

Configuration de réseaux VPDN par utilisateur sans informations de domaine ou DNIS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Informations générales](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration du serveur RADIUS](#)

[Vérification](#)

[Exemple de sortie de la commande show](#)

[Dépannage](#)

[Dépannage des commandes](#)

[Exemple de sortie de débogage](#)

[Informations connexes](#)

Introduction

Ce document fournit un exemple de configuration pour les VPDN par utilisateur sans informations de domaine ou DNIS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Logiciel Cisco IOS® version 12.1(4) ou ultérieure.
- Logiciel Cisco IOS Version 12.1(4)T ou ultérieure.

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

Dans les scénarios VPDN (Virtual Private Dial Network), le serveur d'accès au réseau (NAS) (un concentrateur d'accès L2TP, ou LAC) établit le tunnel VPDN vers la passerelle Home Gateway (LNS) en fonction des informations propres à l'utilisateur. Ce tunnel VPDN peut être L2F (Level 2 Forwarding) ou L2TP (Layer 2 Tunneling Protocol). Pour déterminer si un utilisateur doit utiliser un tunnel VPDN, vérifiez :

- Indique si le nom de domaine fait partie du nom d'utilisateur. Par exemple, avec le nom d'utilisateur tunnelme@cisco.com, le NAS transfère cet utilisateur au tunnel pour cisco.com.
- Le service DNIS (Dialed Number Information Service). Il s'agit d'un renvoi d'appels basé sur le numéro appelé. Cela signifie que le NAS peut transférer tous les appels avec un numéro appelé particulier vers le tunnel approprié. Par exemple, si un appel entrant porte le numéro appelé 5551111, l'appel peut être transféré vers le tunnel VPDN, alors qu'un appel vers 5552222 n'est pas transféré. Cette fonctionnalité nécessite que le réseau Telco fournisse les informations de numéro appelé.

Pour plus d'informations sur la configuration VPDN, consultez [Présentation du VPDN](#).

Dans certaines situations, vous pouvez exiger l'initialisation d'un tunnel VPDN par nom d'utilisateur, avec ou sans besoin d'un nom de domaine. Par exemple, l'utilisateur **ciscouser** peut être tunnelisé sur **cisco.com**, tandis que d'autres utilisateurs peuvent être terminés localement sur le NAS.

Remarque : Ce nom d'utilisateur n'inclut pas les informations de domaine comme dans l'exemple précédent.

La fonctionnalité de configuration VPDN par utilisateur envoie l'intégralité du nom d'utilisateur structuré au serveur AAA (Authentication, Authorization, and Accounting) la première fois que le routeur contacte le serveur AAA. Cela permet au logiciel Cisco IOS de personnaliser les attributs de tunnel pour les utilisateurs individuels qui utilisent un nom de domaine commun ou DNIS.

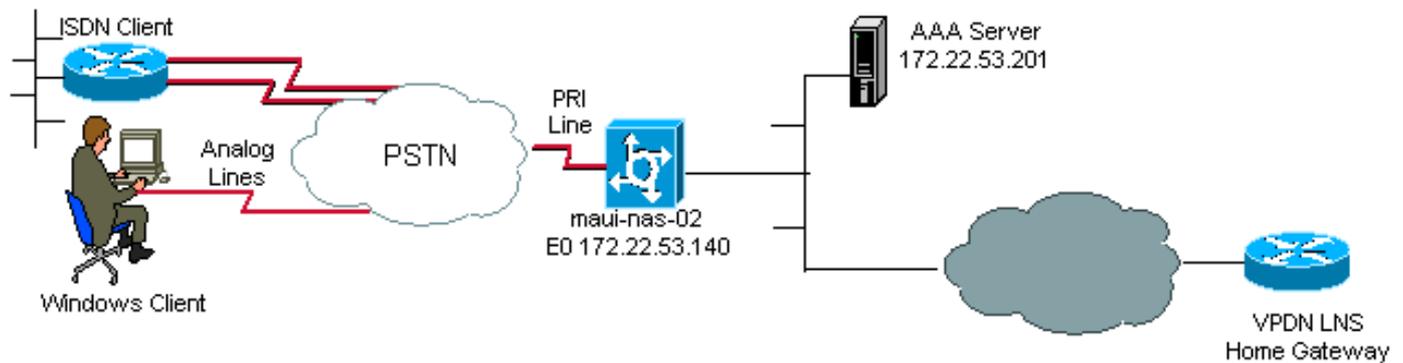
Configuration

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

Les seules commandes VPDN nécessaires sur le NAS (LAC) pour prendre en charge les VPDN par utilisateur sont les commandes de configuration globale **vpdn enable** et **vpdn authen-before-forward**. La commande **vpdn authen-before-forward** demande au NAS (LAC) d'authentifier le nom d'utilisateur complet avant de prendre une décision de transfert. Un tunnel VPDN est alors établi, sur la base des informations retournées par le serveur AAA pour cet utilisateur individuel ; si aucune information VPDN n'est retournée par le serveur AAA, l'utilisateur est arrêté localement. La configuration de cette section montre les commandes nécessaires pour prendre en charge les tunnels sans les informations de domaine dans le nom d'utilisateur.

Remarque : cette configuration n'est pas complète. Seules les commandes VPDN, interface et AAA pertinentes sont incluses.

Remarque : Ce document ne couvre pas tous les protocoles de tunnel et AAA possibles. Par conséquent, cette configuration implémente un tunnel L2TP avec le serveur RADIUS AAA. Adaptez les principes et la configuration abordés ici pour configurer d'autres types de tunnels ou protocoles AAA.

Ce document utilise la configuration suivante :

- NAS VPDN (LAC)

NAS VPDN (LAC)

```
aaa new-model
aaa authentication ppp default group radius
!--- Use RADIUS authentication for PPP authentication.
aaa authorization network default group radius !---
Obtain authorization information from the Radius server.
!--- This command is required for the AAA server to
provide VPDN attributes. ! vpdn enable !--- VPDN is
enabled. vpdn authen-before-forward !--- Authenticate
the complete username before making a forwarding
decision. !--- The LAC sends the username to the AAA
server for VPDN attributes. ! controller E1 0 pri-group
timeslots 1-31 ! interface Serial0:15 dialer rotary-
group 1 !--- D-channel for E1 0 is a member of the
dialer rotary group 1. ! interface Dialer1 !--- Logical
interface for dialer rotary group 1. ip unnumbered
Ethernet0 encapsulation ppp dialer in-band dialer-group
1 ppp authentication chap pap callin ! radius-server
host 172.22.53.201 !--- The IP address of the RADIUS
```

```
server host. !--- This AAA server will supply the
NAS(LAC) with the VPDN attributes for the user. radius-
server key cisco !--- The RADIUS server key.
```

Configuration du serveur RADIUS

Voici quelques configurations utilisateur sur un serveur RADIUS Cisco Secure pour Unix (CSU) :

1. Un utilisateur qui doit être arrêté localement sur le NAS :

```
user1 Password = "cisco"
Service-Type = Framed-User
```

2. Utilisateur pour lequel une session VPDN doit être établie :

```
user2 Password = "cisco"
Service-Type = Framed-User,
Cisco-AVPair = "vpdn:ip-addresses=172.22.53.141",
Cisco-AVPair = "vpdn:l2tp-tunnel-password=cisco",
Cisco-AVPair = "vpdn:tunnel-type=l2tp"
```

Le NAS (LAC) utilise les attributs spécifiés avec le VPDN Cisco-AVPair pour initier le tunnel VPDN à la passerelle Home Gateway. Assurez-vous que vous configurez la passerelle Home Gateway pour accepter les tunnels VPDN à partir du NAS.

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 caller user** : affiche les paramètres d'un utilisateur particulier, tels que la ligne TTY utilisée, l'interface asynchrone (étagère, logement ou port), le numéro de canal DS0, le numéro de modem, l'adresse IP attribuée, les paramètres de bundle PPP et PPP, etc. Si votre version du logiciel Cisco IOS ne prend pas en charge cette commande, utilisez la commande **show user**.
- **show vpdn** : affiche des informations sur les tunnels de protocole L2F et L2TP actifs et les identificateurs de message dans un VPDN.

Exemple de sortie de la commande show

Lorsque l'appel se connecte, utilisez la commande **show caller user *username*** ainsi que la commande **show vpdn** pour vérifier que l'appel a réussi. Un exemple de résultat est présenté ci-dessous :

```
maui-nas-02#show caller user vpdn_authen
```

```
User: vpdn_authen, line tty 12, service Async
Active time 00:09:01, Idle time 00:00:05
Timeouts:          Absolute  Idle      Idle
                   Session   Exec
Limits:            -         -         00:10:00
Disconnect in:    -         -         -
TTY: Line 12, running PPP on As12
```

```
DS0: (slot/unit/channel)=0/0/5
Line: Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits
Status: Ready, Active, No Exit Banner, Async Interface Active
      HW PPP Support Active
Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
              Modem Callout, Modem RI is CD,
              Line is permanent async interface, Integrated Modem
Modem State: Ready
```

User: vpdn_authen, line As12, service PPP

Active time 00:08:58, Idle time 00:00:05

Timeouts: Absolute Idle

Limits: - -

Disconnect in: - -

PPP: LCP Open, CHAP (<- AAA)

IP: Local 172.22.53.140

VPDN: NAS , MID 4, MID Unknown

HGW , NAS CLID 0, HGW CLID 0, tunnel open

!--- The VPDN tunnel is open. Counts: 85 packets input, 2642 bytes, 0 no buffer 0 input errors, 0 CRC, 0 frame, 0 overrun 71 packets output, 1577 bytes, 0 underruns 0 output errors, 0 collisions, 0 interface resets maui-nas-02#**show vpdn**

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID	RemID	Remote Name	State	Remote Address	Port	Sessions
6318	3	HGW	est	172.22.53.141	1701	1

LocID	RemID	TunID	Intf	Username	State	Last Chg	Fastswitch
4	3	6318	As12	vpdn_authen	est	00:09:33	enabled

!--- The tunnel for user vpdn_authen is in established state. %No active L2F tunnels %No active PPTP tunnels %No active PPPoE tunnel

Dépannage

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

Dépannage des commandes

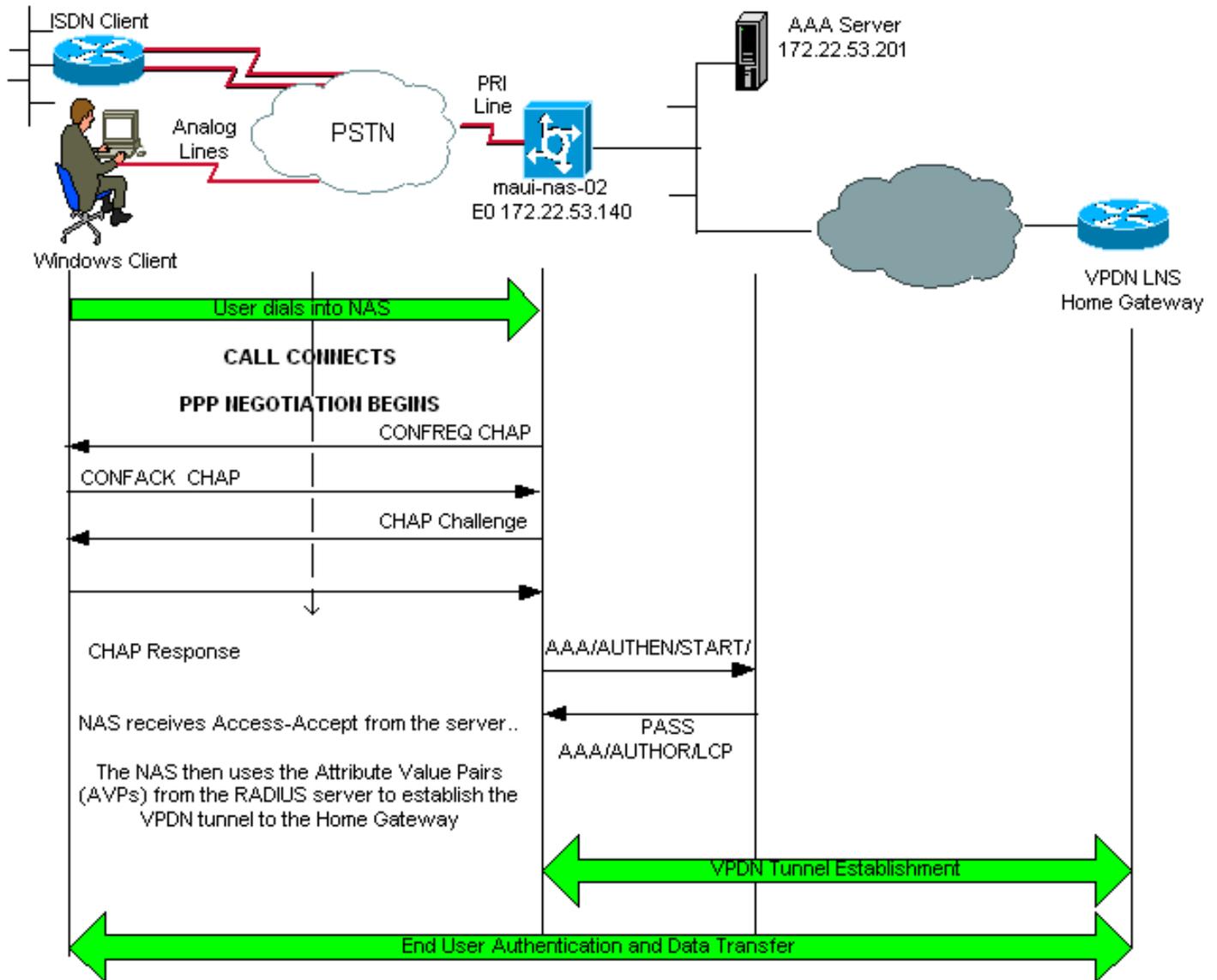
Remarque : avant d'émettre des commandes **debug**, reportez-vous à [Informations importantes sur les commandes de débogage](#).

- **debug ppp authentication** - affiche les messages du protocole d'authentification PPP et inclut les échanges de paquets CHAP (Challenge Handshake Authentication Protocol) et PAP (Password Authentication Protocol).
- **debug aaa authentication** - affiche des informations sur l'authentification AAA/RADIUS.
- **debug aaa Authorization** : affiche des informations sur l'autorisation AAA/RADIUS.
- **debug radius** : affiche les informations de débogage détaillées associées au RADIUS. Utilisez l'[outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) pour décoder les messages debug radius. Par exemple, référez-vous à la section [Exemple de sortie de débogage](#). Utilisez les informations de **debug radius** pour déterminer les attributs négociés.
- **debug tacacs** : affiche les informations de débogage détaillées associées à TACACS+.
- **debug vpdn event** - affiche les erreurs et événements L2x qui font partie de l'établissement ou de l'arrêt normal du tunnel pour les VPDN.
- **debug vpdn error** - affiche les erreurs de protocole VPDN.
- **debug vpdn l2x-event** : affiche les erreurs et événements L2x détaillés qui font partie de l'établissement ou de l'arrêt normal du tunnel pour les VPDN.

- `debug vpdn l2x-error` - affiche les erreurs de protocole L2x VPDN.

Exemple de sortie de débogage

Voici la sortie de débogage pour un appel réussi. Dans cet exemple, notez que le NAS obtient les attributs du tunnel VPDN à partir du serveur Radius.



```
maui-nas-02#show debug
```

```
General OS:
```

```
AAA Authentication debugging is on
```

```
AAA Authorization debugging is on
```

```
PPP:
```

```
PPP authentication debugging is on
```

```
VPN:
```

```
L2X protocol events debugging is on
```

```
L2X protocol errors debugging is on
```

```
VPDN events debugging is on
```

```
VPDN errors debugging is onRadius protocol debugging is on
```

```
maui-nas-02#
```

```
*Jan 21 19:07:26.752: %ISDN-6-CONNECT: Interface Serial10:5 is now connected
```

```
to N/A N/A
```

```
!--- Incoming call. *Jan 21 19:07:55.352: %LINK-3-UPDOWN: Interface Async12, changed state to up
```

```
*Jan 21 19:07:55.352: Async12 PPP: Treating connection as a dedicated line *Jan 21 19:07:55.352:
```

```

As12 AAA/AUTHOR/FSM: (0): LCP succeeds trivially *Jan 21 19:07:55.604: As12 CHAP: O CHALLENGE id
1 len 32 from "maui-nas-02" *Jan 21 19:07:55.732: As12 CHAP: I RESPONSE id 1 len 32 from
"vpdn_authen"
!--- Incoming CHAP response from user vpdn_authen. *Jan 21 19:07:55.732: AAA: parse name=Async12
idb type=10 tty=12 *Jan 21 19:07:55.732: AAA: name=Async12 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=12 channel=0 *Jan 21 19:07:55.732: AAA: parse name=Serial0:5 idb type=12 tty=-1
*Jan 21 19:07:55.732: AAA: name=Serial0:5 flags=0x51 type=1 shelf=0 slot=0 adapter=0 port=0
channel=5 *Jan 21 19:07:55.732: AAA/ACCT/DS0: channel=5, ds1=0, t3=0, slot=0, ds0=5 *Jan 21
19:07:55.732: AAA/MEMORY: create_user (0x628C79EC) user='vpdn_authen' ruser='' port='Async12'
rem_addr='async/81560' authen_type=CHAP service=PPP priv=1 *Jan 21 19:07:55.732:
AAA/AUTHEN/START (4048817807): port='Async12' list='' action=LOGIN service=PPP *Jan 21
19:07:55.732: AAA/AUTHEN/START (4048817807): using "default" list *Jan 21 19:07:55.732:
AAA/AUTHEN/START (4048817807): Method=radius (radius) *Jan 21 19:07:55.736: RADIUS: ustruct
sharecount=1 *Jan 21 19:07:55.736: RADIUS: Initial Transmit Async12 id
6 172.22.53.201:1645, Access-Request, len 89
*Jan 21 19:07:55.736:           Attribute 4 6 AC16358C
*Jan 21 19:07:55.736:           Attribute 5 6 0000000C
*Jan 21 19:07:55.736:           Attribute 61 6 00000000
*Jan 21 19:07:55.736:           Attribute 1 13 7670646E
*Jan 21 19:07:55.736:           Attribute 30 7 38313536
*Jan 21 19:07:55.736:           Attribute 3 19 014CF9D6
*Jan 21 19:07:55.736:           Attribute 6 6 00000002
*Jan 21 19:07:55.736:           Attribute 7 6 00000001
*Jan 21 19:07:55.740: RADIUS: Received from id 6 172.22.53.201:1645,
Access-Accept, len 136
*Jan 21 19:07:55.740:           Attribute 6 6 00000002
*Jan 21 19:07:55.740:           Attribute 26 40 0000000901227670
*Jan 21 19:07:55.740:           Attribute 26 40 0000000901227670
*Jan 21 19:07:55.740:           Attribute 26 30 0000000901187670

```

Les paires de valeurs d'attribut (AVP) nécessaires pour le tunnel VPDN sont désactivées à partir du serveur RADIUS. Cependant, **debug radius** produit une sortie codée indiquant les AVP et leurs valeurs. Vous pouvez coller le résultat affiché en **gras** ci-dessus dans l'[outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement). La sortie suivante en gras est la sortie décodée obtenue à partir de l'outil :

```

Access-Request 172.22.53.201:1645 id 6
Attribute Type 4: NAS-IP-Address is 172.22.53.140
Attribute Type 5: NAS-Port is 12
Attribute Type 61: NAS-Port-Type is Asynchronous
Attribute Type 1: User-Name is vpdn
Attribute Type 30: Called-Station-ID(DNIS) is 8156
Attribute Type 3: CHAP-Password is (encoded)
Attribute Type 6: Service-Type is Framed
Attribute Type 7: Framed-Protocol is PPP
    Access-Accept 172.22.53.201:1645 id 6
Attribute Type 6: Service-Type is Framed
Attribute Type 26: Vendor is Cisco
Attribute Type 26: Vendor is Cisco
Attribute Type 26: Vendor is Cisco
*Jan 21 19:07:55.740: AAA/AUTHEN (4048817807): status = PASS
...
...
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:ip-addresses=172.22.53.141"
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:l2tp-tunnel-password=cisco"
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:tunnel-type=l2tp"
*Jan 21 19:07:55.744: AAA/AUTHOR (733932081): Post authorization status = PASS_REPL
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV service=ppp

```

*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV ip-addresses=172.22.53.141

*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV l2tp-tunnel-password=cisco

*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp

!--- Tunnel information. !--- The VPDN Tunnel will now be established and the call will be authenticated. !--- Since the debug information is similar to that for a normal VPDN call, !--- the VPDN tunnel establishment debug output is omitted.

[Informations connexes](#)

- [Présentation de VPDN](#)
- [Configuration des réseaux commutés privés virtuels](#)
- [Configuration de l'authentification du protocole de tunnel de couche 2 avec RADIUS](#)
- [Configuration de l'authentification du protocole de tunnel de couche 2 avec TACACS+](#)
- [Accès aux pages d'assistance technologique](#)
- [Support technique - Cisco Systems](#)