

Configuration d'un réseau VPDN initié par accès téléphonique en utilisant des groupes VPDN et TACACS+

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Vérification](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Informations connexes](#)

Introduction

Ce document fournit un exemple de configuration pour les réseaux commutés VPDN (Virtual Private Dialup Networks), utilisant des groupes VPDN et TACACS+ (Terminal Access Controller Access Control System Plus).

Conditions préalables

Conditions requises

Avant d'essayer cette configuration, assurez-vous de respecter les conditions suivantes :

Vous devez disposer des éléments suivants :

- Un routeur Cisco pour l'accès client (NAS/LAC) et un routeur Cisco pour l'accès réseau (HGW/LNS) avec une connectivité IP entre eux.
- Noms d'hôtes des routeurs ou noms locaux à utiliser sur les groupes VPDN.
- Protocole de tunnellation à utiliser. Il peut s'agir du protocole L2T (Layer 2 Tunneling) ou L2F (Layer 2 Forwarding).
- Mot de passe permettant aux routeurs d'authentifier le tunnel.
- Un critère de transmission tunnel. Il peut s'agir du nom de domaine ou du service DNIS

(Diald Number Identification Service).

- Noms d'utilisateur et mots de passe de l'utilisateur (appel client entrant).
- Les adresses IP et les clés de vos serveurs TACACS+.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Conventions

Pour plus d'informations sur les conventions des documents, référez-vous aux [Conventions utilisées pour les conseils techniques de Cisco](#).

Informations générales

Pour une présentation détaillée des réseaux commutés privés virtuels (VPDN) et des groupes VPDN, reportez-vous à [Présentation du VPDN](#). Ce document se développe sur la configuration VPDN et ajoute le système TACACS+ (Terminal Access Controller Access Control System Plus).

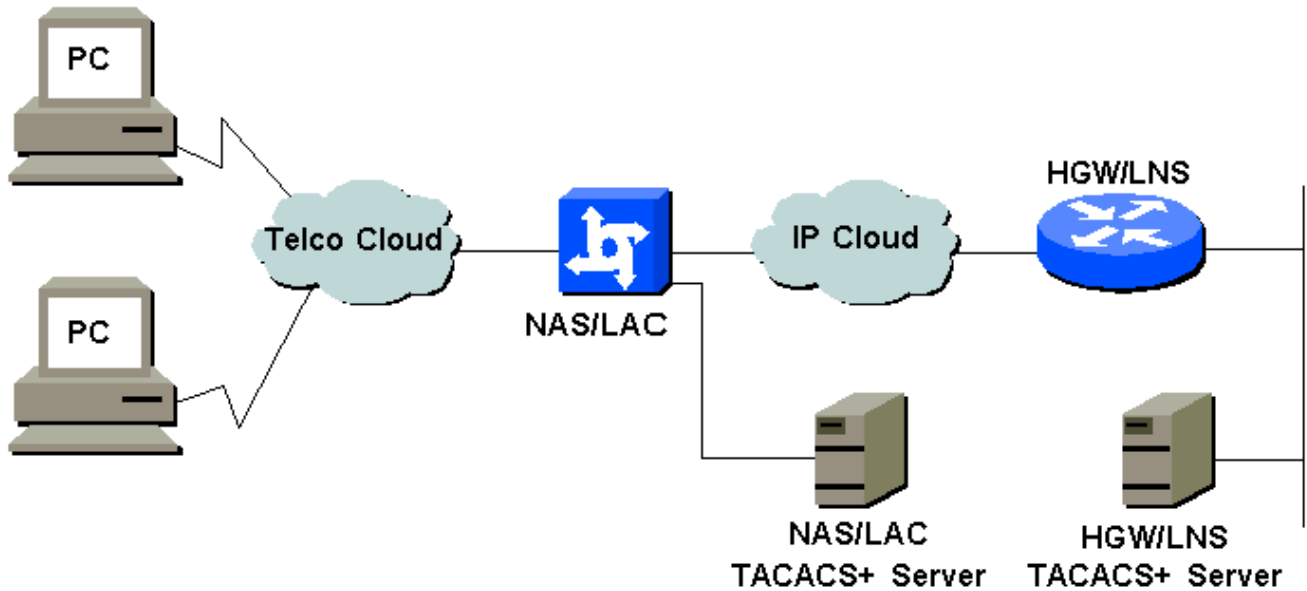
Configuration

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque : Pour en savoir plus sur les commandes utilisées dans le présent document, utilisez [l'outil de recherche de commandes](#) (clients [inscrits](#) seulement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :



Configurations

Ce document utilise les configurations suivantes :

- NAS/LAC
- HGW/LNS
- Fichier de configuration NAS/LAC TACACS+
- Fichier de configuration HGW/LNS TACACS+

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
```

Fichier de configuration NAS/LAC TACACS+

```
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
}
```

Fichier de configuration HGW/LNS TACACS+

```
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 { }
}
```

Vérification

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'[Output Interpreter Tool](#) (clients enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **show vpdn tunnel all** : affiche les détails de tous les tunnels actifs.
- **show user** : affiche le nom de l'utilisateur connecté.
- **show interface virtual-access #** : vous permet de vérifier l'état d'une interface virtuelle particulière sur HGW/LNS.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Remarque : avant d'émettre des commandes **debug**, reportez-vous à [Informations importantes sur](#)

[les commandes de débogage.](#)

- **debug vpdn l2x-events** : affiche la boîte de dialogue entre NAS/LAC et HGW/LNS pour la création de tunnel ou de session.
- **debug ppp authentication** : vous permet de vérifier si un client passe l'authentification.
- **debug ppp negotiation** : vous permet de vérifier si un client passe la négociation PPP. Vous pouvez voir quelles options (telles que, callback, MLP, etc.) et quels protocoles (tels que, IP, IPX, etc.) sont en cours de négociation.
- **debug ppp error** : affiche les erreurs de protocole et les statistiques d'erreur associées à la négociation et au fonctionnement de la connexion PPP.
- **debug vtemplate** —affiche le clonage des interfaces d'accès virtuel sur HGW/LNS. Vous pouvez voir quand l'interface est créée (clonée à partir du modèle virtuel) au début de la connexion commutée et quand l'interface est détruite lorsque la connexion est interrompue.
- **debug aaa authentication** : vous permet de vérifier si l'utilisateur ou le tunnel est authentifié par le serveur AAA (Authentication, Authorization, and Accounting).
- **debug aaa Authorization** : vous permet de vérifier si l'utilisateur est autorisé par le serveur AAA.
- **debug aaa per user** : vous permet de vérifier ce qui est appliqué à chaque utilisateur authentifié. Ceci est différent des débogages généraux listés ci-dessus.

[Informations connexes](#)

- [Pages d'assistance technologique - Composer](#)
- [Support technique - Cisco Systems](#)