RADIUS トンネル属性拡張

RADIUS トンネル属性拡張機能は、RADIUS 属性 90（Tunnel-Client-Auth-ID）と RADIUS 属性 91（Tunnel-Server-Auth-ID）を導入しています。この両方の属性は、ユーザにネットワーク アクセス サーバ（NAS）と RADIUS サーバの認証名の指定を許可することによって、バーチャル プライベート ネットワーク（VPN）での強制的トンネリングのプロビジョニングを支援します。

前提条件

RADIUS 属性の 90 と 91 を使用するには、次のタスクを完了する必要があります。

- AAA をサポートするように NAS を設定する。
- RADIUS をサポートするように NAS を設定する。
- VPN をサポートするように NAS を設定する。

機能制限

RADIUS トンネル属性の 90 と 91 を使用するには、RADIUS サーバがタグ付き属性をサポートしている必要があります。

RADIUS トンネル属性拡張に関する情報

RADIUS トンネル属性拡張の利点

RADIUS トンネル属性拡張の機能により、トンネル イニシエータとトンネル ターミネータの名前が（デフォルト以外で）指定できます。これにより、VPN トンネリングのセットアップ時に、より高度なセキュリティを確立できます。

RADIUS トンネル属性拡張の説明

NAS と RADIUS サーバ間の通信がセットアップされたら、トンネリング プロトコルを有効にできます。トンネリング プロトコルのアプリケーションの一部は自発的ですが、その他は強制的トンネリングを伴います。つまり、ユーザが何らかの処置や選択をしなくてもトンネルが作成されます。このような場合は、NAS から RADIUS サーバにトンネリング情報を伝送して認証を確立するための新しい RADIUS 属性が必要です。この新しい RADIUS 属性を次の表に示します。

（注） 強制的トンネリングでは、配備中のセキュリティ対策がトンネルエンドポイント間のトラフィックにのみ適用されます。トンネル化されたトラフィックの暗号化または完全性保護をエンドツーエンド セキュリティの代替手段と見なさないでください。

表 *1 : RADIUS* トンネル属性

番号	IETF RADIUS トンネル属性	同等の TACACS+ 属性	サポートされているプロトコル	説明
90	Tunnel-Client-Auth-ID	tunnel-id	レイヤ 2 トンネリング プロトコル（L2TP）	トンネル ターミネータを使用してトンネル セットアップを認証する際に、トンネル イニシエータ（NAS とも呼ばれます[1]）によって使用される名前を指定します。
91	Tunnel-Server-Auth-ID	gw-name	レイヤ 2 トンネリング プロトコル（L2TP）	トンネル イニシエータを使用してトンネル セットアップを認証する際に、トンネル ターミネータ（ホーム ゲートウェイとも呼ばれます[2]）によって使用される名前を指定します。

1 L2TP が使用される場合、NAS は L2TP アクセス コンセントレータ（LAC）とも呼ばれます。
2 L2TP が使用される場合、ホーム ゲートウェイは L2TP ネットワーク サーバ（LNS）とも呼ばれます。

RADIUS 属性 90 と RADIUS 属性 91 は次のような状況で追加されます。

- RADIUS サーバが要求を受け入れ、必要な認証名がデフォルトと異なる場合

- アカウンティング要求に値が start と stop のどちらかの Acct-Status-Type 属性が含まれ、トンネル化されたセッションが関係している場合

RADIUS トンネル属性拡張の設定方法

この機能に関連する設定作業はありません。

RADIUS 属性 90 および RADIUS 属性 91 の確認

RADIUS 属性 90 と RADIUS 属性 91 がアクセス受け入れとアカウンティング要求内で送信されていることを確認するには、EXEC モードで次のコマンドを使用します。

コマンド	目的
`Router# debug radius`	RADIUS 関連の情報を表示します。このコマンドの出力は、属性 90 と 属性 91 のどちらがアクセス受け入れとアカウンティング要求内で送信されているかを示します。

RADIUS トンネル属性拡張の設定例

L2TP ネットワーク サーバ設定の例

次の例は、RADIUS トンネリング属性の 90 と 91 を使用した基本的な L2F と L2TP の設定を含む LNS の設定方法を示しています。

```
aaa new-model
aaa authentication login default none
aaa authentication login console none
aaa authentication ppp default local group radius
aaa authorization network default group radius if-authenticated
!
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2tp
virtual-template 1
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface loopback0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
```

```
interface Virtual-Template1
ip unnumbered loopback0
ppp authentication pap
!
radius-server host 1.1.1.1 auth-port 1645 acct-port 1646
radius-server key <deleted>
!
```

RADIUS トンネリング属性の 90 と 91 を含む RADIUS ユーザ プロファイルの例

L2TP トンネル用の RADIUS トンネリング属性の 90 と 91 を含む RADIUS ユーザ プロファイルの例を次に示します。

```
cisco.com Password = "cisco", Service-Type = Outbound
Service-Type = Outbound,
Tunnel-Type = :1:L2TP,
Tunnel-Medium-Type = :1:IP,
Tunnel-Client-Endpoint = :1:"10.0.0.2",
Tunnel-Server-Endpoint = :1:"10.0.0.3",
Tunnel-Client-Auth-Id = :1:"l2tp-cli-auth-id",
Tunnel-Server-Auth-Id = :1:"l2tp-svr-auth-id",
Tunnel-Assignment-Id = :1:"l2tp-assignment-id",
Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
Tunnel-Preference = :1:1
```

その他の参考資料

次の項で、RADIUS トンネル属性拡張の機能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
認証設定	『*Cisco IOS XE Security Configuration Guide: Configuring User Services*, Release 2』の「認証の設定」
RADIUS の設定	『*Cisco IOS XE Security Configuration Guide: Configuring User Services*, Release 2』の「RADIUS の設定」
RADIUS 属性の概要	『*Cisco IOS XE Security Configuration Guide: Configuring User Services*, Release 2』の「RADIUS 属性の概要および RADIUS IETF 属性」。
セキュリティ コマンド	『*Cisco IOS* セキュリティ コマンド リファレンス』

標準

標準	タイトル
この機能でサポートされる新規の標準または変更された標準はありません。また、既存の標準のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	選択したプラットフォーム、Cisco IOS XE ソフトウェア リリース、およびフィーチャ セットの MIB の場所を検索し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。 http://www.cisco.com/go/mibs

RFC

RFC	タイトル
RFC 2868	『*RADIUS Attributes for Tunnel Protocol Support*』

シスコのテクニカル サポート

説明	リンク
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。 お使いの製品のセキュリティ情報や技術情報を入手するために、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。 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。	http://www.cisco.com/en/US/support/index.html

RADIUS トンネル属性拡張の機能情報

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 *2 : RADIUS* トンネル属性拡張の機能情報

機能名	リリース	機能情報
RADIUS トンネル属性拡張	Cisco IOS XE Release 2.1	RADIUS トンネル属性拡張機能は、RADIUS 属性 90（Tunnel-Client-Auth-ID）と RADIUS 属性 91（Tunnel-Server-Auth-ID）を導入しています。この両方の属性は、ユーザにネットワーク アクセス サーバ（NAS）と RADIUS サーバの認証名の指定を許可することによって、バーチャル プライベート ネットワーク（VPN）での強制的トンネリングのプロビジョニングを支援します。 Cisco IOS XE Release 2.1 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。

用語集

Layer 2 Tunnel Protocol (L2TP) ：ISP などのアクセスサービスで仮想トンネルを作成し、顧客のリモートサイトやリモートユーザーを企業のホームネットワークにリンクさせることが可能な Layer 2 Tunneling Protocolです。具体的には、ISP アクセス ポイント（POP）にあるネットワーク アクセス サーバ（NAS）がリモート ユーザと PPP メッセージを交換し、L2F または L2TP の要求や応答を使用して顧客のトンネル サーバと通信し、トンネルのセットアップを行います。

L2TP access concentrator (LAC) ：クライアントが直接接続し、PPP フレームが L2TP ネットワークサーバー（LNS）にトンネリングされるネットワーク アクセス サーバー（NAS）です。LAC は、L2TP が 1 つまたは複数の LNS にトラフィックを渡すために操作するメディアのみを実装します。LAC はPPP 内で伝送されるすべてのプロトコルをトンネルすることができます。また、LAC は着信コールを開始して、発信コールを受け取ります。LAC は L2F ネットワーク アクセス サーバに似ています。

L2TP network server (LNS) ：L2TP トンネルの終端点であり、PPP フレームが処理され、上位層プロトコルに渡されるアクセスポイントです。LNS は PPP を終端させる任意のプラットフォーム上で動作できます。LNS はサーバ側の L2TP プロトコルを処理します。L2TP は、L2TP

のトンネルが到達する1つのメディアにのみ依存します。LNSは発信コールを開始して、着信コールを受け取ります。LNS は L2F テクノロジーのホーム ゲートウェイに似ています。

network access server (NAS)：パケットの世界（インターネットなど）と回線交換の世界（PSTNなど）をインターフェイスする、Cisco プラットフォームまたは AccessPath システムなどのプラットフォームの集合。

トンネル：L2TP アクセス コンセントレータ（LAC）と L2TP ネットワーク サーバ（LNS）間で複数の PPP セッションを伝送可能な仮想パイプ。

バーチャルプライベートネットワーク（VPN）：リモートでダイヤルインネットワークをホーム ネットワークに存在させ、あたかも直接接続されているかのように見せるシステム。VPN は、L2TP と L2F を使用して、L2TP アクセス コンセントレータ（LAC）の代わりに、L2TP ネットワーク サーバ（LNS）でネットワーク接続のレイヤ 2 と上位層を終端させます。

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。