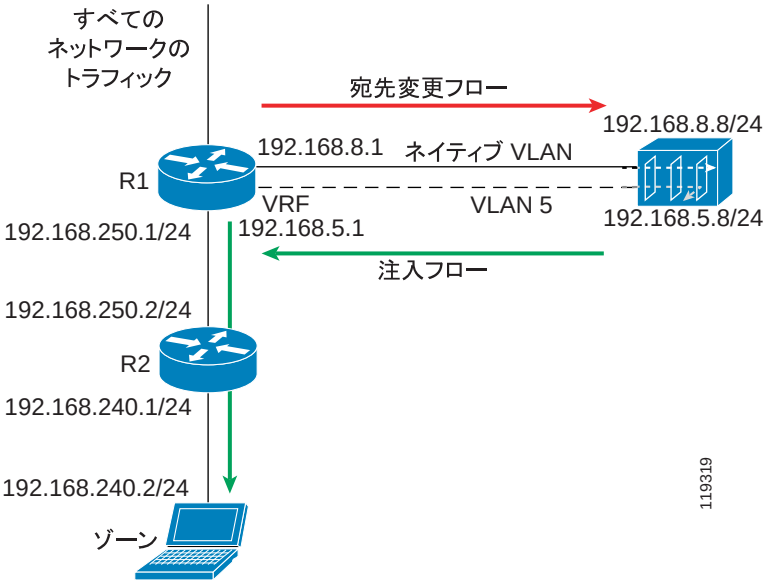
VRF-DST は、レイヤ 3 ネットワーク トポロジで展開されるスタティック転送方式です。この方式では、Guard が、フィルタ処理されたトラフィックをトラフィックの宛先変更元のルータに転送します。

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ます。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



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、次のガイドラインに従います。

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。

- **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） Juniper で VRF に相当するものは「ルーティング インスタンス」と呼ばれます。ルーティング インスタンスは、ルータ内の複数のルーティング / 転送テーブルをサポートします。また、この機能は、動的宛先変更を容易にします。そのため、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お勧めします。詳細については、この章の「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。

（注） VRF-DST 方式は、ネクストホップ ルータがゾーンごとにスタティックである場合にだけ適用できます。

VRF-DST 設定

次の例の設定は、図 4-4 のネットワークを示しています。

Guard の VRF-DST 設定

この項では、Guard の VRF-DST 設定について詳しく説明します。

ネイティブ インターフェイスに関する文

インバンド インターフェイスを設定します。

```
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

インバンド インターフェイスに VLAN 5 を設定します。

```
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

この章の「Guard の BGP 設定」の項の説明に従って、Guard のルータ BGP 設定を入力します。

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 192.1680.5.1 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 ルートが入力されています。

```
ip route 192.168.240.0 255.255.255.0 192.168.5.1
```

（注）　VRF は、IOS バージョン 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

注入先のルータに VRF テーブルを作成します。

```
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

宛先変更元ルータにネイティブ VLAN を設定します。

```
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

注入先のルータに VLAN 5 インターフェイスを設定します。

```
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

ゾーンへのルータ インターフェイスを設定します。

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

BGP に関する文

この章の「Cisco ルータの BGP 設定」の項の説明に従って、ルータ R1 の BGR 設定を入力します。

スタティック VRF-DST に関する文

注入先のルータにスタティック VRF を設定します。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。

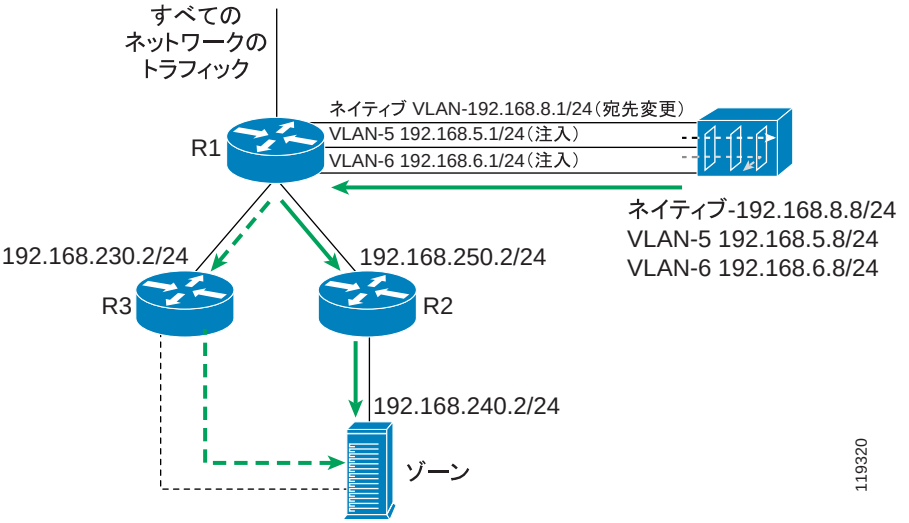
```
ip route vrf Guard-vrf 192.168.240.2 255.255.255.0 192.168.250.2
global
```

Policy Based Routing VLAN（PBR-VLAN）

この方式は、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使用されます。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）トランクが設定されます。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 が設定され、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



PBR-VLAN 設定

次の例の設定は、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。VLAN5 上のゾーン トラフィックは R2 に転送されます。VLAN6 上のゾーン トラフィックは R3 に転送されます。

Guard の PBR-VLAN 設定

この項では、Guard の PBR-VLAN 設定について詳しく説明します。

ネイティブ インターフェイスに関する文

インバンド インターフェイスを設定します。

```
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

インバンド インターフェイスに VLAN 5 を設定します。

```
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

インバンド インターフェイスに VLAN 6 を設定します。

```
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

この章の「Guard の BGP 設定」の項の説明に従って、Guard のルータ BGP 設定を入力します。

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 192.1680.5.1 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 ルートが入力されています。

```
ip route 192.168.240.0 255.255.255.0 192.168.5.1
```

R3 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 R3 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 192.168.6.1 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 ルートが入力されています。

```
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 設定について詳しく説明します。

インターフェイス ネイティブ VLAN に関する文

```
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

ルータ R1 に VLAN-5 を作成します。

```
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

ルータ R1 に VLAN-6 を作成します。

```
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

ネクストホップ ルータへのインターフェイスを設定します。

```
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

この章の「Cisco ルータの BGP 設定」の項の説明に従って、ルータ R1 の BGR 設定を入力します。

ルート マップに関する文（PBR）

ネクストホップ ルータへの PBR を設定します。

```
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
```

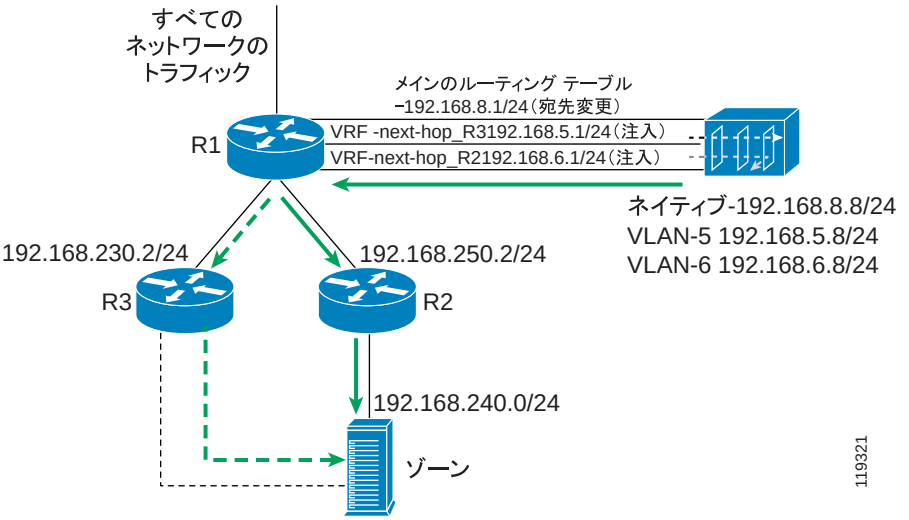
VPN Routing Forwarding VLAN（VRF-VLAN）

この方式は、PBR-VLAN 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。

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



VRF-VLAN 設定

次の例の設定は、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。VLAN5 上のトラフィックは R2 に転送されます。VLAN6 上のトラフィックは R3 に転送されます。

GUARD の VRF-VLAN 設定

この項では、Guard の VRF-VLAN 設定について詳しく説明します。

ネイティブ インターフェイスに関する文

インバンド インターフェイスを設定します。

```
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

インバンド インターフェイスに VLAN 5 を設定します。

```
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

インバンド インターフェイスに VLAN 6 を設定します。

```
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

この章の「Guard の BGP 設定」の項の説明に従って、Guard のルータ BGP 設定を入力します。

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

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 192.1680.5.1 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 ルートが入力されています。

```
ip route 192.168.240.0 255.255.255.0 192.168.5.1
```

R3 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 R3 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 192.168.6.1 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 ルートが入力されています。

```
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 設定について詳しく説明します。

最初の VRF テーブルの作成

ルータ R2 に関連付けられた VRF テーブルを作成します。

```
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

ルータ R1 にネイティブ VLAN を設定します。

```
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

ルータ R1 に VLAN-5 を作成します。

```
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

ルータ R1 に、別の VRF 関連付けを持つ VLAN-6 を作成します。

```
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

ネクストホップ ルータへのインターフェイスを設定します。

```
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

この章の「Cisco ルータの BGP 設定」の項の説明に従って、ルータ R1 の BGR 設定を入力します。

スタティック VRF ルート

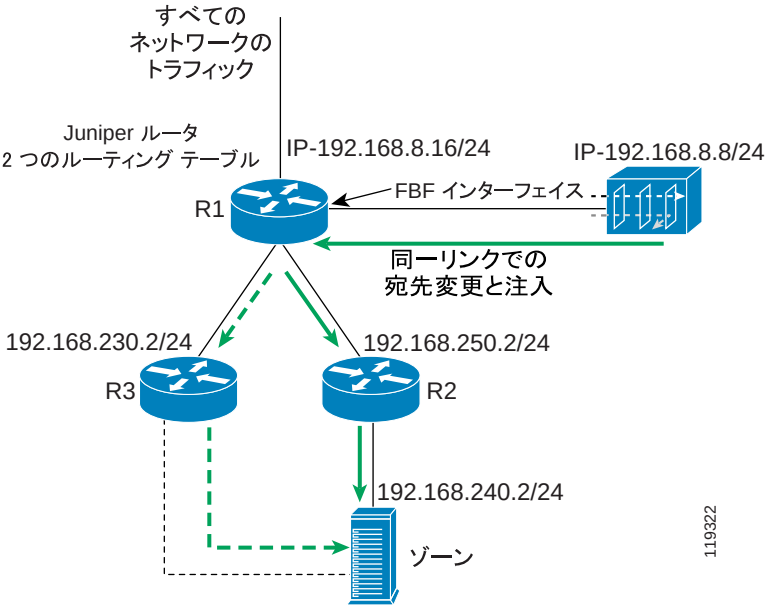
注入先のルータにスタティック VRF を設定します。スタティック VRF は、ゾーンへのルートを指定します。パラメータ global は、ネクストホップへのルートがグローバル ルーティング テーブルからラーニングされることを示します。

```
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
```

Juniper ルータのルーティング インスタンス

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ます。ルーティング インスタンスは、ルータ内の複数のルーティング / 転送テーブルをサポートします。また、この機能は、動的宛先変更を容易にします。そのため、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お勧めします。

図 4-7　Juniper ルータのルーティング インスタンス



Juniper ルータのルーティング インスタンスの設定

ルーティング インスタンスのルータ設定には、次の手順があります。

フィルタの設定：フィルタは、パケット フィルタリング基準を指定します。Guard 用のルータ インターフェイス上のフィルタを、すべてのパケットに一致し、それらのパケットを Guard-interface-routing-table に従ってルーティングするように設定します。

ルーティング インスタンスの設定（guard-interface-routing-table）：
Guard-interface-routing-table は、ゾーン トラフィックのルーティングを指定します。このテーブルは、グローバル ルーティング テーブル（Juniper では inet.0 と呼ばれる）から作成され、Guard によって送信された BGP 通知（Guard のコミュニティ ストリングによって識別される）を除外したものです。

フィルタの設定

フィルタを設定するには、次の手順を実行します。

1. Guard へのインターフェイスにフィルタを作成します。

   次の例のフィルタは、「guard-filter」という名前です。

2. インターフェイス上のすべてのトラフィックを　guard-interface-routing-table に従ってルーティングするようにフィルタを設定します。

Guard へのインターフェイス

Guard 用のルータ インターフェイスを設定します。

```
interfaces {
    ge-0/0/0 {
        unit 0 {
            family inet {
                filter {
                    input guard-filter;
                }
                address 192.168.8.16/24;
            }
        }
    }
}
```

ネクストホップへのインターフェイス

ネクストホップ ルータ R2 用のルータ インターフェイスを設定します。

```
interfaces {
   fe-0/0/0 {
      unit 0 {
        family inet {
          address 192.168.250.1/24:
```

ネクストホップへのインターフェイス

ネクストホップ ルータ R3 用のルータ インターフェイスを設定します。

```
interfaces {
   fe-0/0/1 {
      unit 0 {
        family inet {
          address 192.168.230.1/24:
```

フィルタの設定

ポート 179 宛てのパケットが受け入れられるようにフィルタを設定します。ゾーン宛ての残りのパケットは、Guard-interface-routing-table によって処理されます。

```
filter guard-filter {
  term 10 {
            from {
                destination-port 179;
            }
            then accept;
        }
        term 20 {
            then routing-instance guard-interface-routing-table;
    }
}
```

ルーティング インスタンスの設定（guard-interface-routing-table）

ルーティング インスタンス（guard-interface-routing-table）を設定するには、次の手順を実行します。

routing-instances セクションに Guard-interface-routing-table という名前のサブセクションを追加します。instance-import の routing-options 定義は、このルーティング テーブルにデータが入力される方法を定義します。定義されている auto-export 規則は、このルーティング インスタンスに no export アウトバウンド ポリシーが定義されていることを意味します。ルートのエクスポート元およびインポート先のルーティング テーブルは、既存のポリシー設定を調べることによって定義されます。

ポリシー セクション **without-guard-announcement** は、次のセクションで定義されます。

```
routing-instances {
    Guard-interface-routing-table
        instance-type forwarding;
        routing-options {
            instance-import without-guard-announcement;
            auto-export;
         }
}
```

BGP riverhead コミュニティを持つグローバル ルーティング テーブル ルートを除き、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るように、*without-guard-announcement* という名前のポリシー文を定義します。

instance master コマンドは、グローバル ルーティング テーブルを指定します。

```
policy-options {
    policy-statement without-guard-announcement {
        term 10 {
            from {
                instance master;
                protocol bgp;
                community riverhead;
            }
            then reject;
        }
        term 20 {
            then accept;
        }
    }
}
```

出力の例

次の例は、グローバル ルーティング テーブル inet.0 および guard-interface-routing-table を示しています。

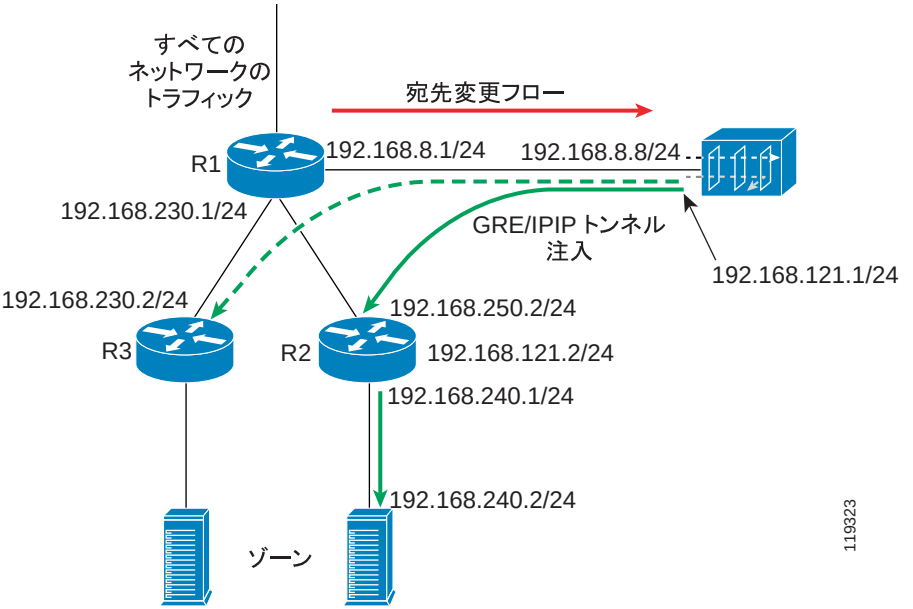
Guard からの BGP 通知は、グローバル ルーティング テーブルには表示されますが、guard-interface-routing-table には表示されないことに注意してください。

```
qa@ww-jnpr-1> run show route table inet.0

192.168.240.0/24   *[Static/5] 1d 05:28:07

  > to 192.168.250.2 via fe-0/0/0.0
192.168.240.0/25   *[BGP/170] 00:00:05, MED 0, localpref 100
                      AS path: 64555 ?
                    > to 192.168.8.8 via ge-0/0/0.0
192.168.240.128/25 *[BGP/170] 00:00:05, MED 0, localpref 100
                      AS path: 64555 ?
                      to 192.168.8.8 via ge-0/0/0.0

qa@ww-jnpr-1# run show route table guard-interface-routing--table
192.168.240.0/24   *[Static/5] 1d 02:26:37
                     to 192.168.250.2 via fe-0/0/0.0
```

トンネル宛先変更

この方式では、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。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 4-8　　トンネル宛先変更



トンネル宛先変更の設定

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 のトンネル宛先変更の設定

ネイティブ インターフェイスに関する文

インバンド インターフェイスを設定します。

```
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

トンネルを設定します。

GRE トンネル

```
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
```

IPIP トンネル

```
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

この章の「Guard の BGP 設定」の項の説明に従って、Guard のルータ BGP 設定を入力します。

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、R2 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 ルートが入力されています。

```
router# configure terminal
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

トンネル転送技術では、トンネルの端にあるルータ（上記の例では R2）の設定が必要であることに注意してください。宛先変更プロセスでは、宛先変更元ルータ（上記の例では R1）の設定が必要です。

R1 の宛先変更設定：BGP に関する文

この章の「Cisco ルータの BGP 設定」の項の説明に従って、ルータ R1 の BGR 設定を入力します。

R2 の転送設定：R2 上のトンネル インターフェイス

ルータ R2 にトンネルを設定します。

```
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
```

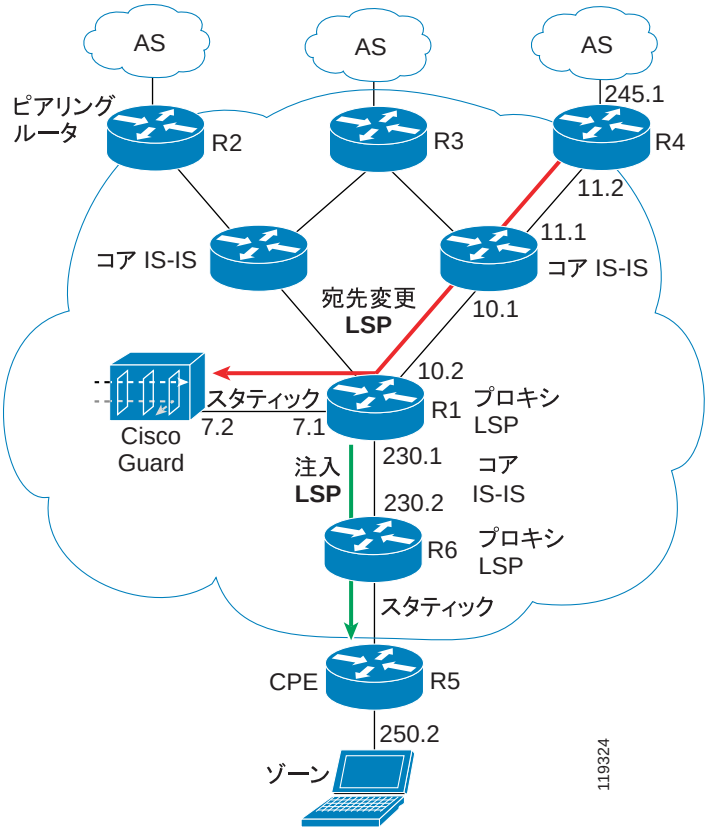
遠隔宛先変更

標準の宛先変更技術では、Cisco 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。

この項で使用する設定例には、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 4-9　遠隔宛先変更の設定



パケット フローの例

（LSP 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 4-9 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詳しく説明します。

Guard の CLI ループバック設定

Guard にループバック インターフェイスを追加します。

```
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

ルーティング設定にループバック インターフェイスを追加します。

ルーティング設定は、Zebra アプリケーションを使用して行います。

```
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

この設定は、ピアリング ルータ R2、R3、および R4 に関連します。

MPLS グローバル設定

ピアリング ルータに MPLS を設定します。

```
mpls ip
ip cef
```

インターフェイス Loopback 0 の設定

Loopback 0 インターフェイスを設定します。

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 3.3.3.3 255.255.255.255
 no ip directed-broadcast
 load-interval 30
```

接続インターフェイスの設定

ネットワーク接続インターフェイスを設定します。

```
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
```

IS-IS 設定

IS-IS を設定します。

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

BGP 設定

BGP を設定します。Guard への iBGP を設定します。

```
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。

インターフェイス Loopback 0 の設定

Loopback 0 インターフェイスを設定します。

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
```

ネットワークへのインターフェイスの設定

ネットワーク接続インターフェイスを設定します。

```
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
```

Guard へのインターフェイスの設定

Guard へのインターフェイスを設定します。

（注）　このインターフェイスには MPLS が設定されないことに注意してください。

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

ゾーンへのインターフェイスの設定

ゾーンへのインターフェイスを設定します。

（注）　このインターフェイスには MPLS が設定されることに注意してください。

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

IS-IS 設定

IS-IS を設定します。

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

スタティック ルートの設定

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。

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 ルートを設定します。

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