

VPDN グループおよび TACACS+ を使用したダイヤルインVPDN設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[背景説明](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[確認](#)

[トラブルシューティング](#)

[トラブルシューティングのためのコマンド](#)

[関連情報](#)

概要

このドキュメントでは、VPDN グループと Terminal Access Controller Access Control System Plus (TACACS+) を使用した、ダイヤルインのバーチャル プライベート ダイヤルアップ ネットワーク (VPDN) 設定例を説明します。

前提条件

要件

この設定を開始する前に、次の要件が満たされていることを確認してください。

次の内容を理解している必要があります。

- クライアント アクセス (NAS/LAC) 用の Cisco ルータと、IP 接続を使用したネットワーク アクセス (HGW/LNS) 用の Cisco ルータ。
- ルータのホスト名または VPDN グループに使用されるローカル名。
- 使用するトンネリング プロトコル。これは、レイヤ 2 トンネリング (L2T) プロトコルまたはレイヤ 2 フォワーディング (L2F) プロトコルにすることができます。
- トンネルを認証するためのルータのパスワード。
- トンネリング基準。これは、ドメイン名または着信番号識別サービス (DNIS) にすることができます。

- ユーザ (ダイヤルインするクライアント) のユーザ名とパスワード。
- TACACS+ サーバの IP アドレスとキー。

使用するコンポーネント

このドキュメントの内容は、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期 (デフォルト) 設定の状態から起動しています。対象のネットワークが稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

表記法

ドキュメントの表記法の詳細は、「[シスコテクニカルティップスの表記法](#)」を参照してください。

背景説明

バーチャルプライベートダイヤルアップネットワーク (VPDN) と VPDN グループの詳細については、『[VPDN について](#)』を参照してください。この文書では、VPDN 設定について詳しく説明し、Terminal Access Controller Access Control System Plus (TACACS+) を補足します。

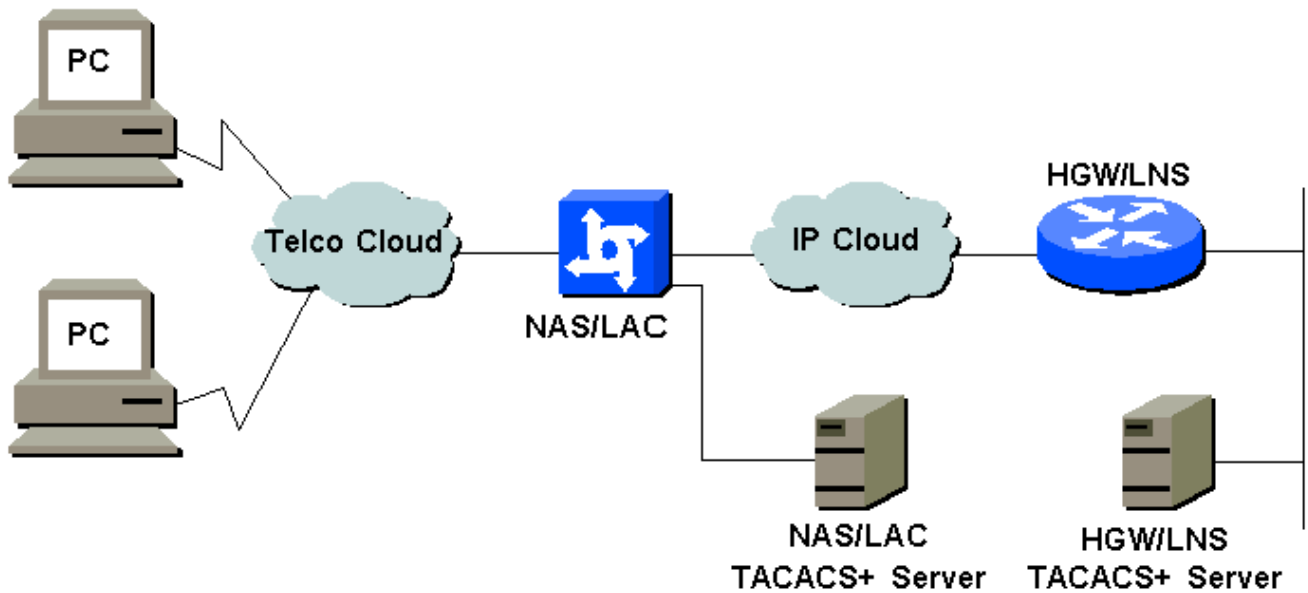
設定

このセクションでは、このドキュメントで説明する機能を設定するために必要な情報を提供しています。

注：この文書で使用されているコマンドの詳細を調べるには、「Command Lookup ツール」を使用してください (登録ユーザのみ)。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。



設定

このドキュメントでは、次の構成を使用します。

- NAS/LAC
- HGW/LNS
- NAS/LAC TACACS+ コンフィギュレーション ファイル
- HGW/LNS TACACS+ コンフィギュレーション ファイル

NAS/LAC

```

!
version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname as5300
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
enable password somethingSecret
!
username john password 0 secret4me
!
ip subnet-zero
!
vpdn enable
!
isdn switch-type primary-5ess
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!

```

```
controller T1 1
  framing esf
  clock source line secondary 1
  linecode b8zs
  pri-group timeslots 1-24
!
controller T1 2
  framing esf
  linecode b8zs
  pri-group timeslots 1-24
!
controller T1 3
  framing esf
  linecode b8zs
  pri-group timeslots 1-24
!
interface Ethernet0
  ip address 172.16.186.52 255.255.255.240
  no ip directed-broadcast
!
interface Serial023
  no ip address
  no ip directed-broadcast
  encapsulation ppp
  ip tcp header-compression passive
  dialer rotary-group 1
  isdn switch-type primary-5ess
  isdn incoming-voice modem
  no cdp enable
!
interface Serial123
  no ip address
  no ip directed-broadcast
  encapsulation ppp
  ip tcp header-compression passive
  dialer rotary-group 1
  isdn switch-type primary-5ess
  isdn incoming-voice modem
  no cdp enable
!
interface Serial223
  no ip address
  no ip directed-broadcast
  encapsulation ppp
  ip tcp header-compression passive
  dialer rotary-group 1
  isdn switch-type primary-5ess
  isdn incoming-voice modem
  no cdp enable
!
interface Serial323
  no ip address
  no ip directed-broadcast
  encapsulation ppp
  ip tcp header-compression passive
  dialer rotary-group 1
  isdn switch-type primary-5ess
  isdn incoming-voice modem
  no cdp enable
!
interface FastEthernet0
  no ip address
  no ip directed-broadcast
  shutdown
```

```
!  
interface Group-Async1  
  ip unnumbered Ethernet0  
  no ip directed-broadcast  
  encapsulation ppp  
  ip tcp header-compression passive  
  async mode interactive  
  peer default ip address pool IPAddressPool  
  no cdp enable  
  ppp authentication chap  
  group-range 1 96  
!  
interface Dialer1  
  ip unnumbered Ethernet0  
  no ip directed-broadcast  
  encapsulation ppp  
  ip tcp header-compression passive  
  dialer-group 1  
  peer default ip address pool IPAddressPool  
  no cdp enable  
  ppp authentication chap  
!  
ip local pool IPAddressPool 10.10.10.1 10.10.10.254  
no ip http server  
ip classless  
ip route 0.0.0.0 0.0.0.0 172.16.186.49  
!  
tacacs-server host 172.16.171.9  
tacacs-server key 2easy  
!  
line con 0  
  login authentication CONSOLE  
  transport input none  
line 1 96  
  autoselect during-login  
  autoselect ppp  
  modem Dialin  
line aux 0  
line vty 0 4  
!  
end
```

HGW/LNS

```
!  
version 12.0  
service timestamps debug uptime  
service timestamps log uptime  
!  
hostname access-9  
!  
aaa new-model  
aaa authentication login default local  
aaa authentication login CONSOLE none  
aaa authentication ppp default if-needed group tacacs+  
aaa authorization network default group tacacs+  
enable password somethingSecret  
!  
ip subnet-zero  
!  
vpdn enable  
!
```

```
vpdn-group DEFAULT
! Default L2TP VPDN group
accept-dialin
  protocol any
  virtual-template 1
local name LNS
lcp renegotiation always
l2tp tunnel password 0 not2tell
!
vpdn-group POP1
accept-dialin
  protocol l2tp
  virtual-template 2
terminate-from hostname LAC
local name LNS
l2tp tunnel password 0 2secret
!
vpdn-group POP2
accept-dialin
  protocol l2f
  virtual-template 3
terminate-from hostname NAS
local name HGW
lcp renegotiation always
!
interface FastEthernet0/0
  ip address 172.16.186.1 255.255.255.240
  no ip directed-broadcast
!
interface Virtual-Template1
  ip unnumbered FastEthernet0/0
  no ip directed-broadcast
  ip tcp header-compression passive
  peer default ip address pool IPaddressPool
  ppp authentication chap
!
interface Virtual-Template2
  ip unnumbered Ethernet0/0
  no ip directed-broadcast
  ip tcp header-compression passive
  peer default ip address pool IPaddressPoolPOP1
  compress stac
  ppp authentication chap
!
interface Virtual-Template3
  ip unnumbered Ethernet0/0
  no ip directed-broadcast
  ip tcp header-compression passive
  peer default ip address pool IPaddressPoolPOP2
  ppp authentication pap
  ppp multilink
!
ip local pool IPaddressPool 10.10.10.1 10.10.10.254
ip local pool IPaddressPoolPOP1 10.1.1.1 10.1.1.254
ip local pool IPaddressPoolPOP2 10.1.2.1 10.1.2.254
ip classless
no ip http server
!
tacacs-server host 172.16.186.9
tacacs-server key not2difficult
!
line con 0

login authentication CONSOLE
```

```
transport input none
line 97 120
line aux 0
line vty 0 4
!
!
end
```

NAS/LAC TACACS+ コンフィギュレーション ファイル

```
key = 2easy

# Use L2TP tunnel to 172.16.186.1 when 4085555100 is
dialed
user = dnis:4085555100 {
    service = ppp protocol = vpdn {
        tunnel-id = anonymous
        ip-addresses = 172.16.186.1
        tunnel-type = l2tp
    }
}

# Password for tunnel authentication
user = anonymous {
    chap = cleartext not2tell
}

###

# Use L2TP tunnel to 172.16.186.1 when 4085555200 is
dialed
user = dnis:4085555200 {
    service = ppp protocol = vpdn {
        tunnel-id = LAC
        ip-addresses = 172.16.186.1
        tunnel-type = l2tp
    }
}

# Password for tunnel authentication
user = LAC {
    chap = cleartext 2secret
}

###

# Use L2F tunnel to 172.16.186.1 when user authenticates
with cisco.com domain
user = cisco.com {
    service = ppp protocol = vpdn {
        tunnel-id = NAS
        ip-addresses = 172.16.186.1
        tunnel-type = l2f
    }
}

# Password for tunnel authentication
user = NAS {
    chap = cleartext cisco
}

# Password for tunnel authentication
```

```
user = HGW {
    chap = cleartext cisco
}
```

HGW/LNS TACACS+ コンフィギュレーション ファイル

```
key = not2difficult

# Password for tunnel authentication
user = NAS {
    chap = cleartext cisco
}

# Password for tunnel authentication
user = HGW {
    chap = cleartext cisco
}

user = santiago {
    chap = cleartext letmein

    service = ppp protocol = lcp { }
    service = ppp protocol = ip { }
}

user = santiago@cisco.com {
    global = cleartext letmein

    service = ppp protocol = lcp { }
    service = ppp protocol = multilink { }
    service = ppp protocol = ip { }
}
```

確認

ここでは、設定が正しく機能していることを確認するために使用する情報を示します。

一部の show コマンドは[アウトプット インタープリタ ツール](#)によってサポートされています (登録ユーザ専用)。このツールを使用することによって、show コマンド出力の分析結果を表示できます。

- show vpdn tunnel all : すべてのアクティブ トンネルの詳細を表示します。
- show user : 接続されているユーザの名前を表示します。
- show interface virtual-access # : HGW/LNS 上の特定の仮想インターフェイスのステータスをチェックできるようにします。

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

[トラブルシューティングのためのコマンド](#)

注 : debug コマンドを発行する前に、『[debug コマンドの重要な情報](#)』を参照してください。

- debug vpdn l2x-events:NAS/LACとHGW/LNSの間のトンネルまたはセッションの作成に関するダイアログを表示します。
- debug ppp authentication : クライアントが認証を通過したかどうかをチェックできるようにします。
- debug ppp negotiation : クライアントが PPP ネゴシエーションを通過したかどうかをチェックできるようにします。ネゴシエートするオプション (コールバックや MLP など) とプロトコル (IP や IPX など) を表示できます。
- debug ppp error : PPP 接続のネゴシエーションと操作に関連付けられたプロトコル エラーとエラー統計情報を表示します。
- debug vtemplate : HGW/LNS 上の仮想アクセス インターフェイスのクローニングを表示します。ダイヤルアップ接続の開始時点でインターフェイスが作成 (仮想テンプレートから複製) されるタイミングと接続の終了時点でインターフェイスが破棄されるタイミングを確認できます。
- debug aaa authentication : ユーザまたはトンネルが認証、許可、アカウントिंग (AAA) サーバによって認証されたかどうかをチェックできるようにします。
- debug aaa authorization : ユーザが AAA サーバによって認可されたかどうかをチェックできるようにします。
- debug aaa per-user : 認証されたユーザごとに何が適用されたかチェックできるようにします。これは、上記の一般的なデバッグとは異なります。

[関連情報](#)

- [テクノロジー サポート ページ - ダイヤル](#)
- [テクニカルサポート - Cisco Systems](#)