



RADIUS 属性 104

RADIUS 属性 104 機能を使用すれば、RADIUS 認可プロファイル内でプライベートルート（属性 104）を指定できます。プライベートルートは、個々のインターフェイス上で受信されたパケットにのみ影響します。ルートはグローバルルーティングテーブルとは別に保存され、ルーティングプロトコルに埋め込まれて再配布されることはありません。

- [RADIUS 属性 104 の前提条件](#)（1 ページ）
- [RADIUS 属性 104 の制約事項](#)（2 ページ）
- [RADIUS 属性 104 に関する情報](#)（2 ページ）
- [RADIUS 属性 104 の適用方法](#)（3 ページ）
- [RADIUS 属性 104 の設定例](#)（6 ページ）
- [その他の参考資料](#)（6 ページ）
- [RADIUS 属性 104 の機能情報](#)（8 ページ）

RADIUS 属性 104 の前提条件

- シスコ RADIUS サーバを使用している必要があります。
- RADIUS の設定に精通している必要があります。
- ポリシーベース ルーティング（PBR）とプライベートルートに精通している必要があります。
- アクセス コントロール リスト（ACL）に精通している必要があります。
- RADIUS 属性 104 機能を使用する前に、RADIUS AAA 認可と RADIUS ルート ダウンロードを設定する必要があります。
- `F:\tips-migration` には以下のメモリ バイトが必要です。
 - 1 つのルート マップ：50 バイト
 - 1 つの `match-set` 句：600 バイト
 - 1 つの拡張 ACL：366 バイト
 - 属性 104 の数 N のメモリ要件は、ユーザ当たり $(600+366)*N+50 \approx 1000*N$ です。

RADIUS 属性 104 の制約事項

- インターフェイス上ですでに PBR がローカル（静的）に設定されている状態で、属性 104 を指定した場合は、ローカルに設定された PBR が無効になります。
- 疑似ネクストホップアドレスを使用する場合は、ネクストホップアドレスのルーティングテーブル内に、使用可能なルートが存在する必要があります。どのルートも使用できない場合は、パケットがポリシールーティングされません。
- ポリシールーティングは `match-set` 句を順序付けせず、最初の一致を優先するため、一致させたい順序で属性を指定する必要があります。
- メトリック番号は属性内で使用できません。

RADIUS 属性 104 に関する情報

ポリシーベース ルーティングの背景

PBR は、定義済みのポリシーに基づいて、データパケットを転送またはルーティングするためのメカニズムを提供します。ポリシーは、宛先アドレスではなく、サービスタイプ、送信元アドレス、優先順位、ポート番号、プロトコルタイプなどの他の要因に依存します。

ポリシーベース ルーティングは着信パケットに適用されます。ポリシーベース ルーティングが有効になっているインターフェイス上で受信されたパケットはすべて、ポリシーベース ルーティングと見なされます。ルータは、ルートマップと呼ばれる拡張パケットフィルタにそれらのパケットを通過させます。ルートマップ内で定義された基準に基づいて、パケットが適切なネクストホップに転送されます。

ルートマップ文のエントリごとに、`match` 句と `set` 句の組み合わせまたはコマンドが 1 つずつ含まれています。`match` 句は、該当するパケットが特定のポリシーを満たしているかどうか（つまり、条件を満たされているかどうか）に関する基準を定義します。`set` 句は、一致基準を満たしたパケットをどのようにルーティングするかに関する指示を提供します。`match` 句は、対応する `set` 句を適用するためにパケットが一致しなければならないフィルタのセットを指定します。

属性 104 とポリシーベース ルートマップ

この項では、属性 104 機能と、そのポリシーベース ルートマップとの連携について説明します。

RADIUS 属性 104 の概要

RADIUS 属性 104 機能を使用すれば、RADIUS 認可プロファイル内でプライベートルートを指定できます。指定したプライベートルートは、個々のインターフェイス上で受信されたパケッ

トにのみ影響します。ルートはグローバルルーティングテーブルとは別に保存され、ルーティングプロトコルに埋め込まれて再配布されることはありません。

許可ルートマップ

ルートマップステートメントは、「許可」または「拒否」にマークすることができます。ステートメントが「許可」にマークされると、一致基準を満たすパケットに `set` 句が適用されます。属性 104 の場合は、ルートマップの設定中に、次のようにルートマップを「許可」としてマークする必要があります。ルートマップの設定に関する情報については、[関連資料 \(6 ページ\)](#) を参照してください。

デフォルトプライベートルート

ポリシールーティングプロセスは、一致するものが見つかるまで、ルートマップに沿って進行します。ルートマップ内で一致するものが見つからなかった場合は、グローバルルーティングテーブルが参照されます。ユーザプロファイル内でデフォルトルートを指定した場合は、事実上、デフォルトルートを越えるルートが無視されます。

ルートマップの順序

ルートマップはサーバ上で適用したい順番に指定する必要があります。

RADIUS 属性 104 の適用方法

RADIUS 属性 104 のユーザプロファイルへの適用

次の内容を RADIUS サーバデータベースに追加することによって、RADIUS 属性 104 をユーザプロファイルに適用できます。

手順の概要

1. RADIUS 属性 104 をユーザプロファイルに適用します。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	RADIUS 属性 104 をユーザプロファイルに適用します。	<pre>Ascend-Private-Route="dest_addr/netmask next_hop"</pre> <p>ルータの宛先ネットワークアドレスは「<code>dest_addr/netmask</code>」で、ネクストホップルータのアドレスは「<code>next_hop</code>」です。</p>

例

発信者に関連付けられた3つのプライベートルートを作成するユーザプロファイルのサンプルを次に示します。

```
username Password="ascend"; User-Service=Framed-User
  Framed-Protocol=PPP,
  Framed-Address=10.1.1.1,
  Framed-Netmask=255.0.0.0,
  Ascend-Private-Route="172.16.1.1/16 10.10.10.1"
  Ascend-Private-Route="192.168.1.1/32 10.10.10.2"
  Ascend-Private-Route="10.20.0.0/1 10.10.10.3"
  Ascend-Private-Route="10.0.0.0/0 10.10.10.4"
```

上のプロファイルを使用すれば、接続用のプライベートルーティングテーブルに、デフォルトルートのほかに次のルートが追加されます。

Destination/Mask	Gateway
172.16.1.1/16	10.10.10.1
192.168.1.1/32	10.10.10.2
10.20.20.20/1	10.10.10.3
10.0.0.0/0	10.10.10.4

ルートマップの確認

次の **show** コマンドを使用して、設定済みのルートマップを確認します。

手順の概要

1. **enable**
2. **show ip policy**
3. **show route-map** [*map-name* | **dynamic** [*dynamic-map-name* | **application** [*application-name*]] | **all**]

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例： Router> enable	特権 EXEC モードを有効にします。 <ul style="list-style-type: none">• パスワードを入力します（要求された場合）。
ステップ 2	show ip policy 例： Router# show ip policy	ポリシー ルーティングに使用されるルートマップを表示します。
ステップ 3	show route-map [<i>map-name</i> dynamic [<i>dynamic-map-name</i> application [<i>application-name</i>]] all]	設定済みのすべてのルートマップを表示するか、指定した1つのルートマップだけを表示します。

	コマンドまたはアクション	目的
	例 : Router# show route-map	

RADIUS プロファイルのトラブルシューティング

プライベートルート設定が正常に動作しない場合は、「[ポリシーベース ルーティングの背景 \(2 ページ\)](#)」を再度読んでみてください。このセクションは、パケットに何が発生しているかを判定するのに役立つことがあります。また、RADIUS プロファイルのトラブルシューティングには、次の **debug** コマンドが使用できます。

手順の概要

1. **enable**
2. **debug radius**
3. **debug aaa per-user**
4. **debug ip policy**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	enable 例 : Router> enable	特権 EXEC モードを有効にします。 • パスワードを入力します (要求された場合)。
ステップ 2	debug radius 例 : Router# debug radius	RADIUS 関連の情報を表示します。
ステップ 3	debug aaa per-user 例 : Router# debug aaa per-user	ユーザ認証として各ユーザに適用される属性を表示します。
ステップ 4	debug ip policy 例 : Router# debug ip policy	IP ルーティングパケットのアクティビティを表示します。

RADIUS 属性 104 の設定例

属性 104 が適用された Route-Map 設定の例

次の出力は、属性 104 が適用された一般的な route-map 設定です。

```
Router# show route-map dynamic
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 0, identifier 1639994476

  Match clauses:
    ip address (access-lists): PBR#1 PBR#2
  Set clauses:
    Policy routing matches: 0 packets, 0 bytes
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 1, identifier 1640264784

  Match clauses:
    ip address (access-lists): PBR#3 PBR#4
  Set clauses:
    Policy routing matches: 0 packets, 0 bytes
route-map AAA-01/08/04-14:13:59.542-1-AppSpec, permit, sequence 2, identifier 1645563704

  Match clauses:
    ip address (access-lists): PBR#5 PBR#6
    length 10 100
  Set clauses:
    ip next-hop 10.1.1.1
    ip gateway10.1.1.1
  Policy routing matches: 0 packets, 0 bytes
Current active dynamic routemaps = 1
```

その他の参考資料

次の項で、RADIUS NAS-IP-Address 属性設定可能性に関する参考資料を紹介します。

関連資料

関連項目	マニュアルタイトル
AAA の設定	『Cisco IOS Security Configuration Guide: Securing User Services』の「認証、認可、およびアカウントिंग (AAA)」の項
RADIUS の設定	「Configuring RADIUS」モジュール。
RADIUS コマンド	『Cisco IOS Security Command Reference』

標準

標準	タイトル
なし	--

MIB

MIB	MIB のリンク
なし	<p>選択したプラットフォーム、Cisco IOS リリース、およびフィーチャセットに関する MIB を探してダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p>http://www.cisco.com/go/mibs</p>

RFC

RFC	タイトル
なし	--

シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンライン リソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報入手するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/en/US/support/index.html</p>

RADIUS 属性 104 の機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 1: RADIUS 属性 104 の機能情報

機能名	リリース	機能情報
RADIUS 属性 104	Cisco IOS XE Release 3.9S	<p>RADIUS 属性 104 機能を使用すれば、RADIUS 認可プロファイル内でプライベートルート（属性 104）を指定できます。プライベートルートは、個々のインターフェイス上で受信されたパケットにのみ影響します。ルートはグローバルルーティングテーブルとは別に保存され、ルーティングプロトコルに埋め込まれて再配布されることはありません。</p> <p>次のコマンドが導入または変更されました。<code>\tips-migration show ip policy</code>、<code>show route-map</code>。</p>

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。