ポリシーベースルーティング

この章では、ポリシーベースルーティング（PBR）をサポートするように ASA を設定する方法について説明します。この項では、ポリシーベースルーティング、PBR のガイドライン PBR の設定について説明します。

ポリシーベース ルーティングについて

従来のルーティングは宛先ベースであり、パケットは宛先 IP アドレスに基づいてルーティングされます。ただし、宛先ベースのルーティング システムでは特定トラフィックのルーティングを変更することが困難です。ポリシーベースルーティング（PBR）では、宛先ネットワークではなく条件に基づいてルーティングを定義できます。PBR では、送信元アドレス、送信元ポート、宛先アドレス、宛先ポート、プロトコル、またはこれらの組み合わせに基づいてトラフィックをルーティングできます。

ポリシーベース ルーティング：

- 区別したトラフィックに Quality of Service（QoS）を提供できます。
- 低帯域幅、低コストの永続パスと、高帯域幅、高コストのスイッチドパスに、インタラクティブ トラフィックとバッチ トラフィックを分散できます。
- インターネット サービス プロバイダーやその他の組織が、さまざまなユーザー セットから発信されるトラフィックを、適切に定義されたインターネット接続を経由してルーティングできます。

ポリシーベース ルーティングには、ネットワーク エッジでトラフィックを分類およびマークし、ネットワーク全体で PBR を使用してマークしたトラフィックを特定のパスに沿ってルーティングすることで、QoS を実装する機能があります。これにより、宛先が同じ場合でも、異

なる送信元から送信されるパケットを別のネットワークにルーティングすることができます。これは、複数のプライベート ネットワークを相互接続する場合に役立ちます。

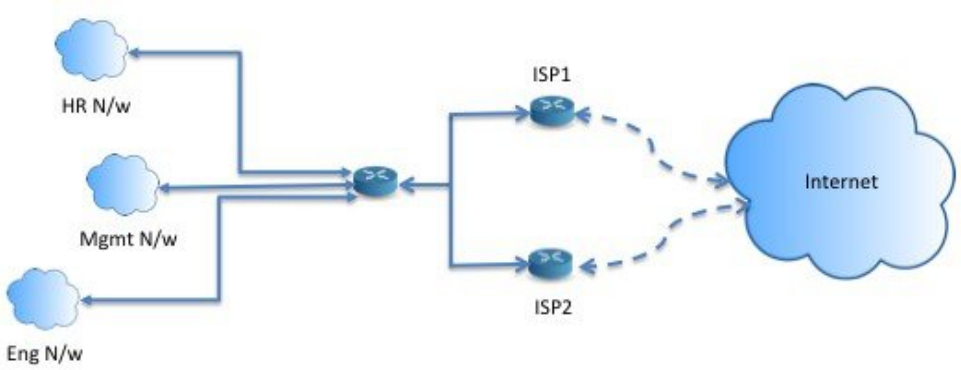
ポリシーベース ルーティングを使用する理由

ロケーション間に 2 つのリンクが導入されている企業を例に説明します。1 つのリンクは高帯域幅、低遅延、高コストのリンクであり、もう 1 つのリンクは低帯域幅、高遅延、低コストのリンクです。従来のルーティング プロトコルを使用する場合、高帯域幅リンクで、リンクの（EIGRP または OSPF を使用した）帯域幅/遅延の特性により実現するメトリックの節約に基づいて、ほぼすべてのトラフィックが送信されます。PBR では、優先度の高いトラフィックを高帯域幅/低遅延リンク経由でルーティングし、その他のすべてのトラフィックを低帯域幅/高遅延リンクで送信します。

ポリシーベース ルーティングの用途のいくつかを以下に示します。

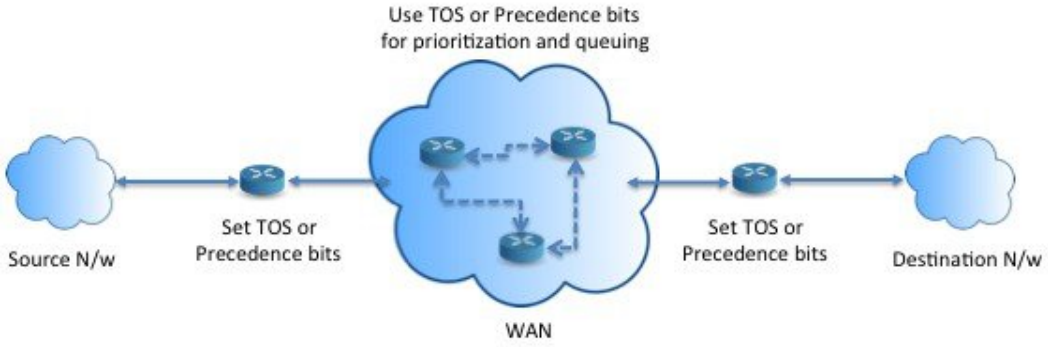
同等アクセスおよび送信元依存ルーティング

このトポロジでは、HR ネットワークと管理ネットワークからのトラフィックは ISP1 を経由するように設定し、エンジニアリング ネットワークからのトラフィックは ISP2 を経由するように設定できます。したがって、ここに示すように、ネットワーク管理者は、ポリシーベース ルーティングを使用して同等アクセスおよび送信元依存ルーティングを実現できます。



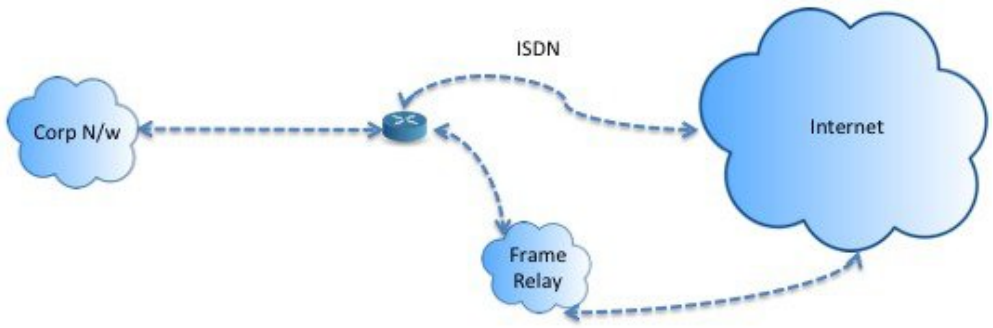
QoS

ネットワーク管理者は、ポリシーベース ルーティングでパケットにタグを付けることにより、ネットワーク トラフィックをネットワーク境界でさまざまなサービス クラスのために分類し、プライオリティ、カスタム、または重み付け均等化のキューイングを使用してそれらのサービス クラスをネットワークのコアに実装できます（下の図を参照）。この設定では、バックボーン ネットワークのコアの各 WAN インターフェイスでトラフィックを明示的に分類する必要がなくなるため、ネットワーク パフォーマンスが向上します。



コスト節約

組織は、特定のアクティビティに関連付けられている一括トラフィックを転送して、帯域幅が高い高コストリンクの使用を短時間にし、さらにここに示すようにトポロジを定義することで帯域幅が低い低コスト リンク上の基本的な接続を継続できます。



ロード シェアリング

ECMP ロード バランシングによって提供されるダイナミックなロード シェアリング機能に加え、ネットワーク管理者は、トラフィックの特性に基づいて複数のパス間にトラフィックを分散するためのポリシーを実装できます。

たとえば、同等アクセスおよび送信元依存ルーティングのシナリオに示すトポロジでは、管理者は、ISP1 を経由する HR netto からのトラフィックと ISP2 を経由するエンジニアリング ネットワークからのトラフィックをロード シェアするようにポリシーベース ルーティングを設定できます。

PBR の実装

ASA は、ACL を使用してトラフィックを照合してから、トラフィックのルーティングアクションを実行します。具体的には、照合のために ACL を指定するルート マップを設定し、次にそのトラフィックに対して1つ以上のアクションを指定します。最後に、すべての着信トラフィックに PBR を適用するインターフェイスにルートマップを関連付けます。

（注） 設定に進む前に、特に NAT と VPN が使用されている場合に、非対称ルーティングによって引き起こされる予期しない動作を回避するために、各セッションの入力トラフィックと出力トラフィックが同じ ISP 側のインターフェイスを通過することを確認してください。

ポリシーベース ルーティングのガイドライン

ファイアウォール モード

ルーテッド ファイアウォール モードでのみサポートされています。トランスペアレント ファイアウォール モードはサポートされません。

フロー別のルーティング

ASA はフロー別にルーティングを実行するため、ポリシー ルーティングは最初のパケットに適用され、その結果決定したルーティングが、そのパケットに対して作成されたフローに格納されます。同一接続に属する後続のパケットはすべてこのフローと照合され、適切にルーティングされます。

出力ルート ルックアップに適用されない PBR ポリシー

ポリシーベース ルーティングは入力専用機能です。つまり、この機能は新しい着信接続の最初のパケットだけに適用され、この時点で接続のフォワード レグの出力インターフェイスが選択されます。着信パケットが既存の接続に属している場合、または NAT が適用されない場合には、PBR がトリガーされないことに注意してください。

初期トラフィックに適用されない PBR ポリシー

（注） 初期接続とは、送信元と宛先の間で必要になるハンドシェイクが完了していない状態を指します。

新しい内部インターフェイスが追加され、一意のアドレスプールを使用して新しい VPN ポリシーが作成されると、新しいクライアントプールの送信元に一致する外部インターフェイスに PBR が適用されます。そのため、PBR はクライアントからのトラフィックを新しいインターフェイスの次のホップに送信します。ただし、PBR は、クライアントへの新しい内部インターフェイスルートとの接続をまだ確立していないホストからのリターントラフィックには関与しません。したがって、有効なルートがないため、ホストから VPN クライアントへのリターントラフィック、具体的には VPN クライアントの応答はドロップされます。内部インターフェイスにおいて、よりメトリックの高い重み付けされたスタティックルートを設定する必要があります。

クラスタ

- クラスタリングがサポートされています。
- クラスタのシナリオでは、スタティック ルートまたはダイナミック ルートがない場合、ip-verify-reverse パスを有効にした非対称トラフィックはドロップされる可能性があります。したがって、ip-verify-reverse パスを無効にすることが推奨されます。

IPv6 のサポート

IPv6 はサポートされます。

パスモニタリングのガイドライン

インターフェイスでパスモニタリングを設定するうえでのガイドラインは、次のとおりです。

- インターフェイスにはインターフェイス名が必要です。
- 管理専用インターフェイスには、パスモニタリングを設定できません。パスモニタリングを設定するには、[このインターフェイスを管理専用にする（Dedicate this interface to management only）] チェックボックスをオフにする必要があります。
- パスモニタリングは、トランスペアレントまたはマルチコンテキスト システム モードのデバイスではサポートされません。
- 自動モニタリングタイプ（auto、auto4、および auto6）は、トンネルインターフェイスではサポートされません。
- パスモニタリングは、次のインターフェイスには設定できません。
  - BVI
  - ループバック
  - DVTI

その他のガイドライン

- ルート マップ関連の既存のすべての設定の制限事項が引き続き適用されます。
- ポリシーベースルーティングには、一致ポリシーリストを含むルートマップを使用しないでください。一致ポリシーリストは BGP にのみ使用されます。

ポリシーベース ルーティングの設定

ルート マップは、1 つ以上のルート マップ文で構成されます。文ごとに、シーケンス番号と permit 句または deny 句が付加されます。各ルート マップ文には、match コマンドと set コマンドが含まれています。match コマンドは、パケット データに適用される一致基準を示します。set コマンドは、パケットに対して実行されるアクションを示します。

- IPv4 と IPv6 の両方の match/set 句でルート マップを設定した場合、または IPv4 および IPv6 トラフィックを照合する統合 ACL を使用した場合、宛先 IP のバージョンに基づいた set アクションが適用されます。
- 複数のネクストホップまたはインターフェイスを set アクションとして設定すると、使用できる有効なオプションが見つかるまですべてのオプションが順に評価されます。設定された複数のオプション間のロード バランシングは実行されません。
- verify-availability オプションは、マルチ コンテキスト モードではサポートされません。

手順

ステップ 1 スタンドアロンまたは拡張アクセス リストを定義します。

access-list *name* **standard** {**permit** | **deny**} {**any4** | **host** *ip_address* | *ip_address mask*}

access-list *name* **extended** {**permit** | **deny**} *protocol source_and_destination_arguments*

例：

```
ciscoasa(config)# access-list testacl extended permit ip
10.1.1.0 255.255.255.0 10.2.2.0 255.255.255.0
```

標準 ACL を使用する場合、照合は宛先アドレスに対してのみ行われます。拡張 ACL を使用する場合、送信元、宛先、またはその両方に対して照合を行えます。

拡張 ACL では、IPv4、IPv6、アイデンティティ ファイアウォール、または Cisco TrustSec パラメータを指定できます。ネットワーク サービス オブジェクトを含めることもできます。完全な構文については、ASA コマンド リファレンスを参照してください。

ステップ 2 ルート マップ エントリを作成します。

route-map *name* {**permit** | **deny**} [*sequence_number*]

例：

```
ciscoasa(config)# route-map testmap permit 12
```

ルート マップのエントリは順番に読み取られます。この順序は、*sequence_number* 引数を使用して指定できます。この引数で指定しなければ、ルートマップエントリを追加した順序が ASA で使用されます。

ACL には、固有の permit および deny 文も含まれます。ルート マップと ACL が permit/permit で一致する場合、ポリシーベース ルーティング処理が続行されます。permit/deny で一致する場合、このルート マップでの処理が終了し、別のルート マップがチェックされます。それでも結果が permit/deny であれば、通常のルーティング テーブルが使用されます。deny/deny で一致する場合、ポリシーベース ルーティング処理が続行されます。

（注） permit または deny アクションとシーケンス番号なしでルート マップを設定した場合、このマップはデフォルトでアクションが permit で、シーケンス番号が 10 であると見なされます。

ステップ 3 アクセス リストを使用して適用される一致基準を定義します。

match ip address *access-list_name* [*access-list_name...*]

例：

```
ciscoasa(config-route-map)# match ip address testacl
```

ステップ 4 1 つ以上の set アクションを設定します。

- ネクストホップ アドレスを設定します。

  set {ip | ipv6} next-hop *ipv4_or_ipv6_address*

  複数のネクストホップ IP アドレスを設定できます。その場合、ルーティングできる有効なネクスト ホップ IP アドレスが見つかるまで、それらのアドレスが指定された順で評価されます。設定済みのネクストホップは、直接接続する必要があります。そうでなければ、set アクションが適用されません。

- デフォルトのネクストホップ アドレスを設定します。

  set {ip | ipv6} default next-hop *ipv4_or_ipv6_address*

  一致するトラフィックに対する通常のルート ルックアップが失敗すると、ASA はここで指定されたネクスト ホップ IP アドレスを使用してトラフィックを転送します。

- 再帰ネクスト ホップ IPv4 アドレスを設定します。

  set ip next-hop recursive *ip_address*

  set ip next-hop と **set ip default next-hop** はどちらも、ネクストホップが直接接続されたサブネット上に存在している必要があります。**set ip next-hop recursive** では、ネクストホップ アドレスが直接接続されている必要はありません。代わりにネクストホップ アドレスで再帰ルックアップが実行され、一致するトラフィックは、ルータで使用されているルーティング パスに従って、そのルート エントリで使用されているネクストホップに転送されます。

- ルート マップの次の IPv4 ホップが使用できるかどうかを確認します。

  set ip next-hop verify-availability *next-hop-address sequence_number* **track** *object*

  ネクスト ホップの到達可能性を確認するには、SLA モニター追跡オブジェクトを設定できます。複数のネクストホップの可用性を確認するために、複数の **set ip next-hop verify-availability** コマンドを異なるシーケンス番号と異なるトラッキング オブジェクトで設定できます。

- パケットの出力インターフェイスを設定します。

  set interface *interface_name*

  または

set interface null0

このコマンドにより、一致するトラフィックを転送するために使用するインターフェイスが設定されます。複数のインターフェイスを設定できます。その場合、有効なインターフェイスが見つかるまで、それらのインターフェイスが指定された順で評価されます。**null0** を指定すると、ルートマップと一致するすべてのトラフィックがドロップされます。指定されたインターフェイス（静的または動的のいずれか）経由でルーティングできる宛先のルートが存在している必要があります。

- インターフェイスのコストに基づいて出力インターフェイスを設定します。

  set adaptive-interface cost *interface_list*

  出力インターフェイスは、スペースで区切られたインターフェイスのリストから選択されます。インターフェイスのコストが同じである場合、アクティブ-アクティブ設定であり、出力インターフェイスでパケットがロードバランシング（ラウンドロビン）されます。コストが異なる場合、コストが最も低いインターフェイスが選択されます。インターフェイスは、アップしている場合にのみ考慮されます。次に例を示します。

  ```
  set adaptive-interface cost output1 output2
  ```

- デフォルトのインターフェイスを null0 に設定します。

  set default interface null0

  通常のルート ルックアップが失敗すると、ASA はトラフィックを null0 に転送し、トラフィックがドロップされます。

- IP ヘッダーに Don't Fragment（DF）ビット値を設定します。

  set ip df {0|1}

- パケットに Differentiated Services Code Point（DSCP）または IP プレシデンスの値を設定することによって、IP トラフィックを分類します。

  set {ip | ipv6} dscp *new_dscp*

（注） 複数の set アクションが設定されている場合、ASA は、これらを次の順序で評価します。 **set ip next-hop verify-availability; set ip next-hop**; **set ip next-hop recursive**; **set interface; set adaptive-interface cost**; **set ip default next-hop**; **set default interface**

ステップ 5 インターフェイスを設定して、インターフェイス コンフィギュレーション モードを開始します。

interface *interface_id*

例：

```
ciscoasa(config)# interface GigabitEthernet0/0
```

ステップ 6 ルートマップの基準として **set adaptive-interface cost** を使用する場合は、インターフェイスでコストを設定します。

policy-route cost *value*

値は 1 ー 65535 です。デフォルトは 0 です。この値は、コマンドの **no** バージョンを使用してリセットできます。値が小さいほど、プライオリティが高くなります。たとえば、1 は 2 よりも優先されます。

policy-route コストを設定し、ルートマップで **set adaptive-interface cost** コマンドを使用すると、出力トラフィックは、同じインターフェイスコストを持つ任意の選択されたインターフェイス間（アップしていると仮定）でラウンドロビン ロード バランシングされます。コストが異なる場合、コストの高いインターフェイスが、最もコストの低いインターフェイスへのバックアップとして使用されます。

たとえば、2 つの WAN リンクに同じコストを設定すると、これらのリンク間でトラフィックをロードバランシングして、パフォーマンスを向上させることができます。ただし、一方の WAN リンクの帯域幅が他方よりも高い場合は、高帯域幅リンクのコストを 1 に設定し、低帯域幅リンクを 2 に設定して、高帯域幅リンクがダウンしている場合にのみ低帯域幅リンクを使用します。

ステップ 7 インターフェイスのピアのモニタリングタイプを設定して、柔軟なメトリックを収集できます。

policy-route path-monitoring {**IPv4** | **IPv6** | **auto** | **auto4** | **auto6**}

それぞれの説明は次のとおりです。

- [自動（auto）]：自動 IPv4 と同じように、インターフェイスの IPv4 デフォルトゲートウェイ（存在する場合）に ICMP プローブを送信します。それ以外の場合は、自動 IPv6 と同じように、インターフェイスの IPv6 デフォルトゲートウェイに送信します。
- [ipv4]：モニタリングのために、指定されたピア IPv4 アドレス（ネクストホップ IP）に ICMP プローブを送信します。
- [ipv6]：モニタリングのために、指定されたピア IPv4 アドレス（ネクストホップ IP）に ICMP プローブを送信します。
- [auto4]：インターフェイスの IPv4 デフォルトゲートウェイに ICMP プローブを送信します。
- [auto6]：インターフェイスの IPv6 デフォルトゲートウェイに ICMP プローブを送信します。

例：

```
ciscoasa(config-if)# policy-route ?

interface mode commands/options:
  cost             set interface cost
  path-monitoring  Keyword for path monitoring
  route-map        Keyword for route-map
ciscoasa(config-if)# policy-route path-monitoring ?
interface mode commands/options:
  A.B.C.D     peer-ipv4
  X:X:X:X::X  peer-ipv6
  auto        Use remote peer IPv4/6 based on config
  auto4       Use only IPv4 address based on config
```

```
  auto6       Use only IPv6 address based on config

ciscoasa(config-if)# policy-route path-monitoring auto
```

インターフェイスでパスモニタリング設定をクリアするには、**clear path-monitoring** コマンドを使用します。

例：

```
clear path-montoring outside1
```

ステップ 8 ポリシーベース ルーティングを through-the-box トラフィック用に設定します。

`policy-route route-map` *route_map_name*

例：

```
ciscoasa(config-if)# policy-route route-map testmap
```

既存のポリシーベース ルーティング マップを削除するには、単にこのコマンドの **no** 形式を入力します。

例：

```
ciscoasa(config-if)# no policy-route route-map testmap
```

ポリシーベース ルーティングの例

以下のセクションでは、ルートマップの設定、ポリシーベース ルーティング（PBR）の例と、PBR の具体的な動作例を示します。

ルート マップ コンフィギュレーションの例

次の例では、アクションとシーケンスが指定されないため、暗黙的に permit のアクションと 10 のシーケンス番号が想定されます。

```
ciscoasa(config)# route-map testmap
```

次の例では、match 基準が指定されないため、暗黙的に match は「any」と見なされます。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10
```

この例では、<acl> と一致するすべてのトラフィックが、ポリシー ルーティングされ、外部インターフェイス経由で転送されます。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
```

```
ciscoasa(config-route-map)# set interface outside
```

次の例では、インターフェイスまたはネクストホップのアクションが設定されていないため、<acl>に一致するすべてのトラフィックのdf bitおよびdscpフィールドがコンフィギュレーションに従って変更され、通常のルーティングを使用して転送されます。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl>
set ip df 1
set ip precedence af11
```

次の例では、<acl_1> に一致するすべてのトラフィックがネクストホップ 1.1.1.10 を使用して転送され、<acl_2> に一致するすべてのトラフィックがネクストホップ 2.1.1.10 を使用して転送され、残りのトラフィックはドロップされます。「match」基準がない場合、暗黙的にmatchは「any」と見なされます。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address <acl_1>
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address <acl_2>

ciscoasa(config-route-map)# set ip next-hop 2.1.1.10
ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# set interface Null0
```

次の例では、ルートマップの評価は、（i）route-mapアクションpermitとaclアクションpermitがsetアクションを適用する、（ii）route-mapアクションdenyとaclアクションpermitが通常のルート ルックアップにスキップする、（iii）permit/denyのroute-mapアクションとaclアクションdenyが次のroute-mapエントリを続行するといったものになります。次のroute-mapエントリを使用できない場合は、通常のルート ルックアップにフォールバックします。

```
ciscoasa(config)# route-map testmap permit 10
ciscoasa(config-route-map)# match ip address permit_acl_1 deny_acl_2
ciscoasa(config-route-map)# set ip next-hop 1.1.1.10

ciscoasa(config)# route-map testmap deny 20
ciscoasa(config-route-map)# match ip address permit_acl_3 deny_acl_4
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10

ciscoasa(config)# route-map testmap permit 30
ciscoasa(config-route-map)# match ip address deny_acl_5
ciscoasa(config-route-map)# set interface outside
```

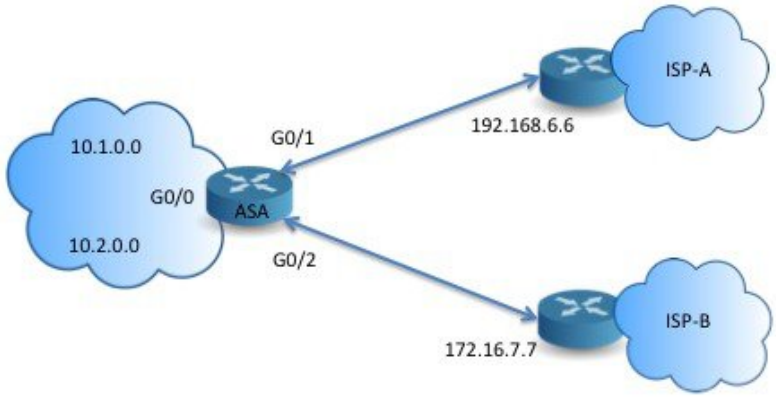
次の例では、複数のsetアクションを設定すると、それらのアクションが上記の順序で評価されます。setアクションのすべてのオプションが評価され、それらを適用できない場合にのみ、次のsetアクションが考慮されます。この順序設定により、すぐに使用可能な最短のネクストホップが最初に試行され、その後、次のすぐに使用可能な最短のネクストホップが試行される、といったようになります。

```
ciscoasa(config)# route-map testmap permit 10
```

```
ciscoasa(config-route-map)# match ip address acl_1
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.10 1 track 1
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.11 2 track 2
ciscoasa(config-route-map)# set ip next-hop verify-availability 1.1.1.12 3 track 3
ciscoasa(config-route-map)# set ip next-hop 2.1.1.10 2.1.1.11 2.1.1.12
ciscoasa(config-route-map)# set ip next-hop recursive 3.1.1.10
ciscoasa(config-route-map)# set interface outside-1 outside-2
ciscoasa(config-route-map)# set ip default next-hop 4.1.1.10 4.1.1.11
ciscoasa(config-route-map)# set default interface Null0
```

PBR の設定例

ここでは、次のシナリオ用に PBR を設定するために必要な設定の完全なセットについて説明します。



まず、インターフェイスを設定する必要があります。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# ip address 10.1.1.1 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif outside-1
ciscoasa(config-if)# ip address 192.168.6.5 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/2
ciscoasa(config-if)# no shutdown
ciscoasa(config-if)# nameif outside-2
ciscoasa(config-if)# ip address 172.16.7.6 255.255.255.0
```

次に、トラフィックを照合するためのアクセスリストを設定する必要があります。

```
ciscoasa(config)# access-list acl-1 permit ip 10.1.0.0 255.255.0.0
ciscoasa(config)# access-list acl-2 permit ip 10.2.0.0 255.255.0.0
```

必要な set アクションとともに、一致基準として上記のアクセスリストを指定することで、ルートマップを設定する必要があります。

```
ciscoasa(config)# route-map equal-access permit 10
ciscoasa(config-route-map)# match ip address acl-1
ciscoasa(config-route-map)# set ip next-hop 192.168.6.6

ciscoasa(config)# route-map equal-access permit 20
ciscoasa(config-route-map)# match ip address acl-2
ciscoasa(config-route-map)# set ip next-hop 172.16.7.7

ciscoasa(config)# route-map equal-access permit 30
ciscoasa(config-route-map)# set ip interface Null0
```

ここで、このルート マップをインターフェイスに接続する必要があります。

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map equal-access
```

ポリシー ルーティング設定を表示するには：

```
ciscoasa(config)# show policy-route
Interface                   Route map
GigabitEthernet0/0   equal-access
```

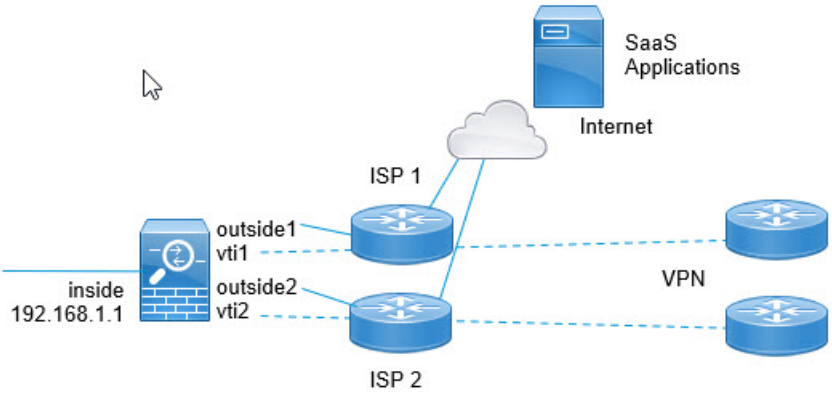
ソフトウェアデファインド WAN を使用したダイレクト インターネット アクセス

一般的な分散拠点ネットワークでは、サイト間 VPN を使用してブランチを企業のハブに接続します。すべての非ローカルトラフィックは、社内ネットワークに転送されます。社内ネットワークでは、必要に応じて内部サービスまたはインターネットに転送されます。

この設定により、企業のハブでボトルネックが発生します。一部のブランチトラフィックが Google 検索や Gmail などのインターネットサービス向けである場合、インターネットに転送する前に企業ネットワークに転送する必要はありません。

ポリシーベースルーティングを使用すると、企業ネットワークのサービスを必要としないトラフィックに対して、ブランチから直接のインターネットアクセスを設定できます。したがって、インターネットへのトラフィックは企業のハブに送信されず、ハブは企業ネットワークの内部サービス宛てのトラフィックのみを処理する必要があります。この設定により、ネットワーク全体のパフォーマンスとスループットが向上します。

次に、2 つの外部インターフェイスが異なるインターネット サービス プロバイダーに接続し、仮想トンネルインターフェイス（VTI）が企業ネットワークへのサイト間 VPN 接続を行う、次の設定の直接インターネットアクセスを設定する例を示します。この例では、選択した SaaS アプリケーション宛てのトラフィックをインターネットに転送し、企業ネットワークをバイパスする方法を示します。



始める前に

この例では、ブランチを企業ハブに接続するために、外部（WAN 側）インターフェイスで定義された仮想トンネルインターフェイス（VTI）を使用してサイト間 VPN がすでに定義されていて、正しく機能していることを前提としています。したがって、VTI インターフェイスにルーティングされるトラフィックは企業ネットワークに転送され、外部インターフェイスに直接ルーティングされるトラフィックはインターネットに転送されます。

また、DNS サーバ設定し、デバイスインターフェイスで DNS 解決を有効にしていることも前提としています。スヌーピングされるサーバを確認するには、**show dns trusted-source detail** コマンドを使用します。使用するサーバを制限する場合は、**no dns trusted-source** コマンドを使用して、選択したサーバのスヌーピングをオフにします。

手順

ステップ 1 ネットワーク サービス オブジェクトとグループを設定して、目的のトラフィックを定義します。

次の例では、Office365 と Webex を定義するオブジェクトを作成し、これらを含む SaaS_Applications オブジェクトグループを作成します。オブジェクトグループを作成する必要があります。アクセス コントロール エントリでオブジェクトを直接使用することはできません。

```
object network-service office365
    domain outlook.office365.com tcp eq 443
    domain onlineapps.live.com tcp eq 443
    domain skype.live.com tcp eq 443

object network-service webex
    domain webex.com tcp eq 443

object-group network-service SaaS_Applications
    network-service-member office365
    network-service-member webex
```

ステップ 2 目的のトラフィックと一致する拡張 ACL を作成します。

次の例では、内部ネットワークから SaaS アプリケーション オブジェクト グループへのトラフィックを照合します。

```
access-list DIA_traffic extended permit ip 192.168.1.0 255.255.255.0
object-group-network-service SaaS_Applications
```

ステップ 3 （任意）出力インターフェイスのコストを設定します。

output1 および output2 インターフェイスがすでに設定され、機能していると仮定すると、policy-route cost コマンドを追加するだけです。ラウンドロビン処理を使用して 2 つの出力 WAN リンク間でロードバランシングを行うようにシステムを設定する場合、この手順は任意です。ただし、アクティブ/バックアップ設定を作成する場合は、コストを設定する必要があります。この場合、ダウンしていない限り 1 つのリンクが使用されます。

次に、等コストのアクティブ/アクティブ設定の例を示します。

```
interface G0/0
  nameif outside1
  policy-route cost 1

interface G0/1
  nameif outside2
  policy-route cost 1
```

次に、output1 が優先リンクで、output2 は output1 がダウンしている場合にのみ使用される例を示します。

```
interface G0/0
  nameif outside1
  policy-route cost 1

interface G0/1
  nameif outside2
  policy-route cost 2
```

ステップ 4 拡張 ACL に一致するルートマップを作成し、それに応じてトラフィックを転送します。

次の例では、ACL を使用してトラフィックを照合し、適応インターフェイスのコストを使用してトラフィックを出力インターフェイスに転送します。

```
route-map mymap 10
  match ip address DIA_traffic
  set adaptive-interface cost outside1 outside2
```

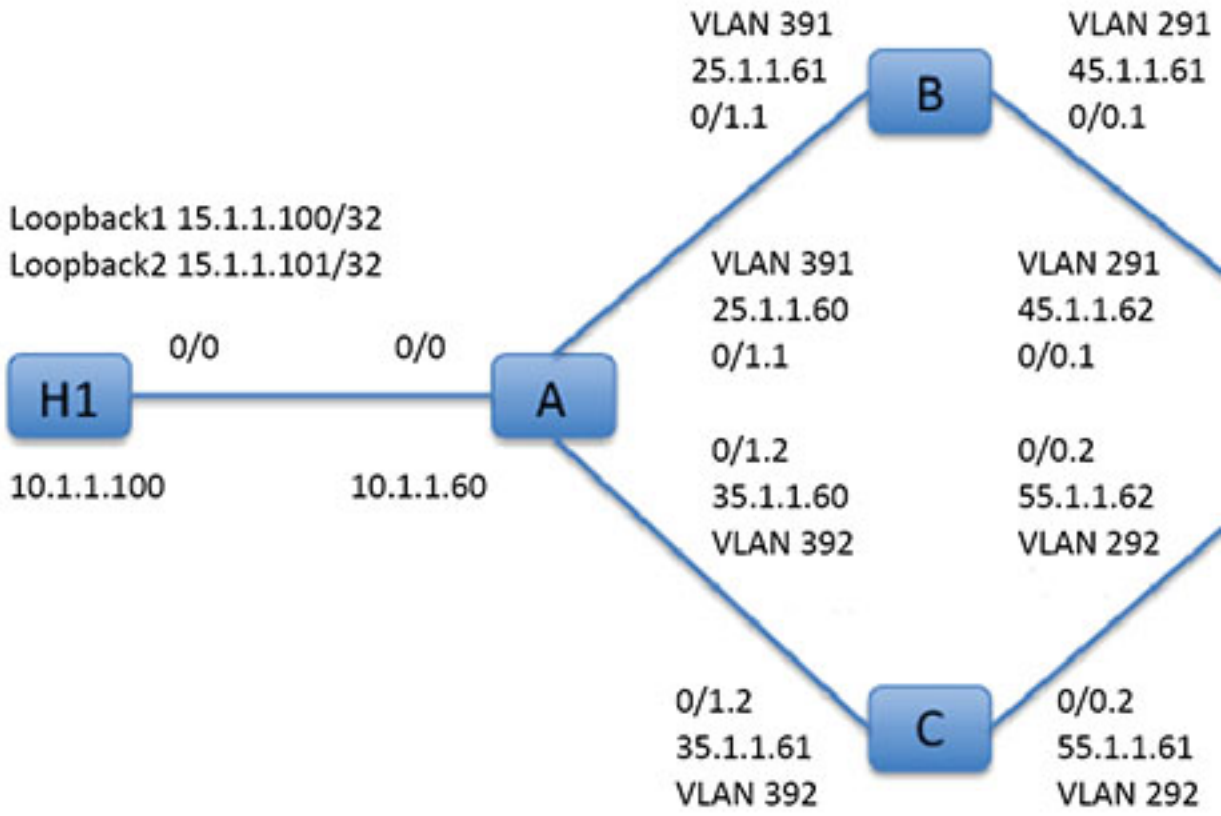
ステップ 5 SaaS トラフィックを外部インターフェイスに送信するために、入力インターフェイスでポリシーベースルーティングを設定します。

次の例では、ルートマップを内部インターフェイスに接続して、直接インターネットアクセスのポリシーベースルーティングを有効にします。

```
interface G1/0
  nameif inside
  policy-route route-map mymap
```

アクションでのポリシーベース ルーティング

このテスト設定を使用して、異なる一致基準および set アクションでポリシーベース ルーティングが設定され、それらがどのように評価および適用されるのかを確認します。



まず、セットアップに関係するすべてのデバイスの基本設定から始めます。ここで、A、B、C、および D は ASA デバイスを表し、H1 および H2 は IOS ルータを表します。

ASA-A：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 10.1.1.60 255.255.255.0
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
```

```
ciscoasa(config-if)# ip address 25.1.1.60 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1.2
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif dmz
ciscoasa(config-if)# security-level 50
ciscoasa(config-if)# ip address 35.1.1.60 255.255.255.0
```

ASA-B：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 45.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.1
ciscoasa(config-if)# vlan 391
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 25.1.1.61 255.255.255.0
```

ASA-C：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 55.1.1.61 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# no shut

ciscoasa(config)# interface GigabitEthernet0/1.2
ciscoasa(config-if)# vlan 392
ciscoasa(config-if)# nameif inside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 35.1.1.61 255.255.255.0
```

ASA-D：

```
ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# no shut

ciscoasa(config) #interface GigabitEthernet0/0.1
ciscoasa(config-if)# vlan 291
ciscoasa(config-if)# nameif inside-1
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 45.1.1.62 255.255.255.0
```

```
ciscoasa(config)# interface GigabitEthernet0/0.2
ciscoasa(config-if)# vlan 292
ciscoasa(config-if)# nameif inside-2
ciscoasa(config-if)# security-level 100
ciscoasa(config-if)# ip address 55.1.1.62 255.255.255.0

ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# nameif outside
ciscoasa(config-if)# security-level 0
ciscoasa(config-if)# ip address 65.1.1.60 255.255.255.0
```

H1：

```
ciscoasa(config)# interface Loopback1
ciscoasa(config-if)# ip address 15.1.1.100 255.255.255.255

ciscoasa(config-if)# interface Loopback2
ciscoasa(config-if)# ip address 15.1.1.101 255.255.255.255

ciscoasa(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.60
```

H2：

```
ciscoasa(config)# interface GigabitEthernet0/1
ciscoasa(config-if)# ip address 65.1.1.100 255.255.255.0

ciscoasa(config-if)# ip route 15.1.1.0 255.255.255.0 65.1.1.60
```

H1 から送信されるトラフィックをルーティングするように ASA-A で PBR を設定します。

ASA-A：

```
ciscoasa(config-if)# access-list pbracl_1 extended permit ip host 15.1.1.100 any

ciscoasa(config-if)# route-map testmap permit 10
ciscoasa(config-if)# match ip address pbracl_1
ciscoasa(config-if)# set ip next-hop 25.1.1.61

ciscoasa(config)# interface GigabitEthernet0/0
ciscoasa(config-if)# policy-route route-map testmap

ciscoasa(config-if)# debug policy-route
```

H1： ping 65.1.1.100 repeat 1 source loopback1

```
pbr: policy based route lookup called for 15.1.1.100/44397 to 65.1.1.100/0 proto 1
sub_proto 8 received on interface inside
pbr: First matching rule from ACL(2)
pbr: route map testmap, sequence 10, permit; proceed with policy routing
pbr: evaluating next-hop 25.1.1.61
pbr: policy based routing applied; egress_ifc = outside : next_hop = 25.1.1.61
```

パケットは、ルートマップのネクストホップアドレスを使用して想定どおりに転送されます。

ネクストホップを設定した場合、入力ルートテーブルで検索して設定したネクストホップに接続されたルートを特定し、対応するインターフェイスを使用します。この例の入力ルートテーブルを次に示します（一致するルート エントリが強調表示されています）。

```
in   255.255.255.255 255.255.255.255 identity
in   10.1.1.60       255.255.255.255 identity
in   25.1.1.60       255.255.255.255 identity
in   35.1.1.60       255.255.255.255 identity
in   10.127.46.17    255.255.255.255 identity
in   10.1.1.0        255.255.255.0   inside
in   25.1.1.0        255.255.255.0   outside
in   35.1.1.0        255.255.255.0   dmz
```

次に、ASA-A の dmz インターフェイスからの H1 loopback2 から送信されるパケットをルーティングするように ASA-A を設定します。

```
ciscoasa(config)# access-list pbracl_2 extended permit ip host 15.1.1.101 any

ciscoasa(config)# route-map testmap permit 20
ciscoasa(config-route-map)# match ip address pbracl
ciscoasa(config-route-map)# set ip next-hop 35.1.1.61

ciscoasa(config)# show run route-map
!
route-map testmap permit 10
  match ip address pbracl_1
  set ip next-hop 25.1.1.61
!
route-map testmap permit 20
  match ip address pbracl_2
  set ip next-hop 35.1.1.61
!
```

H1：ping 65.1.1.100 repeat 1 source loopback2

デバッグを示します。

```
pbr: policy based route lookup called for 15.1.1.101/1234 to 65.1.1.100/1234 proto 6
sub_proto 0 received on interface inside
pbr: First matching rule from ACL(3)
pbr: route map testmap, sequence 20, permit; proceed with policy routing
pbr: evaluating next-hop 35.1.1.61
pbr: policy based routing applied; egress_ifc = dmz : next_hop = 35.1.1.61
```

さらに、入力ルート テーブルから選択されたルートのエントリをここに示します。

```
in   255.255.255.255 255.255.255.255 identity
 in   10.1.1.60       255.255.255.255 identity
 in   25.1.1.60       255.255.255.255 identity
 in   35.1.1.60       255.255.255.255 identity
 in   10.127.46.17    255.255.255.255 identity
 in   10.1.1.0        255.255.255.0   inside
 in   25.1.1.0        255.255.255.0   outside
 in   35.1.1.0        255.255.255.0   dmz
```

ポリシーベース ルーティングの履歴

表 *1:* ルート マップの履歴

機能名	プラットフォームリリース	機能情報
PBR のパスモニタリングメトリック。	9.18(1)	PBR はメトリックを使用して、トラフィックを転送するための最適なパス（出力インターフェイス）を決定します。パスモニタリングは、メトリックが変更されたモニタリング対象インターフェースを PBR に定期的に通知します。PBR は、モニタリング対象インターフェイスの最新のメトリック値をパス モニタリング データベースから取得し、データパスを更新します。 新規/変更されたコマンド：**clear path-monitoring**、**policy-route**、**show path-monitoring**

機能名	プラットフォームリリース	機能情報
ポリシーベース ルーティング	9.4(1)	ポリシーベースルーティング（PBR）は、ACL を使用して指定された QoS でトラフィックが特定のパスを経由するために使用するメカニズムです。ACL では、パケットのレイヤ3およびレイヤ4 ヘッダーの内容に基づいてトラフィックを分類できます。このソリューションにより、管理者は区別されたトラフィックにQoSを提供し、低帯域幅、低コストの永続パス、高帯域幅、高コストのスイッチドパスの間でインタラクティブ トラフィックとバッチ トラフィックを分散でき、インターネット サービス プロバイダーとその他の組織は明確に定義されたインターネット接続を介して一連のさまざまなユーザーから送信されるトラフィックをルーティングできます。 **set ip next-hop verify-availability**、**set ip next-hop**、**set ip next-hop recursive**、**set interface**、**set ip default next-hop**、**set default interface**、**set ip df**、**set ip dscp**、**policy-route route-map**、**show policy-route**、**debug policy-route** の各コマンドが導入されました。
ポリシーベース ルーティングの IPv6 サポート	9.5(1)	ポリシーベース ルーティングで IPv6 アドレスがサポートされました。 次のコマンドが導入されました。**set ipv6 next-hop**、**set default ipv6-next hop**、**set ipv6 dscp**
ポリシーベース ルーティングの VXLAN サポート	9.5(1)	VNI インターフェイスでポリシーベースルーティングを有効にできるようになりました。 変更されたコマンドはありません。

機能名	プラットフォームリリース	機能情報
アイデンティティ ファイアウォールと Cisco TrustSec でのポリシーベース ルーティングのサポート	9.5(1)	アイデンティティ ファイアウォールと Cisco TrustSec を設定し、ポリシーベース ルーティングのルートマップでアイデンティティ ファイアウォールと Cisco TrustSec ACL を使用できるようになりました。 変更されたコマンドはありません。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。