CHAPTER 5

トラフィックの宛先変更の設定

この章では、Cisco Anomaly Guard Module（Guard モジュール）でのトラフィックの宛先変更の設定方法について説明します。

（注） 1 Gbps で動作する Guard モジュールと 3 Gbps で動作する Guard モジュールでは、動作と設定に違いがあります。この章では、1 Gbps 動作と 3 Gbps 動作の違いについて説明します。特に記載がない限り、この章の情報は両方のモードの動作に適用されます。詳細については、P.1-9 の「1 Gbps と 3 Gbps の帯域幅オプションについて」を参照してください。

この章は、次の項で構成されています。

トラフィックの宛先変更について

トラフィックの宛先変更とは、次の目的でゾーン トラフィックを Guard モジュールに宛先変更するプロセスのことです。

- DDoS 攻撃（分散型サービス拒絶攻撃）の軽減：Guard モジュールは、トラフィックを分析し、悪意のあるパケットを削除し、クリーンなトラフィックをメイン データ パスに戻します。
- トラフィック ラーニング：Guard モジュールは、トラフィックを分析してゾーン固有の保護ポリシーを作成し、変更を加えずにゾーンのメイン トラフィック パスにトラフィックを戻します。

宛先変更には、次の 2 つのタスクが含まれます。

- ハイジャック：ゾーン トラフィックのルーティングの宛先を変更するために Guard モジュールが使用するプロセス。これによって、保護またはラーニングがアクティブな場合に、トラフィックが Guard モジュールに流れるようになります。ゾーン トラフィックは、通常のスーパーバイザ エンジンのオンボード ルーティング テーブルをバイパスします。
- 注入：正当なトラフィックを元のネットワーク データ パスに戻すために Guard モジュールが使用するプロセス。

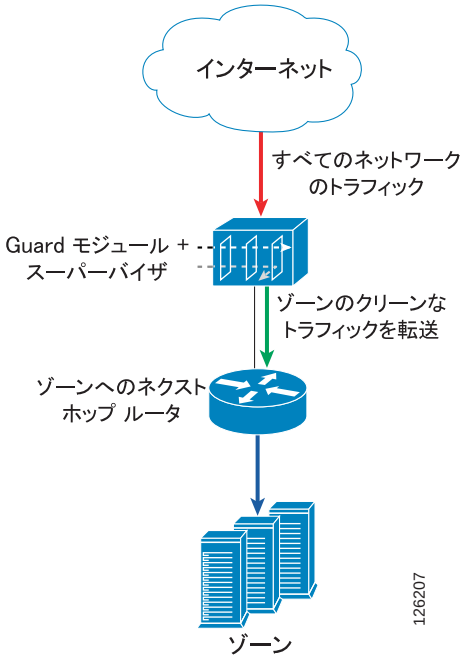
この項では、次のトピックについて取り上げます。

ネットワーク設定

Guard モジュールは、次のネットワーク設定のどちらかに設置できます。

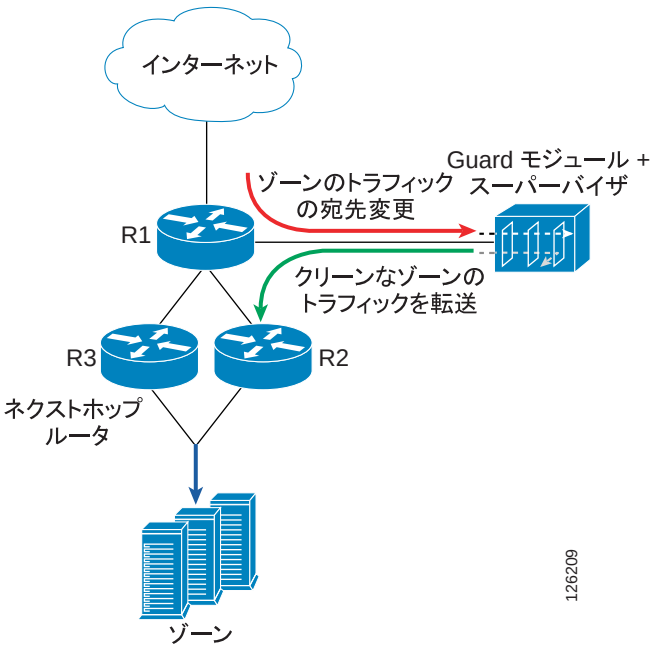
- インライン ネットワーク設定：メイン パスに存在するスイッチまたはルータに Guard モジュールを設置できます（ゾーン トラフィックはすでにこのスイッチまたはルータを通過しています）。この設定では、Guard モジュールは、スーパーバイザ エンジンのオンボード ルーティング テーブルにスタティック ルートを追加することで、ゾーン トラフィックをハイジャックして、正当なトラフィックを元の宛先に再び注入します。図 5-1 に、インライン ネットワーク設定の例を示します。

図 5-1　インライン ネットワーク設定



- アウトオブパス ネットワーク設定：ゾーン トラフィックのメイン ラインに配置されていなくても、メイン ラインの外側にあるスイッチまたはルータに Guard モジュールを設置できます。この設定では、Guard モジュールはゾーン トラフィックのメイン ラインからスイッチまたはルータにゾーントラフィックをハイジャックします。ハイジャックを設定する場合、Guard モジュールはスーパーバイザ エンジンのオンボード ルーティング テーブルにスタティック ルートを追加します。このスタティック ルートが Border Gateway Protocol（BGP）などの関連ルーティング プロトコルによってアドバタイズされるよう、スイッチまたはルータ上のルーティング テーブルの再配布をあらかじめ設定しておく必要があります。図 5-2 に、アウトオブパス ネットワーク設定の例を示します。

図 5-2　アウトオブパス ネットワーク設定



宛先変更のメカニズムについて

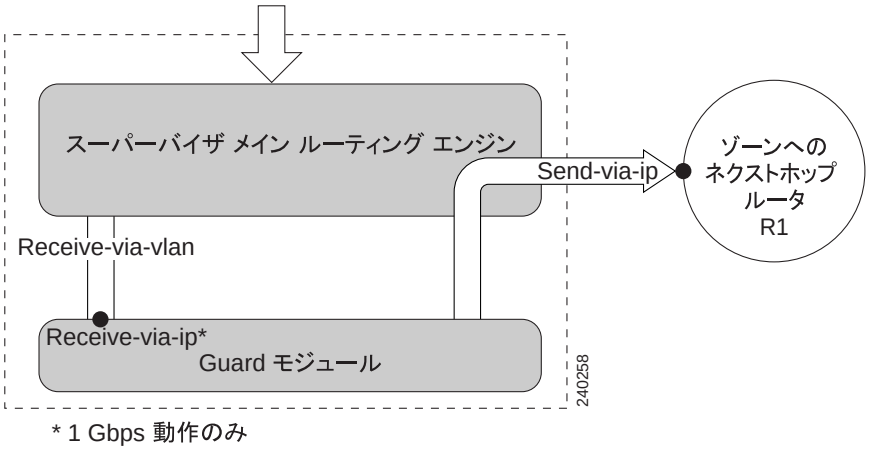
Guard モジュールの宛先変更設定は、定義するすべてのゾーンに適用されます。宛先変更設定は、パケットを各サブネットにルーティングする方法を定義したり、ハイジャックと注入の両方に必要なルートを定義します。Guard モジュールがゾーンを保護している場合、またはユーザがラーニング プロセスをアクティブにする場合、Guard モジュールは宛先変更の設定とゾーンの定義を使用して、そのゾーンを宛先とするトラフィックを宛先変更する方法と、トラフィックをゾーンのメイン トラフィック パスに再び注入する方法を判別します。

Guard モジュールは、Route Health Injection（RHI）という内部プロトコルを使用し、スーパーバイザ エンジンのオンボード ルーティング テーブルにルートを追加します。Guard モジュールは、Guard モジュールがゾーンを保護している場合、またはユーザがゾーンのラーニング プロセスをアクティブにする場合にルートを追加します。ゾーン保護およびラーニング プロセスが終了すると、Guard モジュールはルートを削除します。

（注）　3 Gbps 動作の場合は、スーパーバイザ エンジンが、Guard モジュールの 3 つのインターフェイス ポートすべてで宛先変更されたトラフィックのロード バランシングを実行します。1 Gbps 動作の場合は、ポート 2 のみがデータ トラフィックを搬送するため、インターフェイス間のロード バランシングは実行されません。

図 5-3 に、スーパーバイザ エンジンのオンボード ルーティング テーブルと Guard モジュールの間でパケットをルーティングする方法を示します。

図 5-3　宛先変更プロセス



* 1 Gbps 動作のみ

この項では、次のトピックについて取り上げます。

- ハイジャック パラメータの設定
- トラフィック注入パラメータの設定
- ハイジャック パラメータの注入ルートへの関連付け
- 宛先変更ルートの表示

ハイジャック パラメータの設定

ゾーンの保護をアクティブにすると、スーパーバイザ エンジンのオンボード ルーティング エンジンが、ゾーン トラフィックを Guard モジュールにハイジャックします。スーパーバイザ エンジンから Guard モジュールへのトラフィックは、receive-via-vlan VLAN にハイジャックされます。トラフィックのハイジャックと注入には、同じ VLAN を設定できます。

Guard モジュールは、スーパーバイザ エンジンのオンボード ルーティング テーブルにスタティック ルートをインストールします。このとき、ゾーンへのネクストホップとして Guard モジュールを指します。スタティック ルートはゾーンのトラフィックが Guard モジュールにハイジャックされることを保証します。Guard モジュールは、最長プレフィクスの照合アルゴリズムを使用します。つまり、各ルートをより長いプレフィクスを持つ 2 つのルートに分割し、これらのルートをスーパーバイザ エンジンのオンボード ルーティング テーブルにアドバタイズします。たとえば、24 ビット長のゾーン サブネット（クラス C）のルートは、25 ビット長のゾーン サブネットの 2 つのルートとして発行されます。

複数のハイジャック ルートを設定できます。各ハイジャック ルートは、ルート プリファレンスを定義する重みを持ちます。スーパーバイザ エンジンのオンボード ルーティング エンジンは、最大の重みを持つパスを優先的に使用します。デフォルトでは、すべてのハイジャック ルートに重みとして 1 が追加されています。デフォルトの重みを変更して、複数のハイジャック ルート間のプリファレンスを定義することができます。

ハイジャック パラメータを注入ルートに関連付けることができます。また、すべての注入ルートに当てはまるグローバル ハイジャック パラメータを設定できます。

（注）　ハイジャック パラメータを入力しない場合は、Guard モジュールがパラメータを動的に設定します。VLAN ID 値は、Guard モジュールの 3 つのインターフェイス（giga1、giga2、および giga3）でユーザが定義した VLAN ID に動的に設定されます。3 つのインターフェイスで VLAN を定義しない場合、Guard モジュールはネイティブ VLAN（VLAN 1）を使用します。

ハイジャック パラメータを注入ルートに関連付ける方法については、P.5-6 の「トラフィック注入パラメータの設定」を参照してください。

（1 Gbps 動作のみ）グローバルなハイジャック パラメータを設定するには、次のコマンドを使用します。

diversion hijacking {**receive-via-ip** *receive-via-ip* | **receive-via-vlan** [*receive-via-vlan* | **native**] | **weight** *weight*}

表 5-1　diversion hijacking コマンドの引数とキーワード（1 Gbps 動作）

パラメータ	説明
receive-via-ip *receive-via-ip*	スーパーバイザ エンジンがゾーン トラフィックを Guard モジュールに転送するときの IP アドレスを指定します。
receive-via-vlan	スーパーバイザ エンジンがゾーン トラフィックを Guard モジュールに転送するときに使用される VLAN を指定します。
receive-via-vlan	（オプション）スーパーバイザ エンジンの VLAN。
native	（オプション）スーパーバイザ エンジンのネイティブ VLAN を指定します。
weight *weight*	宛先変更ハイジャック ルートの重みを指定します。デフォルトは 1 です。

（3 Gbps 動作のみ）グローバルなハイジャック パラメータを設定するには、次のコマンドを使用します。

diversion hijacking {**native vlan** *vlan_name* | **receive-via-vlan** *receive-via-vlan* | **weight** *weight*}

表 5-2 で、**diversion hijacking** コマンドの引数とキーワードについて説明します。

表 5-2　diversion hijacking コマンドの引数とキーワード（3 Gbps 動作）

パラメータ	説明
native-vlan *vlan_name*	スーパーバイザ エンジンがゾーン トラフィックを Guard モジュールに転送するときに使用されるネイティブ VLAN を指定します。デフォルトのネイティブ VLAN は VLAN 1 です。 デフォルト値を復元する場合は、**no diversion hijacking native vlan** コマンドを入力します。
receive-via-vlan *receive-via-vlan*	スーパーバイザ エンジンがゾーン トラフィックを Guard モジュールに転送するときに使用される VLAN を指定します。
weight *weight*	宛先変更ハイジャック ルートの重みを指定します。デフォルトは 1 です。

トラフィック注入パラメータの設定

Guard モジュールは、ハイジャックされたストリームから悪意のあるパケットを削除し、正当なトラフィックを、スーパーバイザ エンジンのオンボード ルーティング エンジン（レイヤ 3）に戻すか、またはゾーンのメイン トラフィック パス（レイヤ 2）に直接戻します。Guard モジュールは正当なトラフィックを VLAN *send-via-vlan* 上で送信します。レイヤ 2 注入の場合は、ネクストホップ ルータと Guard モジュールが同じ VLAN 上に存在する必要があります。レイヤ 2 でゾーンのメイン トラフィック パスにトラフィックを注入するには、ゾーンへのネクストホップがネクストホップ ルータの IP アドレスになるように設定します。

注意　レイヤ 2 注入を設定する場合は、ルーティング ループが発生する可能性があるので、ネクストホップ ルータとしてスーパーバイザ エンジンの IP アドレスを入力しないでください。

トラフィック注入パラメータを設定するには、次のコマンドを使用します。

diversion injection *ip-address ip-mask* **nexthop** *next-hop*

表 5-3 で、**diversion injection** コマンドの引数とキーワードについて説明します。

表 5-3　diversion injection コマンドの引数とキーワード

パラメータ	説明
ip-address	ゾーンの IP アドレス。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.100.1）。
ip-mask	ゾーンの IP サブネット マスク。サブネット マスクをドット区切り 10 進表記で入力します（たとえば 255.255.255.0）。デフォルトのサブネット マスクは、255.255.255.255 です。
nexthop *next-hop*	ネクストホップ ルータ IP アドレスを指定します。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.100.1）。

IP アドレスおよびサブネット マスクは、特定のゾーンの IP アドレスおよびサブネット マスクと一致している必要はありません。これらは、ゾーン定義のサブセットにすることも、複数のゾーンのサブネットにすることもできます。たとえば、1 つまたは 2 つのコマンドを使用して、候補となる数百ものゾーンのネットワークについてトラフィックの宛先変更を設定することができます。

ハイジャック パラメータの注入ルートへの関連付け

ハイジャック パラメータを注入ルートに関連付けることができます。また、すべての注入ルートに当てはまるグローバル ハイジャック パラメータを設定できます。

（1 Gbps 動作のみ）ハイジャック パラメータを注入ルートに関連付けるには、次のコマンドを使用します。

diversion injection *ip-address ip-mask* **nexthop** *next-hop* [**hijacking** {**receive-via-ip** *receive-via-ip* | **receive-via-vlan** *receive-via-vlan* | **weight weight**}]

表 5-4 で、**diversion injection hijacking** コマンドの引数とキーワードについて説明します。

表 5-4　diversion injection hijacking コマンドの引数（1 Gbps 動作）

パラメータ	説明
ip-address	ゾーンの IP アドレス。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.100.1）。
ip-mask	ゾーンの IP サブネット マスク。サブネット マスクをドット区切り 10 進表記で入力します（たとえば 255.255.255.0）。デフォルトのサブネット マスクは、255.255.255.255 です。
nexthop *next-hop*	ネクストホップ ルータ IP アドレスを指定します。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.100.1）。
hijacking	（オプション）ハイジャック パラメータを注入ルートに関連付けます。
receive-via-ip *receive-via-ip*	スーパーバイザ エンジンがゾーン トラフィックを Guard モジュールに転送するときの IP アドレスを指定します。
receive-via-vlan *receive-via-vlan*	スーパーバイザ エンジンがゾーン トラフィックを Guard モジュールに転送するときに使用される VLAN を指定します。
weight *weight*	宛先変更ハイジャック ルートの重みを指定します。デフォルト値は 1 です。

（3 Gbps 動作のみ）ハイジャック パラメータを注入ルートに関連付けるには、次のコマンドを使用します。

diversion injection *ip-address ip-mask* **nexthop** *next-hop* [**hijacking** {**receive-via-vlan** *receive-via-vlan* | **weight** *weight*}]

表 5-5 で、**diversion injection hijacking** コマンドの引数とキーワードについて説明します。

表 5-5　diversion injection hijacking コマンドの引数とキーワード（3 Gbps 動作）

パラメータ	説明
ip-address	ゾーンの IP アドレス。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.100.1）。
ip-mask	ゾーンの IP サブネット マスク。サブネット マスクをドット区切り 10 進表記で入力します（たとえば 255.255.255.0）。デフォルトのサブネット マスクは、255.255.255.255 です。
nexthop *next-hop*	ネクストホップ ルータ IP アドレスを指定します。IP アドレスをドット区切り 10 進表記で入力します（たとえば 192.168.100.1）。

表 5-5　diversion injection hijacking コマンドの引数とキーワード（3 Gbps 動作）（続き）

パラメータ	説明
hijacking	（オプション）ハイジャック パラメータを注入ルートに関連付けます。
receive-via-vlan *receive-via-vlan*	スーパーバイザ エンジンがゾーン トラフィックを Guard モジュールに転送するときに使用される VLAN を指定します。
weight *weight*	宛先変更ハイジャック ルートの重みを指定します。デフォルト値は 1 です。

宛先変更ルートの表示

Guard モジュールは、RHI メッセージを使用して、スーパーバイザ エンジンのオンボード ルーティング テーブルを変更します。Guard モジュールは、ゾーン保護をイネーブルにした場合またはゾーンのラーニング プロセスをアクティブにした場合にルートを追加し、ゾーン保護とラーニング プロセスが終了したときにルートを削除します。

Guard モジュールの宛先変更の設定を表示するには、**show diversion** コマンドを使用します。

Guard モジュールがゾーンを保護している場合やゾーン トラフィックの特性だけをラーニングしている場合に、Guard モジュールがスーパーバイザまたはエンジン上にアドバタイズした RHI メッセージを表示できます。

Guard モジュールがアドバタイズしたルートを表示するには、スーパーバイザ エンジンで次のコマンドを使用します。

show anomaly-guard module *module_number* **advertised-route**

module_number 引数には、モジュールが装着されているスロットの番号を指定します。

次の 3 Gbps 動作例は、Guard モジュールがスーパーバイザ エンジンにアドバタイズしたルートを表示する方法を示しています。

```
Sup# show anomaly-guard module 9 advertised-route
RHI routes added by slot 9
      ip               mask             nexthop          vlan     weight
      --------------   --------------   --------------   ------   ------
A     192.168.252.8    255.255.255.0    192.168.8.10     8        1
A     192.168.252.8    255.255.255.0    192.168.8.12     8        1
A     192.168.252.8    255.255.255.0    192.168.8.14     8        1
A     192.168.252.10   255.255.255.0    192.168.8.10     8        1
A     192.168.252.10   255.255.255.0    192.168.8.12     8        1
A     192.168.252.10   255.255.255.0    192.168.8.14     8        1
```

Guard モジュールがスタティック ルートを追加したことを確認するには、スーパーバイザ エンジン上に次のコマンドを入力して、スーパーバイザ エンジンのオンボード ルーティング テーブルを表示します。

show ip route

次の 3 Gbps 動作例は、Guard モジュールがスーパーバイザ エンジンのオンボード ルーティング テーブルに追加したスタティック ルートを表示する方法を示しています。スタティック ルートには、「S」というマークが付いています。

```
Sup# show ip route 192.168.252.8
Routing entry for 192.168.252.8/24, 3 known subnets
Variably subnetted with 2 masks
S    192.168.252.10/32 [1/0] via 192.168.8.10, Vlan8
    [1/0] via 192.168.8.12, Vlan8
    [1/0] via 192.168.8.14, Vlan8
S    192.168.252.8/32 [1/0] via 192.168.8.10, Vlan8
    [1/0] via 192.168.8.12, Vlan8
    [1/0] via 192.168.8.14, Vlan8
```

インライン ネットワーク設定での Guard モジュールの設定

インライン ネットワーク設定では、ゾーンのクリティカル パス上にあるスイッチまたはルータに Guard モジュールが取り付けられます。つまり、ゾーンが Guard モジュールによって保護されているかどうかに関係なく、ゾーン トラフィックはこのスイッチまたはルータを通過します。

この項では、次のトピックについて取り上げます。

トラフィック ハイジャックの設定

トラフィックの宛先変更を設定するため、Guard モジュールは、最長プレフィックス照合を使用した RHI メッセージを使用してスーパーバイザ エンジンのオンボード ルーティング テーブルにルートを追加します。詳細については、P.5-5 の「ハイジャック パラメータの設定」を参照してください。

トラフィック注入の設定

正当なトラフィックを元のデータ パスに戻す場合は、レイヤ 2 またはレイヤ 3 のトラフィック注入を設定できます。詳細については、P.5-18 の「トラフィック注入方式について」を参照してください。

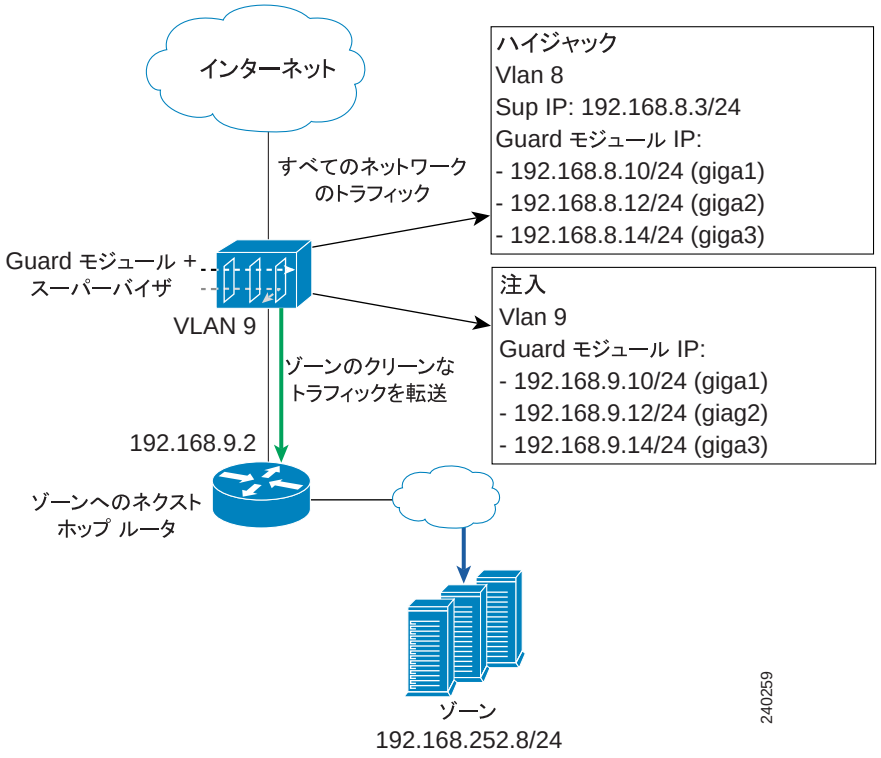
インライン ネットワーク設定の例

図 5-4 に、インライン ネットワーク設定におけるトラフィックの宛先変更の例を示します。以降の例は、次の条件に基づいています。

- ハイジャックはレイヤ 3 で実行される。
- 注入はレイヤ 2 で実行される。
- Guard モジュールは、3 Gbps 動作のソフトウェア イメージを使用しており、ユーザは 3 つのインターフェイス ポートすべてを設定する必要があります（1 Gbps 動作の場合は、データ トラフィック用の 1 つのインターフェイス ポートのみを設定します）。詳細については、P.1-9 の「1 Gbps と 3 Gbps の帯域幅オプションについて」を参照してください。

（注）　トラフィックの宛先変更を設定する前に、ネットワークを設定する必要があります。第 2 章「スーパーバイザ エンジンへの Guard モジュールの設定」および第 3 章「Guard モジュールの初期化」を参照してください。

図 5-4　レイヤ 3 トポロジを持つインライン ネットワーク設定のサンプル（3 Gbps 動作）



- Guard モジュールは、スイッチのスロット 9 に設置されている。
- スイッチ上のポート GigabitEthernet2/2 は、VLAN 9 でネクストホップ ルータに接続されている。

図 5-4 に示す 3 Gbps 動作での設定例にあるようにスーパーバイザ エンジンと Guard モジュールを設定するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、スーパーバイザ エンジン上にスイッチまたはルータ インターフェイスを設定します。

```
Sup# conf term
Sup(config)# vlan 8,9
Sup(config)# anomaly-guard module 9 port 1 allowed-vlan 8,9
Sup(config)# anomaly-guard module 9 port 2 allowed-vlan 8,9
Sup(config)# anomaly-guard module 9 port 3 allowed-vlan 8,9
Sup(config)# interface vlan 8
Sup(config-if)# ip address 192.168.8.3 255.255.255.0
Sup(config-if)# no ip proxy-arp
Sup(config-if)# no shutdown
Sup(config-if)# exit
Sup(config)# interface vlan 9
Sup(config-if)# ip address 192.168.9.3 255.255.255.0
Sup(config-if)# no ip proxy-arp
Sup(config-if)# no shutdown
Sup(config-if)# exit
Sup(config)# interface GigabitEthernet2/2
Sup(config-if)# switchport
Sup(config-if)# switchport mode access
Sup(config-if)# switchport access vlan 9
```

ステップ 2　Guard モジュール上に Guard モジュール VLAN インターフェイスを設定するには、次のコマンドを入力します。

```
user@GUARD# conf term
user@GUARD-conf# interface giga 1.8
user@GUARD-conf-if-giga1.8# ip address 192.168.8.10 255.255.255.0
user@GUARD-conf-if-giga1.8# no shutdown
user@GUARD-conf-if-giga1.8# interface giga 1.9
user@GUARD-conf-if-giga1.9# ip address 192.168.9.10 255.255.255.0
user@GUARD-conf-if-giga1.9# no shutdown
user@GUARD-conf-if-giga1.9# interface giga 2.8
user@GUARD-conf-if-giga2.8# ip address 192.168.8.12 255.255.255.0
user@GUARD-conf-if-giga2.8# no shutdown
user@GUARD-conf-if-giga2.8# interface giga 2.9
user@GUARD-conf-if-giga2.9# ip address 192.168.9.12 255.255.255.0
user@GUARD-conf-if-giga2.9# no shutdown
user@GUARD-conf-if-giga2.9# interface giga 3.8
user@GUARD-conf-if-giga3.8# ip address 192.168.8.14 255.255.255.0
user@GUARD-conf-if-giga3.8# no shutdown
user@GUARD-conf-if-giga3.8# interface giga 3.9
user@GUARD-conf-if-giga3.9# ip address 192.168.9.14 255.255.255.0
user@GUARD-conf-if-giga3.9# no shutdown
user@GUARD-conf-if-giga3.9# exit
```

ステップ 3　Guard モジュールでトラフィックの宛先変更を設定するには、次のコマンドを入力します。

```
user@GUARD# conf term
user@GUARD-conf# diversion hijacking receive-via-vlan 8
user@GUARD-conf# diversion injection 192.168.252.0 255.255.255.0 nexthop 192.168.9.2
```

ステップ 4　**protect** コマンドまたは **learning** コマンドを入力して、ゾーンをアクティブにします。

詳細については、P.6-10 の「Guard モジュールの Detector とのゾーン設定の同期」および第 10 章「ゾーンの保護」を参照してください。

ステップ 5　Guard モジュールがアドバタイズしたルートを表示するには、スーパーバイザ エンジンで **show anomaly-guard module advertised-route** コマンドを入力します。

次の例は、Guard モジュールがスーパーバイザ エンジンにアドバタイズしたルートを表示する方法を示しています。

```
Sup# show anomaly-guard module 9 advertised-route
RHI routes added by slot 9

      ip               mask             nexthop          vlan     weight
      --------------   --------------   --------------   ------   ------
A     192.168.252.0    255.255.255.128  192.168.8.10     8        1
A     192.168.252.0    255.255.255.128  192.168.8.12     8        1
A     192.168.252.0    255.255.255.128  192.168.8.14     8        1
A     192.168.252.128  255.255.255.128  192.168.9.10     8        1
A     192.168.252.128  255.255.255.128  192.168.9.12     8        1
A     192.168.252.128  255.255.255.128  192.168.9.14     8        1
```

（注）　Guard モジュールは、Guard モジュールがゾーンを保護している場合、またはユーザがラーニング プロセスをアクティブにする場合にこれらのルートをアドバタイズします。

ステップ 6　スーパーバイザ エンジンのオンボード ルーティング テーブルに追加されたスタティック ルートを表示するには、**show ip route** コマンドを入力します。

次の例は、スーパーバイザ エンジンのオンボード ルーティング テーブルに追加されたスタティック ルートを表示する方法を示しています。

```
Sup# show ip route 192.168.252.0
Routing entry for 192.168.252.0/24, 3 known subnets
    Variably subnetted with 2 masks
S       192.168.252.128/25 [1/0] via 192.168.8.10, Vlan8
    [1/0] via 192.168.8.12, Vlan8
    [1/0] via 192.168.8.14, Vlan8
S       192.168.252.0/25 [1/0] via 192.168.8.10, Vlan8
    [1/0] via 192.168.8.12, Vlan8
    [1/0] via 192.168.8.14, Vlan8
```

アウトオブパス ネットワーク設定での Guard モジュールの設定

アウトオブパス ネットワーク設定では、Guard モジュールは、ゾーン トラフィックの通常のラインにあるスイッチまたはルータではなく、ゾーン トラフィックのラインの外側にあるスイッチまたはルータに設置されます。ゾーン トラフィックは、ゾーン トラフィックの通常のラインからスイッチまたはルータに宛先変更されます。

この項では、次のトピックについて取り上げます。

トラフィック ハイジャックの設定

トラフィックの宛先変更を設定するには、Guard モジュールにより、RHI メッセージを使用するスーパーバイザ エンジンのオンボード ルーティング テーブルにスタティック ルートを追加します。ゾーン トラフィックが Guard モジュールに直接転送されることを保証する最長プレフィックス照合を使用します。詳細については、P.5-5 の「ハイジャック パラメータの設定」を参照してください。

Guard モジュールがゾーンを保護している場合、またはユーザがラーニング プロセスをアクティブにする場合、Guard モジュールはスーパーバイザ エンジンのオンボード ルーティング テーブルを変更します。ゾーン トラフィックがハイジャックされるルータ（宛先変更元ルータ）に Border Gateway Protocol（BGP; ボーダー ゲートウェイ プロトコル）アナウンスメントを発行するように、スーパーバイザ エンジンまたは Multilayer Switch Feature Card（MSFC; マルチレイヤ スイッチ フィーチャ カード）を設定する必要があります。BGP アナウンスメントは、内部 BGP（iBGP）アナウンスメントの場合も、外部 BGP（eBGP）アナウンスメントの場合もあります。スーパーバイザ エンジンがアドバタイズする 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。アナウンスメントにより、特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。ゾーンの Guard モジュールからトラフィックを転送するルータが BGP アナウンスメントを転送しないことを保証するには、*no-advertise* と *no-export* の BGP コミュニティ ストリングを設定します。*no-advertise* および *no-export* BGP コミュニティ ストリングを設定することで、ゾーンが宛先になっているパケットがネクストホップ ルータに到達したときに、ルータがパケットをゾーンに転送して、Guard モジュールに戻さないことを保証します。

トラフィック注入の設定

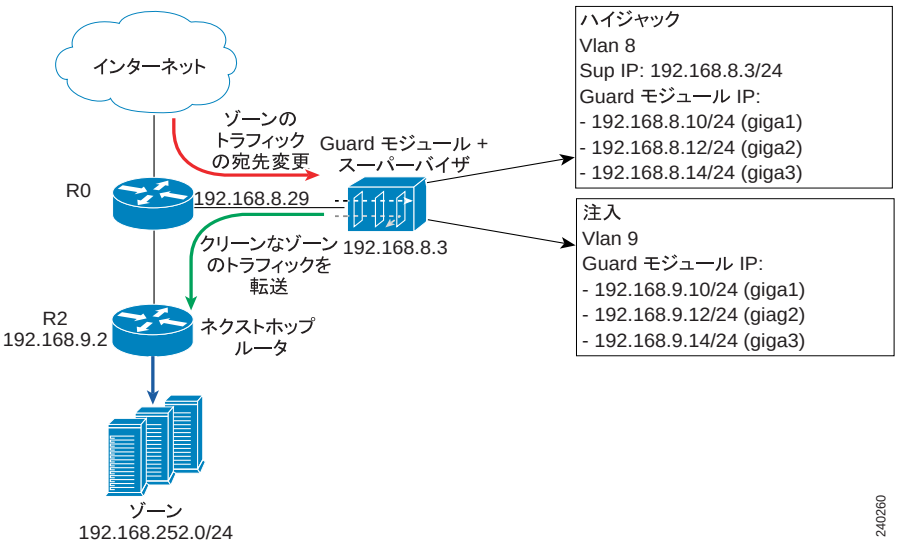
正当なトラフィックを元のデータ パスに戻す場合は、レイヤ 2 またはレイヤ 3 のトラフィック注入を設定できます。詳細については、P.5-18 の「トラフィック注入方式について」を参照してください。

アウトオブパス ネットワーク設定の例

図 5-5 に、アウトオブパス ネットワーク設定におけるトラフィックの宛先変更の例を示します。この例では、レイヤ 3 でハイジャックが、レイヤ 2 で注入が実行されています。

（注）　トラフィックの宛先変更を設定する前に、ネットワークを設定する必要があります。詳細については、第 2 章「スーパーバイザ エンジンへの Guard モジュールの設定」および第 3 章「Guard モジュールの初期化」を参照してください。

図 5-5　レイヤ 3 トポロジを持つアウトオブパス ネットワーク設定のサンプル（3 Gbps 動作）



- Guard モジュールは、スイッチまたはルータのスロット 9 に設置されています。
- スイッチまたはルータ上のポート Gigabit Ethernet 2/2 は、VLAN 9 のネクストホップ ルータに接続されています。
- R0 と R2 は Autonomous System（AS; 自律システム）100 に存在し、Guard モジュールは AS 55 に存在します。

（注）　Guard モジュールがゾーンを保護していない場合、トラフィックは R0 から R2 に直接流れます。ゾーン トラフィックのルートは、大きな（1 より大きい）重みを持つか、Guard モジュールのルートよりも限定的でないルートを持つ必要があります。

図 5-5 に示す 3 Gbps 動作での設定例にあるようにスーパーバイザ エンジンと Guard モジュールを設定するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、スーパーバイザ エンジン上にスイッチまたはルータ インターフェイスを設定します。

```
sup# conf term
Sup(config)# vlan 8,9
Sup(config)# anomaly-guard module 9 port 1 allowed-vlan 8,9
Sup(config)# anomaly-guard module 9 port 2 allowed-vlan 8,9
Sup(config)# anomaly-guard module 9 port 3 allowed-vlan 8,9
Sup(config)# interface vlan 8
Sup(config-if)# ip address 192.168.8.3 255.255.255.0
Sup(config-if)# no ip proxy-arp
Sup(config-if)# no shutdown
Sup(config-if)# exit
Sup(config)# interface vlan 9
Sup(config-if)# ip address 192.168.9.3 255.255.255.0
Sup(config-if)# no ip proxy-arp
Sup(config-if)# no shutdown
Sup(config-if)# exit
Sup(config)# interface GigabitEthernet2/2
Sup(config-if)# switchport mode trunk
Sup(config-if)# switchport trunk encapsulation dot1q
Sup(config-if)# switchport
Sup(config-if)# switchport trunk allowed vlan 8,9
```

ステップ 2　Guard モジュールにより、スーパーバイザ エンジンのオンボード ルーティング テーブルに追加するスタティック ルートだけが隣接ルータに発行されるよう、スーパーバイザ エンジンに 2 つのルート マップを設定します。次のコマンドを入力することで、*no-advertise* と *no-export* の BGP コミュニティ ストリングを設定します。

```
sup# conf term
Sup(config)# access-list 61 permit 192.168.8.10
Sup(config)# access-list 61 permit 192.168.8.12
Sup(config)# access-list 61 permit 192.168.8.14
Sup(config)# route-map PERMIT_GUARD_ONLY permit 10
Sup(config-route-map)# match ip next-hop 61
Sup(config-route-map)# set community no-export no-advertise
Sup(config-route-map)# exit
Sup(config)# route-map PERMIT_GUARD_ONLY deny 20
Sup(config)# route-map STA2BGP permit 10
Sup(config-route-map)# match ip next-hop 61
Sup(config-route-map)# exit
Sup(config)# route-map STABGP deny 20
```

ステップ 3　スーパーバイザ エンジンに BGP 再配布ルートを設定します。AS 100 の隣接ルータを定義します。次のコマンドを入力することで、スーパーバイザ エンジンが Guard モジュールの *receive-via-ip* アドレスに等しい宛先 IP アドレスを使用してオンボード ルーティング テーブルにスタティック ルートを追加するたびに BGP アナウンスメントを発行するように、スーパーバイザ エンジンを設定します。

```
sup# conf term
Sup(config)# router bgp 55
Sup(config-router)# bgp log-neighbor-changes
Sup(config-router)# neighbor 192.168.8.29 remote-as 100
Sup(config-router)# address-family ipv4
Sup(config-router-af)# redistribute static route-map STA2BGP
Sup(config-router-af)# neighbor 192.168.8.29 route-map PERMIT_GUARD_ONLY out
Sup(config-router-af)# neighbor 192.168.8.29 activate
Sup(config-router-af)# no auto-summary
Sup(config-router-af)# no synchronization
Sup(config-router-af)# exit-address-family
```

ステップ 4　Guard モジュール上に Guard モジュール インターフェイスを設定するには、次のコマンドを入力します。

```
user@GUARD# conf term
user@GUARD-conf# interface giga 1.8
user@GUARD-conf-if-giga1.8# ip address 192.168.8.10 255.255.255.0
user@GUARD-conf-if-giga1.8# no shutdown
user@GUARD-conf-if-giga1.8# interface giga 2.8
user@GUARD-conf-if-giga2.8# ip address 192.168.8.12 255.255.255.0
user@GUARD-conf-if-giga2.8# no shutdown
user@GUARD-conf-if-giga2.8# interface giga 3.8
user@GUARD-conf-if-giga3.8# ip address 192.168.8.14 255.255.255.0
user@GUARD-conf-if-giga3.8# no shutdown
user@GUARD-conf-if-giga3.8# interface giga 1.9
user@GUARD-conf-if-giga1.9# ip address 192.168.9.10 255.255.255.0
user@GUARD-conf-if-giga1.9# no shutdown
user@GUARD-conf-if-giga1.9# interface giga 2.9
user@GUARD-conf-if-giga2.9# ip address 192.168.9.12 255.255.255.0
user@GUARD-conf-if-giga2.9# no shutdown
user@GUARD-conf-if-giga2.9# interface giga 3.9
user@GUARD-conf-if-giga3.9# ip address 192.168.9.14 255.255.255.0
user@GUARD-conf-if-giga3.9# no shutdown
user@GUARD-conf-if-giga3.9# exit
```

ステップ 5　Guard モジュールでトラフィックの宛先変更を設定するには、次のコマンドを入力します。

```
user@GUARD# conf term
user@GUARD-conf# diversion hijacking receive-via-vlan 8
user@GUARD-conf# diversion injection 192.168.252.0 255.255.255.0 nexthop 192.168.9.2
```

ステップ 6　次のコマンドを入力して、ルータ R0 上に BGP 設定を設定します。

```
RouterR0# conf term
RouterR0(config)# router bgp 100
RouterR0(config-router)# neighbor 192.168.8.3 remote-as 55
```

ステップ 7　**protect** コマンドまたは **learning** コマンドを入力して、ゾーンをアクティブにします。

詳細については、P.6-10 の「Guard モジュールの Detector とのゾーン設定の同期」および第 10 章「ゾーンの保護」を参照してください。

ステップ 8　Guard モジュールがアドバタイズしたルートを表示するには、スーパーバイザ エンジンで **show anomaly-guard module advertised-route** コマンドを入力します。

次の例は、Guard モジュールがスーパーバイザ エンジンにアドバタイズしたルートを表示する方法を示しています。

```
Sup# show anomaly-guard module 9 advertised-route
RHI routes added by slot 9

      ip               mask             nexthop          vlan     weight
      --------------   --------------   --------------   ------   ------
A     192.168.252.8    255.255.255.0    192.168.8.10     8        1
A     192.168.252.8    255.255.255.0    192.168.8.12     8        1
A     192.168.252.8    255.255.255.0    192.168.8.14     8        1
```

（注）　Guard モジュールは、ゾーンを保護している場合、またはユーザがラーニング プロセスだけをアクティブにする場合にこれらのルートをアドバタイズします。

ステップ 9　スーパーバイザ エンジンのオンボード ルーティング テーブルに追加されたスタティック ルートを表示するには、**show ip route** コマンドを入力します。

次の例は、スーパーバイザ エンジンのオンボード ルーティング テーブルに追加されたスタティック ルートを表示する方法を示しています。

```
Sup# show ip route
...
192.168.252.0/24 is variably subnetted, 3 subnets, 2 masks
S       192.168.252.0/25 [1/0] via 192.168.8.10, Vlan8
    [1/0] via 192.168.8.12, Vlan8
    [1/0] via 192.168.8.14, Vlan8
S       192.168.252.128/25 [1/0] via 192.168.8.10, Vlan8
    [1/0] via 192.168.8.12, Vlan8
    [1/0] via 192.168.8.14, Vlan8
```

ステップ 10　ルータ R0 がゾーンへの新しいルート（Guard モジュールによってアドバタイズされたもの）をルーティング テーブルに追加したことを確認します。ルータ R0 上の BGP ルーティング テーブルを表示します。

次の例は、Guard モジュールがゾーンへの新しいルートをアドバタイズする前の BGP ルーティング テーブルを示しています。

```
RouterR0# show ip bgp
.
.
.
   Network          Next Hop          Metric LocPrf     Weight   Path
*>  192.168.252.0/24  192.168.9.2       0                 0        100 ?
```

次の例は、Guard モジュールがゾーンへの新しいルートをアドバタイズした後の BGP ルーティング テーブルを示しています。

```
RouterR0# show ip bgp
.
.
.
   Network          Next Hop          Metric LocPrf     Weight   Path
*>  192.168.252.0/25  192.168.8.3       0                 0        55 ?
*>  192.168.252.128/25192.168.8.3       0                 0        55 ?

RouterR0#
```

トラフィック注入方式について

この項では、Guard モジュールからネクストホップ ルータに正当なトラフィックを注入する際に使用される各方式について説明します。方式は、2 つのメイン ネットワーク トポロジによって異なります。

- レイヤ 2 トポロジ
- レイヤ 3 トポロジ

レイヤ 2 トポロジ

レイヤ 2 トポロジでは、Guard モジュールは、正当なトラフィックを元の宛先に戻すために、正当なトラフィックをネクストホップ ルータに直接転送します。スーパーバイザ エンジンがルーティングを決定する必要はありません。

Guard モジュールは、ネクストホップ ルータの IP アドレスに Address Resolution Protocol（ARP; アドレス解決プロトコル）クエリーを送信して、ネクストホップ ルータの MAC アドレスを特定します（詳細については、P.5-6 の「トラフィック注入パラメータの設定」を参照）。次に、関連するネクストホップ ルータに接続されているスイッチまたはルータ インターフェイスに正当なトラフィックを転送します。スーパーバイザ エンジンとゾーンへのネクストホップ ルータは同じ VLAN 上に存在する必要があり、Guard モジュールはその VLAN 上に IP アドレスを持っている必要があります。

設定例については、P.5-9 の「インライン ネットワーク設定の例」および P.5-14 の「アウトオブパス ネットワーク設定の例」を参照してください。

レイヤ 3 トポロジ

レイヤ 3 トポロジでは、スーパーバイザ エンジンはルーティングの決定を行い、正当なトラフィックを元の宛先に注入して戻す必要があります。Guard モジュールは、正当なトラフィックを次の宛先のどちらかに注入できます。

- 別のルータまたは VLAN : 設定例については、P.5-9 の「インライン ネットワーク設定の例」を参照してください。
- トラフィックのハイジャック元に戻す。

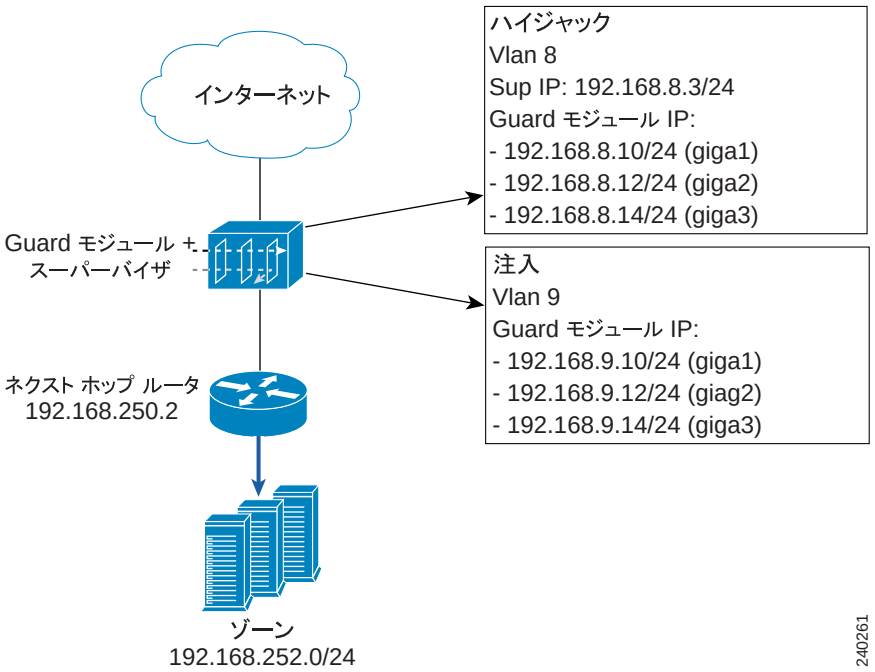
protect コマンドまたは **learning** コマンドを入力してゾーンをアクティブにする場合、Guard モジュールは、ゾーンへの最適パスとしてリストされるようにルーティング テーブルを変更します（ルーティング テーブルは、ネットワーク トポロジに応じて、スーパーバイザ エンジンのオンボード ルーティング テーブルまたは隣接ルータのルーティング テーブルのどちらかです）。Guard モジュールが正当なトラフィックをトラフィックのハイジャック元に戻す場合、ルーティング ループが発生することがあります。ルーティング ループが発生しないようにするには、ルーティング規則を Guard モジュールがゾーンに転送する正当なトラフィックに関連付け、これらのルーティング規則がグローバル ルーティング テーブルを無効にするように設定します。

Virtual Private Network（VPN）Routing および Forwarding（VRF）インスタンスを使用すると、スーパーバイザ エンジンのオンボード ルーティング テーブルを使用せずにスーパーバイザ エンジンのオンボード ルーティング エンジンに追加の転送テーブルを作成し、ループを避けながらトラフィックを転送できます。この転送テーブルを使用して、Guard モジュールからゾーンに送信されるパケットをルーティングするための代替注入パスを定義します。転送テーブルには、ゾーンへのネクストホップ ルータにトラフィックを転送する方法についての情報だけを含めます。

ゾーン トラフィックは、ネクストホップ ルータに直接転送するか、Generic Routing Encapsulation（GRE）または IP in IP（IPIP）トンネルに注入することができます。

図 5-6 は、レイヤ 3 注入設定の例を表示します。

図 5-6　レイヤ 3 注入の設定例（3 Gbps 動作）



この項では、次のトピックについて取り上げます。

- VRF トラフィック注入のための Guard モジュールとスーパーバイザ エンジンの設定
- トラフィックの直接注入
- トンネルを介したトラフィック注入

VRF トラフィック注入のための Guard モジュールとスーパーバイザ エンジンの設定

VRF は、レイヤ 3 ネットワーク トポロジで展開されるトラフィック注入方式です。この方式では、Guard モジュールが、正当なトラフィックをトラフィックのハイジャック元のルータに再び注入します。VRF は、インライン ネットワーク設定とアウトオブパス ネットワーク設定の両方に適用できます。

VRF を使用すると、グローバルなルーティング / 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。このテーブルは、Guard モジュールとのインターフェイス上で受信されるトラフィックをルーティングするように設定します。

（注）　図 5-6 の設定は、インライン ネットワーク設定とアウトオブパス ネットワーク設定の両方に適用されます。

- ハイジャック 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 Guard モジュールにハイジャックする場合に使用します。この VLAN 上のトラフィックは、グローバル ルーティング テーブルに従って転送されます。次の例では、ハイジャック用に VLAN 8 を使用します。

- 注入インターフェイス：このインターフェイスは、戻されたトラフィックを Guard モジュールからゾーンのメイン データ パスに注入する場合に使用します。このインターフェイスに VRF テーブルを設定します。VRF テーブル内のスタティック ルートは、Guard モジュールからゾーンに送信されたすべてのトラフィックをネクストホップ ルータに転送するように設定します。次の例では、注入用に VLAN 9 を使用します。

（注）　複数のネクストホップ ルータを設定できます。

図 5-6 の設定例で示したようにスーパーバイザ エンジンと Guard モジュールを設定するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、スーパーバイザ エンジン上に VRF テーブルを作成します。

```
Sup# conf term
Sup(config)# ip vrf Guard-vrf
Sup(config-vrf)# rd 100:1
```

ステップ 2　次のいずれかのタスクを実行して、スーパーバイザ エンジン上に VRF テーブルを設定します。

- トラフィックをネクストホップ ルータに直接注入する。
- トンネルを介してトラフィックを注入する。

詳細については、P.5-21 の「トラフィックの直接注入」および P.5-22 の「トンネルを介したトラフィック注入」を参照してください。

ステップ 3　次のコマンドを入力して、スーパーバイザ エンジンに VLAN インターフェイスを設定し、このインターフェイスを Guard モジュールに関連付けます。

```
Sup# conf term
Sup(config)# interface vlan 8
Sup(config-if)# ip address 192.168.8.3 255.255.255.0
Sup(config-if)# no ip proxy-arp
Sup(config-if)# no ip directed-broadcast
Sup(config-if)# no shutdown
Sup(config-if)# exit
Sup(config)# interface vlan 9
Sup(config-if)# ip vrf forwarding Guard-vrf
Sup(config-if)# ip address 192.168.9.3 255.255.255.0
Sup(config-if)# no ip proxy-arp
Sup(config-if)# no shutdown
Sup(config-if)# exit
Sup(config)# anomaly-guard module 9 port 1 allowed-vlan 8,9
Sup(config)# anomaly-guard module 9 port 2 allowed-vlan 8,9
Sup(config)# anomaly-guard module 9 port 3 allowed-vlan 8,9
```

ステップ 4　Guard モジュール上に Guard モジュール インターフェイスを設定するには、次のコマンドを入力します。

```
user@GUARD# conf term
user@GUARD-conf# interface giga 1.8
user@GUARD-conf-if-giga1.8# ip address 192.168.8.10 255.255.255.0
user@GUARD-conf-if-giga1.8# no shutdown
user@GUARD-conf-if-giga1.8# interface giga 2.8
user@GUARD-conf-if-giga2.8# ip address 192.168.8.12 255.255.255.0
user@GUARD-conf-if-giga2.8# no shutdown
user@GUARD-conf-if-giga2.8# interface giga 3.8
user@GUARD-conf-if-giga3.8# ip address 192.168.8.14 255.255.255.0
user@GUARD-conf-if-giga3.8# no shutdown
user@GUARD-conf-if-giga3.8# interface giga 1.9
user@GUARD-conf-if-giga1.9# ip address 192.168.9.10 255.255.255.0
user@GUARD-conf-if-giga1.9# no shutdown
user@GUARD-conf-if-giga1.9# interface giga 2.9
user@GUARD-conf-if-giga2.9# ip address 192.168.9.12 255.255.255.0
user@GUARD-conf-if-giga2.9# no shutdown
user@GUARD-conf-if-giga2.9# interface giga 3.9
user@GUARD-conf-if-giga3.9# ip address 192.168.9.14 255.255.255.0
user@GUARD-conf-if-giga3.9# no shutdown
user@GUARD-conf-if-giga3.9# exit
```

ステップ 5　Guard モジュールでトラフィックの宛先変更を設定するには、次のコマンドを入力します。

```
user@GUARD# conf term
user@GUARD-conf# diversion hijacking receive-via-vlan 8
user@GUARD-conf# diversion injection 192.168.252.0 255.255.255.0 nexthop 192.168.9.3
```

ステップ 6　次のいずれかの方法を使用して、トラフィック注入を設定します。

- ゾーンに直接トラフィックを注入する（「トラフィックの直接注入」の項を参照）。
- GRE または IPIP トンネルを介してゾーンにトラフィックを注入する（「トンネルを介したトラフィック注入」の項を参照）。

トラフィックの直接注入

スーパーバイザ エンジンで次のコマンドを入力して、ゾーンへのルートを指定するために VRF テーブルにスタティック ルートを追加することによって、トラフィックをゾーンに直接注入できます。

```
Sup(config)# ip route vrf Guard-vrf 192.168.252.0 255.255.255.0 192.168.250.2 global
```

global キーワードは、ネクストホップ ルータ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。

または、VRF ごとに特定のルーティング プロトコル インスタンスを定義することもできます。たとえば、**address-family ipv4 vrf** コマンドを使用すると、VRF の特定の BGP インスタンスを作成できます。

トンネルを介したトラフィック注入

トンネルを介したトラフィック注入を設定するには、次の手順を実行します。

ステップ 1　次のコマンドを入力して、スーパーバイザ エンジン上にトンネルを設定します。

（注）　次の例では、GRE トンネルを使用します。

```
Sup# conf term
Sup(config)# interface tunnel5
Sup(config-if)# ip address 192.168.145.2 255.255.255.252
Sup(config-if)# tunnel source 192.168.8.3
Sup(config-if)# tunnel destination 192.168.7.1
```

ステップ 2　次のコマンドを入力して、ネクストホップ ルータにトンネルの終端を設定します。

```
Router# conf term
Router(config)# interface tunnel5
Router(config-if)# ip address 192.168.145.1 255.255.255.252
Router(config-if)# tunnel source 192.168.7.1
Router(config-if)# tunnel destination 192.168.8.3
```

ステップ 3　次のコマンドを入力して、ゾーンへのルートを指定する VRF テーブルに、スーパーバイザ エンジン上でのスタティック ルートを追加します。

```
Sup(config)# ip route vrf Guard-vrf 192.168.252.0 255.255.255.0 192.168.145.1 global
```

global キーワードは、ネクストホップ ルータ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。

Guard モジュールのネットワーク設定の検証

3 Gbps 動作の場合にのみ、Guard モジュールはネットワーク設定を検証し、3 つのインターフェイス ポートが正しく設定およびアクティブにされていることを確認します。検証プロセスの間、Guard モジュールは次のネットワーク設定パラメータをチェックします。

- データ トラフィック VLAN の設定：Guard モジュールは、トラフィックの宛先変更用に設定（**diversion hijacking** コマンドまたは **diversion injection** コマンドを使用）した VLAN ごとに、次の設定パラメータを確認します。
  - 各 VLAN は、3 つのインターフェイスすべてで定義されます。
  - 各 VLAN は、インターフェイスのそれぞれで異なる IP アドレスを使用して設定されます。IP アドレスは同じサブネット上に存在する必要があります。

  VLAN を設定する方法の詳細については、P.3-9 の「Guard モジュールのインターフェイスでの VLAN の設定」を参照してください。
- 物理インターフェイスの設定：Guard モジュールは、次のインターフェイス設定パラメータを確認します。
  - データ トラフィックでネイティブ VLAN が使用されている場合は、3 つのインターフェイスのすべてが IP アドレスを指定して設定されます。各 IP アドレスは固有の値で、同じサブネットに属します。
  - 3 つのインターフェイスのすべてがアクティブ（**no shutdown** コマンドを使用）です。

  物理インターフェイスを設定する方法の詳細については、P.3-8 の「物理インターフェイスの設定」を参照してください。
- プロキシ設定：各物理インターフェイスは、少なくとも 1 つのプロキシを使用して設定されます。

  プロキシ アドレスを定義する方法の詳細については、P.3-13 の「プロキシ IP アドレスの設定」を参照してください。
- スタティック ルート：トラフィック注入のネクストホップ宛先に向けたスタティック ルートです。

  スタティック ルートを設定する方法の詳細については、P.5-9 の「トラフィック注入の設定」を参照してください。

Guard モジュールは、ゾーン保護またはラーニング プロセスがアクティブにされる場合にはいつでも、ネットワーク設定を自動的に検証します。Guard モジュールに対して、ネットワーク設定を検証するよう手動で要求することもできます。

この項では、次のトピックについて取り上げます。

ネットワーク設定の手動検証

グローバル モードまたは設定モードで **validate network-config** コマンドを使用することにより、ネットワーク設定を検証するよう Guard モジュールに対して手動で要求することができます。

次の例は、設定モードでネットワーク設定を検証する方法を示しています。

```
admin@rhTWJaffa-conf#validate network-config
Interfaces and vlans configuration is valid
Proxy configuration is valid
```

自動検証アクションの設定

ゾーン保護をアクティブにすると、Guard モジュールはネットワーク設定を自動的に検証します。設定問題が検出されると、Guard モジュールは、警告を発するかゾーン保護のアクティブ化に失敗します。ネットワーク設定に問題が存在する場合に Guard モジュールによって実行されるアクションを設定するには、設定モードで次のコマンドを使用します。

validate-action network-config {**activation-fail** | **activation-warn**}

表 5-6 に、**validate-action network-config** コマンドのキーワードを示します。

表 5-6　validate-action network-config コマンドのキーワード

パラメータ	説明
activation-fail	ネットワーク設定に問題が存在する場合に、Guard モジュールがゾーンをアクティブにしないように指定します。
activation-warn	ネットワーク設定に問題が存在する場合に、Guard モジュールが警告を発するように指定します。