RADIUS トンネル アトリビュート拡張

RADIUS トンネル アトリビュート拡張機能を使用すれば、VPN トンネリングをセットアップするときに、トンネル イニシエータとターミネータの名前（デフォルト以外）を指定して、より高いレベルのセキュリティを設定できます。

機能情報の確認

ご使用のソフトウェア リリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報と注意事項については、ご使用のプラットフォームとソフトウェア リリースに対応したリリース ノートを参照してください。この章に記載されている機能の詳細、および各機能がサポートされているリリースのリストについては、「RADIUS トンネル アトリビュート拡張の機能情報」（P.7）を参照してください。

プラットフォーム サポートと Cisco IOS および Catalyst OS ソフトウェア イメージ サポートに関する情報を入手するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

この章の構成

RADIUS トンネル アトリビュート拡張の前提条件

RADIUS アトリビュートの 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。

RADIUS トンネル アトリビュート拡張の制約事項

RADIUS トンネル アトリビュートの 90 と 91 を使用するには、RADIUS サーバがタグ付きアトリビュートをサポートしている必要があります。

RADIUS トンネル アトリビュート拡張に関する情報

RADIUS トンネル アトリビュート拡張機能は、RADIUS アトリビュート 90（Tunnel-Client-Auth-ID）と RADIUS アトリビュート 91（Tunnel-Server-Auth-ID）を導入しています。この両方のアトリビュートは、ユーザに Network Access Server（NAS; ネットワーク アクセス サーバ）と RADIUS サーバの認証名の指定を許可することによって、Virtual Private Network（VPN; バーチャル プライベート ネットワーク）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。

RADIUS トンネル アトリビュート拡張の動作方法

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 アトリビュートが必要です。この新しい RADIUS アトリビュートを表 1 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 アトリビュート

番号	IETF RADIUS トンネル アトリビュート	同等の TACACS+ アトリビュート	サポートされているプロトコル	説明
90	Tunnel-Client-Auth-ID	tunnel-id	• Layer 2 Forwarding（L2F; レイヤ 2 フォワーディング） • Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）	トンネル ターミネータによるトンネル セットアップの認証時に、トンネル イニシエータ（NAS とも呼ばれる[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	• Layer 2 Forwarding（L2F; レイヤ 2 フォワーディング） • Layer 2 Tunneling Protocol（L2TP; レイヤ 2 トンネリング プロトコル）	トンネル イニシエータによるトンネル セットアップの認証時に、トンネル ターミネータ（ホーム ゲートウェイとも呼ばれる[2]）によって使用される名前を指定します。

1. L2TP が使用されている場合は、NAS が L2TP Access Concentrator（LAC; L2TP アクセス コンセントレータ）として参照されます。
2. L2TP が使用されている場合は、ホーム ゲートウェイが L2TP Network Server（LNS; L2TP ネットワーク サーバ）として参照されます。

RADIUS アトリビュート 90 と RADIUS アトリビュート 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 アトリビュートが含まれ、トンネル化されたセッションが関係している場合

RADIUS アトリビュート 90 と RADIUS アトリビュート 91 の確認方法

RADIUS アトリビュート 90 と RADIUS アトリビュート 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、アトリビュート 90 と アトリビュート 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 アトリビュート拡張の設定例

ここでは、次の設定例について説明します。

- 「L2TP Network Server（LNS; L2TP ネットワーク サーバ）設定の例」
- 「RADIUS トンネリング アトリビュートの 90 と 91 を含む RADIUS ユーザ プロファイル：例」

L2TP Network Server（LNS; 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 アトリビュートの 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 l2f-cli-auth-id password 0 l2f-cli-pass
username l2f-svr-auth-id password 0 l2f-svr-pass
username l2tp-svr-auth-id password 0 l2tp-tnl-pass
!
vpdn enable
vpdn search-order domain
!
vpdn-group 1
accept-dialin
protocol l2f
virtual-template 1
terminate-from hostname l2f-cli-auth-id
local name l2f-svr-auth-id
!
vpdn-group 2
accept-dialin
protocol l2tp
virtual-template 2
terminate-from hostname l2tp-cli-auth-id
local name l2tp-svr-auth-id
!
interface Ethernet1/0
ip address 10.0.0.3 255.255.255.0
no ip route-cache
no ip mroute-cache
!
interface Virtual-Template1
ip unnumbered Ethernet1/0
ppp authentication pap
!
interface Virtual-Template2
ip unnumbered Ethernet1/0
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 アトリビュートの 90 と 91 を含む RADIUS ユーザ プロファイル：例

RADIUS トンネリング アトリビュートの 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。このエントリは 2 つのトンネルをサポートします。1 つは L2F 用、もう 1 つは L2TP 用です。:1 が指定されたタグ エントリは L2F トンネルをサポートし、:2 が指定されたタグ エントリは L2TP トンネルをサポートします。

```
cisco.com Password = "cisco", Service-Type = Outbound
    Service-Type = Outbound,
    Tunnel-Type = :1:L2F,
    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:"l2f-cli-auth-id",
    Tunnel-Server-Auth-Id = :1:"l2f-svr-auth-id",
    Tunnel-Assignment-Id = :1:"l2f-assignment-id",
    Cisco-Avpair = "vpdn:nas-password=l2f-cli-pass",
    Cisco-Avpair = "vpdn:gw-password=l2f-svr-pass",
    Tunnel-Preference = :1:1,
    Tunnel-Type = :2:L2TP,
    Tunnel-Medium-Type = :2:IP,
    Tunnel-Client-Endpoint = :2:"10.0.0.2",
    Tunnel-Server-Endpoint = :2:"10.0.0.3",
    Tunnel-Client-Auth-Id = :2:"l2tp-cli-auth-id",
    Tunnel-Server-Auth-Id = :2:"l2tp-svr-auth-id",
    Tunnel-Assignment-Id = :2:"l2tp-assignment-id",
    Cisco-Avpair = "vpdn:l2tp-tunnel-password=l2tp-tnl-pass",
    Tunnel-Preference = :2:2
```

その他の参考資料

次の項で、RADIUS トンネル アトリビュート拡張に関する参考資料を紹介します。

関連資料

内容	参照先
認証	「Configuring Authentication」モジュール
RADIUS アトリビュート	「RADIUS Attributes Overview and RADIUS IETF Attributes」モジュール
VPDN	『*Cisco IOS VPDN Configuration Guide*, Release 15.0』

規格

規格	タイトル
なし	—

MIB

MIB	MIB リンク
なし	選択したプラットフォーム、Cisco IOS リリース、および機能セットの MIB を検索してダウンロードする場合は、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
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。 以下を含むさまざまな作業にこの Web サイトが役立ちます。 ・テクニカル サポートを受ける ・ソフトウェアをダウンロードする ・セキュリティの脆弱性を報告する、またはシスコ製品のセキュリティ問題に対する支援を受ける ・ツールおよびリソースへアクセスする - Product Alert の受信登録 - Field Notice の受信登録 - Bug Toolkit を使用した既知の問題の検索 ・Networking Professionals（NetPro）コミュニティで、技術関連のディスカッションに参加する ・トレーニング リソースへアクセスする ・TAC Case Collection ツールを使用して、ハードウェアや設定、パフォーマンスに関する一般的な問題をインタラクティブに特定および解決する この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/techsupport

RADIUS トンネル アトリビュート拡張の機能情報

表 2 に、この機能のリリース履歴を示します。

ご使用の Cisco IOS ソフトウェア リリースによっては、コマンドの中に一部使用できないものがあります。特定のコマンドに関するリリース情報については、コマンド リファレンス マニュアルを参照してください。

Cisco Feature Navigator を使用すると、プラットフォームおよびソフトウェア イメージのサポート情報を検索できます。Cisco Feature Navigator を使用すると、特定のソフトウェア リリース、機能セット、またはプラットフォームをサポートする Cisco IOS ソフトウェア イメージおよび Catalyst OS ソフトウェア イメージを確認できます。Cisco Feature Navigator には、http://tools.cisco.com/ITDIT/CFN/jsp/index.jsp からアクセスできます。Cisco.com のアカウントは必要ありません。

（注） 表 2 には、一連の Cisco IOS ソフトウェア リリースのうち、特定の機能が初めて導入された Cisco IOS ソフトウェア リリースだけが記載されています。特に明記していないかぎり、その機能は、一連の Cisco IOS ソフトウェア リリースの以降のリリースでもサポートされます。

表 2　RADIUS トンネル アトリビュート拡張の機能情報

機能名	リリース	機能情報
RADIUS トンネル アトリビュート拡張の機能情報	12.1(5)T 12.2(4)B3 12.2(13)T	RADIUS トンネル アトリビュート拡張機能を使用すれば、VPN トンネリングをセットアップするときに、トンネル イニシエータとターミネータの名前（デフォルト以外）を指定して、より高いレベルのセキュリティを設定できます。 この機能は、Cisco IOS Release 12.1(5)T で導入されました。 この機能は、Cisco IOS Release 12.2(4)B3 に統合されました。 この機能は、Cisco IOS Release 12.2(13)T に統合されました。

用語集

L2TP アクセス コンセントレータ（LAC）：クライアントが直接接続し、PPP フレームが L2TP Network Server（LNS; L2TP ネットワーク サーバ）にトンネリングされる Network Access Server（NAS; ネットワーク アクセス サーバ）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 ネットワーク サーバ（LNS）：L2TP トンネルの終端点で、PPP フレームが処理され、上位レイヤ プロトコルに渡されるアクセス ポイント。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。

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

ネットワーク アクセス サーバ（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シスコ 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

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 と上位レイヤを終端させます。

レイヤ 2 トンネル プロトコル（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 ユーザを会社のホーム ネットワークにリンクさせることが可能なレイヤ 2 トンネリング プロトコル。具体的には、ISP Point of Presence（POP; アクセス ポイント）にある Network Access Server（NAS; ネットワーク アクセス サーバ）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。

レイヤ 2 フォワーディング（L2F）：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 ユーザを会社のホーム ネットワークにリンクさせることが可能なレイヤ 2 トンネリング プロトコル。具体的には、ISP Point of Presence（POP; アクセス ポイント）にある Network Access Server（NAS; ネットワーク アクセス サーバ）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。

Cisco and the Cisco Logo are trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and other countries. A listing of Cisco's trademarks can be found at www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1005R)

このマニュアルで使用している IP アドレスおよび電話番号は、実際のアドレスおよび電話番号を示すものではありません。マニュアル内の例、コマンド出力、ネットワーク トポロジ図、およびその他の図は、説明のみを目的として使用されています。説明の中に実際のアドレスおよび電話番号が使用されていたとしても、それは意図的なものではなく、偶然の一致によるものです。

© 2000–2009 Cisco Systems, Inc.
All rights reserved.

Copyright © 2000–2011, シスコシステムズ合同会社.
All rights reserved.