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。この章は、次の項で構成されています。

Catalyst 6500 シリーズ スイッチまたは 7600 シリーズ ルータに Cisco Anomaly Guard Module（Guard モジュール）をインストールできます。詳細については、P.1-2 の「Cisco Anomaly Guard Module について」を参照してください。

Guard モジュールは攻撃を検出すると、ゾーンのトラフィックを自分宛に宛先変更します。Guard モジュールはデータ フローを分析し、すべての DDoS 要素をブロックし、宛先変更されたストリームから悪意のあるパケットを除去し、正当なトラフィックを元の宛先に転送して、目的のゾーンに流れることができるようにします。

ラーニング プロセスをアクティブにすると、Guard モジュールはゾーンのトラフィックを自分宛に宛先変更します。Guard モジュールは、トラフィックを分析して、保護ポリシーを作成し、変更は加えずに、トラフィックをゾーンのメイン トラフィック パスに戻します。

ゾーン トラフィックを Guard モジュールに宛先変更してからメインのデータ パスに戻すサイクル全体は、宛先変更プロセスと呼ばれます。攻撃の疑いがない場合は、宛先変更プロセスをアクティブにする必要はなく、Guard モジュールはゾーン トラフィックを監視しません。

トラフィックの宛先変更について

宛先変更には、2 つのタスクが含まれます。

- ハイジャック：Guard　モジュールがゾーンを保護している場合、Guard　モジュールはゾーン トラフィックのルーティングを変更して、トラフィックが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て Guard モジュールに流れるようにします。
- 注入：Guard モジュールは、正当なトラフィックを元のデータ パスに戻します。

この項では、次のトピックについて取り上げます。

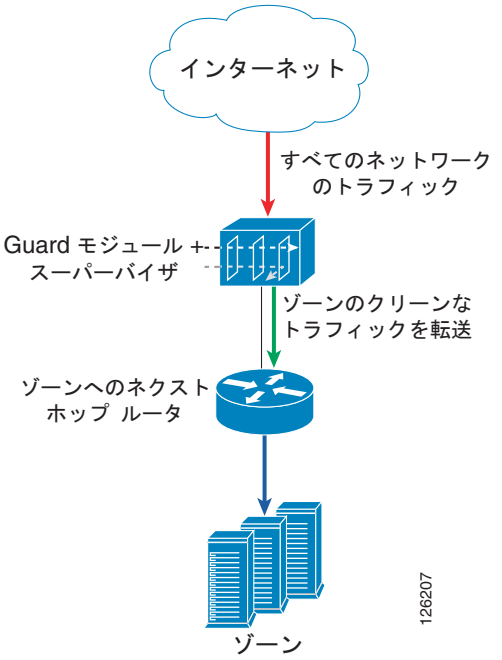
- ネットワーク設定
- 宛先変更のメカニズムについて

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。

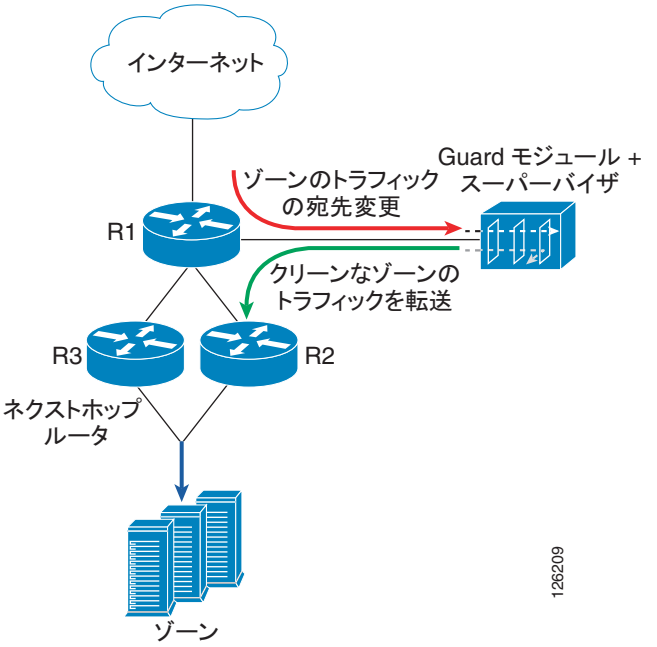
- インライン ネットワーク設定での Guard モジュールの設定：メイン パスに存在するスイッチまたはルータに Guard モジュールを設置します（つまり、ゾーン トラフィックはすでにこのスイッチまたはルータを通過しています）。この設定では、Guard モジュールは、スーパーバイザ エンジンのオンボード ルーティング テーブルにスタティック ルートを追加することで、ゾーン トラフィックをハイジャックして、正当なトラフィックを元の宛先に再び注入します。図 5-1 に、インライン ネットワーク設定の例を示します。

図 5-1　　インライン ネットワーク設定



- アウトオブパス ネットワーク設定での Guard モジュールの設定：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、ラインの外側にあるスイッチまたはルータに Guard モジュールを設置します。この設定では、ゾーン トラフィックはゾーンの通常のラインからスイッチまたはルータにハイジャックされています。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

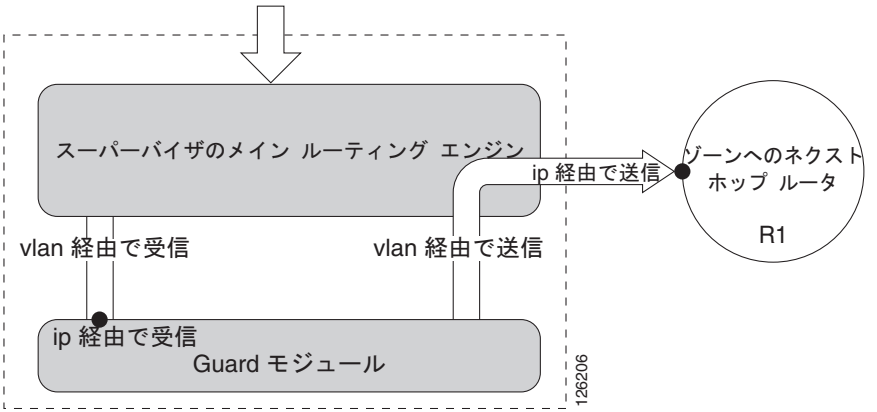
Guard モジュールの宛先変更設定は、グローバルで、すべてのゾーンに適用されます。宛先変更設定は、パケットを各サブネットにルーティングする方法を定義したり、ハイジャックと注入の両方に必要なルートを定義します。Guard モジュールがゾーンを保護している場合、またはユーザがラーニング プロセスをアクティブにする場合、Guard モジュールは宛先変更の設定とゾーンの定義を確認し、そのゾーンを宛先とするトラフィックを宛先変更する方法と、トラフィックをゾーンのメイン トラフィック パスに再び注入する方法を判別します。

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。

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



（注） Receive-via-vlan および Send-via-vlan に同じ VLAN ID 番号を設定することができます。

この項では、次のトピックについて取り上げます。

- ハイジャック パラメータの設定
- 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。Guard モジュールは receive-via-ip IP アドレスを使用して、この VLAN でゾーン トラフィックを受信します。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。

特定のハイジャック 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 モジュールのインターフェイス giga2 に定義された VLAN ID に動的に設定され、receive-via-ip はその VLAN の IP アドレスに設定されます。VLAN が定義されていない場合、VLAN ID は 1 に設定され、receive-via-ip は giga2 インターフェイスの IP アドレスに設定されます。

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.5-7 の「注入パラメータの設定」を参照してください。

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* | **weight** *weight*}

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

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 トラフィックを転送する Guard モジュールの IP アドレス。
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。
weight *weight*	宛先変更ハイジャック ルートの重み。デフォルト値は 1 です。

デフォルト値を復元する場合は、**no diversion hijacking** コマンドを入力します。

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。

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 5-2 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 5-2　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 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*	next-hop ルータ 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 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。

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 5-3 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 5-3　diversion injection hijacking コマンドの引数

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 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*	next-hop ルータ 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）。
hijacking	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 トラフィックを転送する Guard モジュールの IP アドレス。
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。
weight *weight*	宛先変更ハイジャック ルートの重み。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化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、モジュールがインストールされているスロットの番号を指定します。

次の例は、スーパーバイザ エンジン上に Guard モジュールがアドバタイズしたルートを表示する方法と、ルートの例を表示します。

```
Sup# show anomaly-guard module 9 advertised-route
RHI routes added by slot 9
    ip  masknexthopvlanweight
    ------------------------------------------------------
A   192.168.252.8255.255.255.0192.168.8.1081
```

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
C    192.168.8.0/24 is directly connected, Vlan8
S    192.168.252.8/32 [1/0] via 192.168.8.10, 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、Guard モジュールはゾーンのクリティカル パスに常駐するスイッチまたはルータに設置されます。つまり、ゾーンが Guard モジュールによって保護され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。

ハイジャックの設定

宛先変更を設定する場合、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.5-6 の「ハイジャック パラメータの設定」を参照してください。

注入の設定

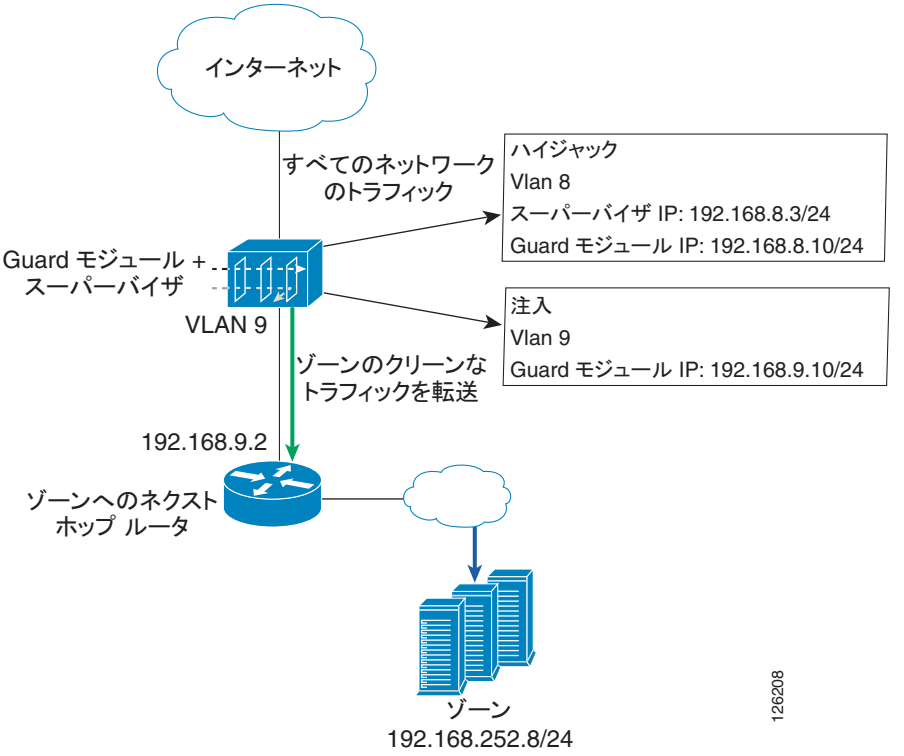
正当なトラフィックを元のデータ パスに戻す場合は、レイヤ 2 またはレイヤ 3 のトラフィック注入を設定できます。詳細については、P.5-24 の「トラフィック注入方式について」を参照してください。

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）　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 5-4　　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



- 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。

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 2 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 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 2
user@GUARD-conf-if-giga2# no shutdown
user@GUARD-conf-if-giga2# exit
user@GUARD-conf# interface giga 2.8
user@GUARD-conf-if-giga2.8# ip address 192.168.8.10 255.255.255.0
user@GUARD-conf-if-giga2.8# no shutdown
user@GUARD-conf-if-giga2.89# exit
user@GUARD-conf#interface giga 2.9
user@GUARD-conf-if-giga2.9# ip address 192.168.9.10 255.255.255.0
user@GUARD-conf-if-giga2.9# no shutdown
user@GUARD-conf-if-giga2.9# exit
```

ステップ 3　次のコマンドを入力することで、Guard モジュール上に宛先変更を設定します。

```
user@GUARD# conf term
user@GUARD-conf# diversion hijacking receive-via-ip 192.168.8.10
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化します。

詳細については、P.6-15 の「Guard モジュールの Cisco Traffic Anomaly Detector Module 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  masknexthopvlanweight
    ------------------------------------------------------
A   192.168.252.0255.255.255.128192.168.8.1081
A   192.168.252.128255.255.255.128192.168.8.1081
```

（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
...
192.168.252.0/24 is variably subnetted, 3 subnets, 2 masks
S       192.168.252.0/25 [1/0] via 192.168.8.10, Vlan8
S       192.168.252.128/25 [1/0] via 192.168.8.10, 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。

ハイジャックの設定

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.5-6 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 BGP（EBGP または IBGP）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 MSFC を設定する必要があります。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。

注入の設定

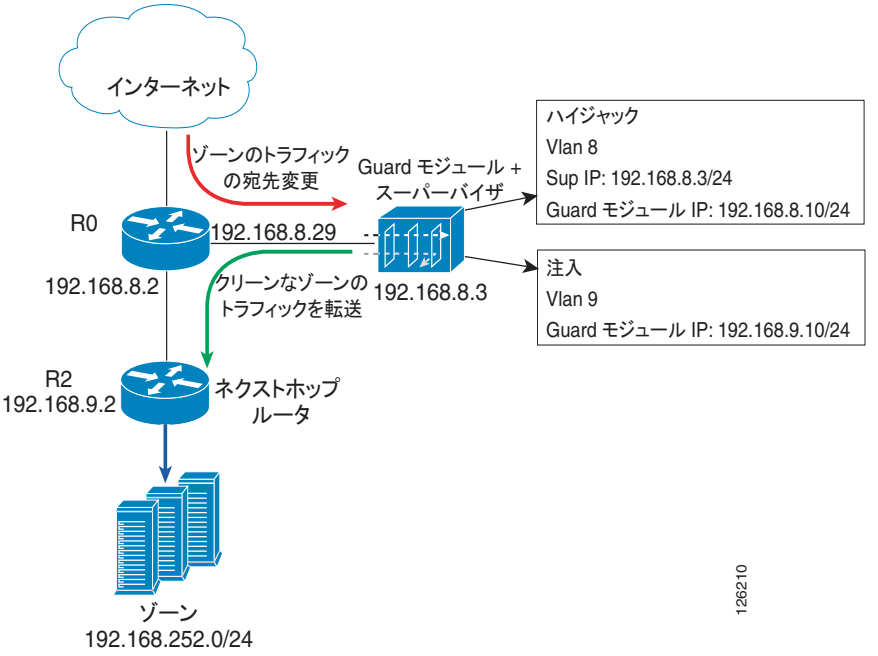
正当なトラフィックを元のデータ パスに戻す場合は、レイヤ 2 またはレイヤ 3 のトラフィック注入を設定できます。詳細については、P.5-24 の「トラフィック注入方式について」を参照してください。

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） 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



- 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。

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、設定例で示す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 2 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 access vlan 9
Sup(config-if)# switchport mode access
```

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)# 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
```

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 PERMIT_GUARD_ONLY
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 2.8
user@GUARD-conf-if-giga2.8# ip address 192.168.8.10 255.255.255.0
user@GUARD-conf-if-giga2.8# no shutdown
user@GUARD-conf-if-giga2.8# exit
user@GUARD-conf# interface giga 2.9
user@GUARD-conf-if-giga2.9# ip address 192.168.9.10 255.255.255.0
user@GUARD-conf-if-giga2.9# no shutdown
user@GUARD-conf-if-giga2.9# exit
```

ステップ 5　次のコマンドを入力することで、Guard モジュール上に宛先変更を設定します。

```
user@GUARD# conf term
user@GUARD-conf# diversion hijacking receive-via-ip 192.168.8.10
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化します。

詳細については、P.6-15 の「Guard モジュールの Cisco Traffic Anomaly Detector Module 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  masknexthopvlanweight
    ------------------------------------------------------
A   192.168.252.8255.255.255.0192.168.8.1081
```

（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
S       192.168.252.128/25 [1/0] via 192.168.8.10, 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
.
.
.
    NetworkNext HopMetric LocPrfWeightPath
*>  192.168.252.0/24192.168.9.200100 ?
```

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
.
.
.
    NetworkNext HopMetric LocPrfWeightPath
*>  192.168.252.0/25192.168.8.30055 ?
*>  192.168.252.128/25192.168.8.30055 ?

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

このトポロジでは、正当なトラフィックを元の宛先に戻すために、Guard モジュールが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 ARP 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.5-7 の「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.5-12 の「インライン ネットワーク設定の例」および P.5-18 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

このトポロジでは、正当なトラフィックを元の宛先に再び注入するために、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.5-12 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。

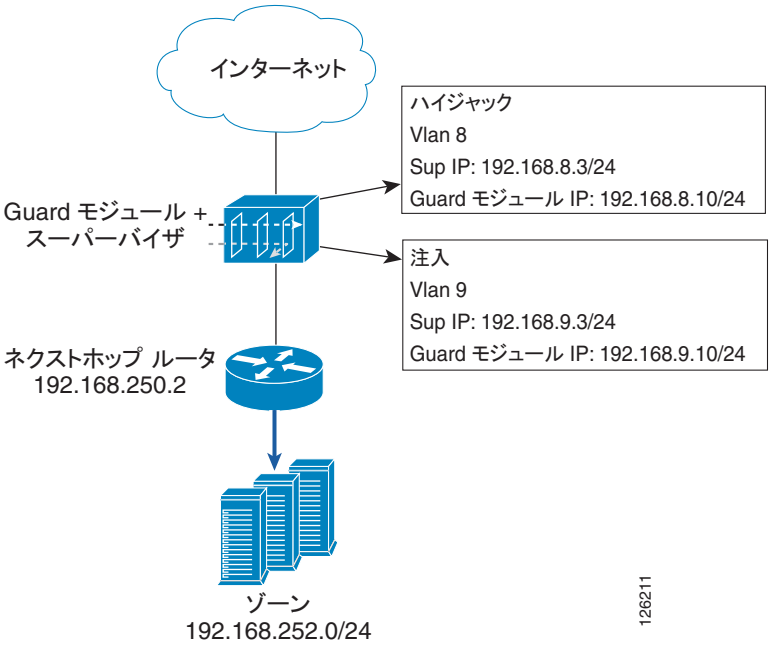
protect コマンドまたは **learning** コマンドを入力してゾーンをアクティブにする場合、Guard モジュールは、ゾーンへの最良のパスとしてリストされるようにルーティング テーブルを変更します（ルーティング テーブルは、ネットワーク トポロジに応じて、スーパーバイザ エンジンのオンボード ルーティング テーブルまたは隣接ルータのルーティング テーブルのどちらかです）。Guard モジュールが正当なトラフィックをトラフィックのハイジャック元に戻す場合、ルーティング ループが発生することがあります。ルーティング ループが発生しないようにするには、ルーティング規則を Guard モ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



VRF 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。

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.5-29 の「直接注入」および P.5-30 の「トンネルを介した注入」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 2 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 2.8
user@GUARD-conf-if-giga2.8# ip address 192.168.8.10 255.255.255.0
user@GUARD-conf-if-giga2.8# no shutdown
user@GUARD-conf-if-giga2.8# exit
user@GUARD-conf# interface giga 2.9
user@GUARD-conf-if-giga2.9# ip address 192.168.9.10 255.255.255.0
user@GUARD-conf-if-giga2.9# no shutdown
user@GUARD-conf-if-giga2.9# exit
```

ステップ 5　次のコマンドを入力することで、Guard モジュール上に宛先変更を設定します。

```
user@GUARD# conf term
user@GUARD-conf# diversion hijacking receive-via-ip 192.168.8.10
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、注入を設定します。

- ゾーンに直接トラフィックを注入
- 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

詳細については、P.5-29 の「直接注入」および P.5-30 の「トンネルを介した注入」を参照してください。

直接注入

スーパーバイザ エンジン上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 VRF テーブルに、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
192.168.250.2 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。

トンネルを介した注入

トンネルを介した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。