Configuration de l'authentification du protocole L2TP (Layer 2 Tunnel Protocol) avec RADIUS

Contenu

Introduction

Ce document dépeint comment configurer un scénario de Réseau privé virtuel à accès commuté (VPDN) de protocol (L2TP) de tunnel de la couche 2 utilisant des attributs de tunnel téléchargés d'un serveur de RAYON. Dans cet exemple, le concentrateur L2TP Access (LAC) reçoit la connexion entrante et contacte le serveur de RAYON de LAC. Les consultations de serveur de RAYON que le tunnel attribue pour le domaine de l'utilisateur (par exemple, cisco.com) et passe les attributs de tunnel au LAC. Basé sur ces attributs, le LAC initie un tunnel au serveur de réseau L2TP (LNS). Une fois que le tunnel est établi, le LNS authentifie l'utilisateur final à l'aide de son propre serveur de RAYON.

Remarque: Ce document suppose que le NAS (LAC) a été configuré pour l'accès commuté

général. Pour plus d'informations sur la façon configurer le cadran, référez-vous à configurer le RADIUS AAA de base pour des clients entrant.

Pour plus d'informations sur L2TP et VPDNs, référez-vous à ces documents :

- Présentation de VPDN
- Configurer des réseaux privés virtuels
- Tunnel Protocol de la couche 2

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Deux routeur Cisco 2511
- Version de logiciel 12.0(2).T de Cisco IOS®
- Cisco Secure ACS pour l'UNIX, Cisco Secure ACS pour Windows, ou Merit RADIUS

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

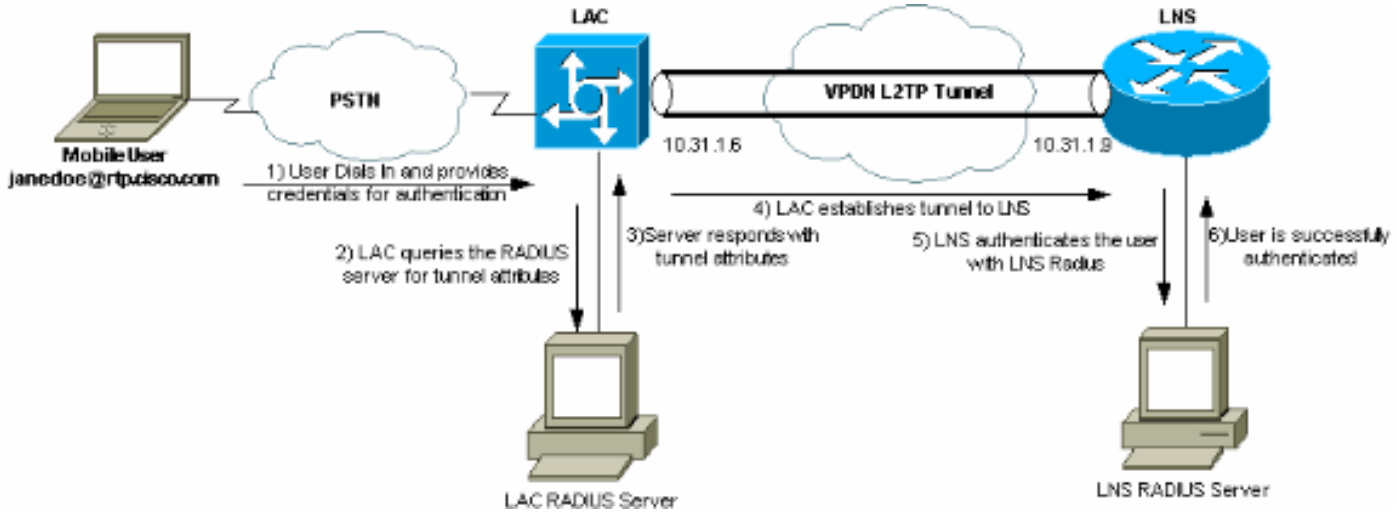
Configuration du serveur RADIUS

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

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau indiquée dans le diagramme suivant.



Configuration RADIUS de LAC - Cisco Secure ACS pour l'UNIX

La configuration RADIUS de LAC inclut l'utilisateur « rtp.cisco.com » (qui est le domaine utilisé par le client). Le mot de passe pour cet utilisateur doit être Cisco.

```
# ./ViewProfile -p 9900 -u rtp.cisco.com
user = rtp.cisco.com{
radius=Cisco {
check_items= {
2="cisco"
}
reply_attributes= {
6=5
9,1="vpdn:tunnel-id=DEFGH"
9,1="vpdn:tunnel-type=l2tp"
9,1="vpdn:ip-addresses=10.31.1.9"
9,1="vpdn:l2tp-tunnel-password=ABCDE"
}
}
}
```

Pour plus d'informations sur la configuration RADIUS sur le LAC, référez-vous au profil RADIUS à l'usage de la section de LAC dans le tunnel Protocol de la couche 2.

Configuration RADIUS LNS - Cisco Secure ACS pour l'UNIX

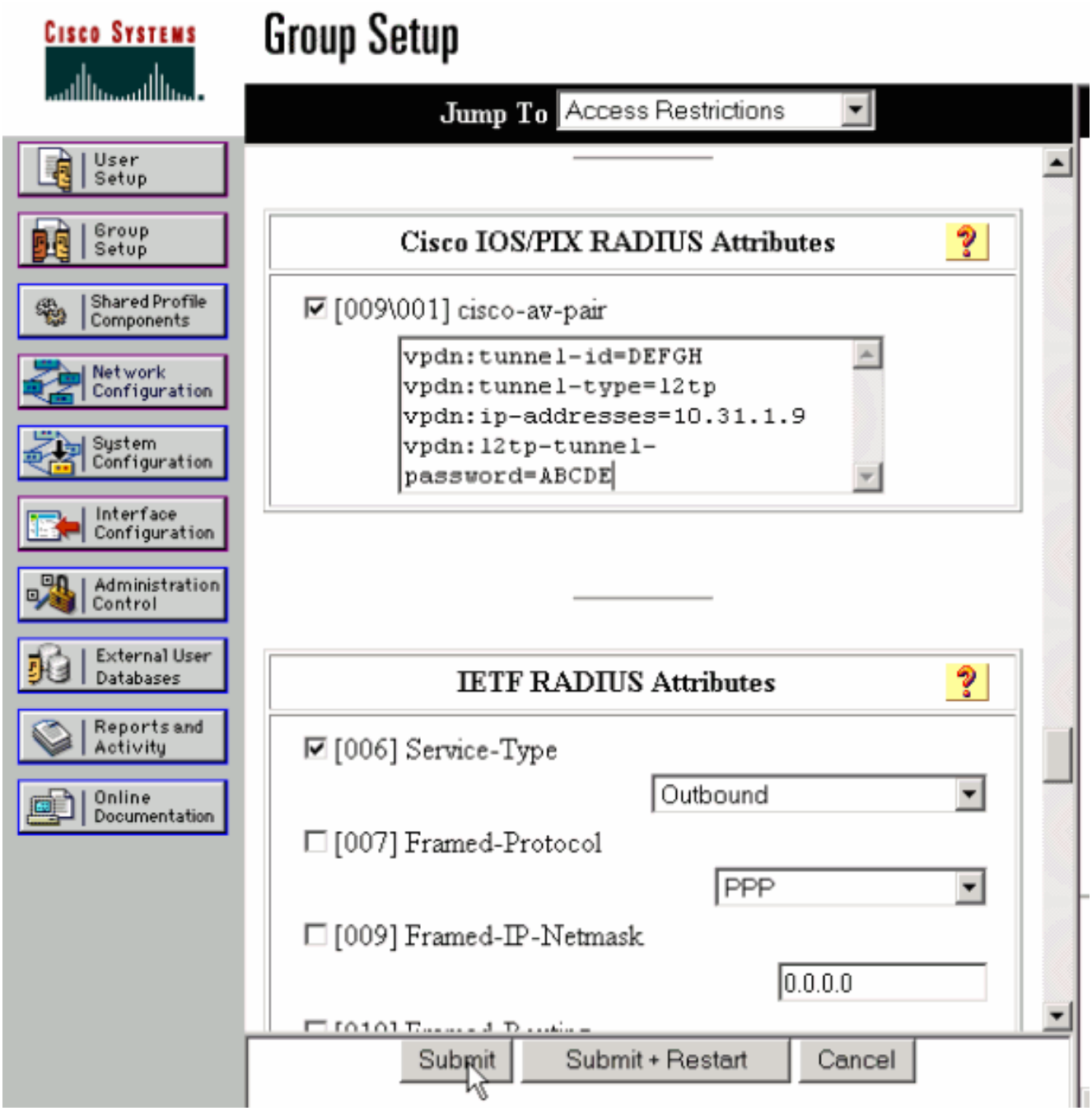
```
# ./ViewProfile -p 9900 -u janedoe@rtp.cisco.com
user = janedoe@rtp.cisco.com{
radius=Cisco {
check_items= {
2="rtp"
}
reply_attributes= {
6=2
7=1
}
}

}
```

Configuration RADIUS de LAC - Cisco Secure ACS pour Windows

Procédez comme suit :

1. Dans le secteur de configuration réseau, installez l'authentification de serveur d'accès à distance de LAC (NAS) pour utiliser le **RAYON (Cisco IOS/PIX)**.
2. Configurez l'utilisateur « rtp.cisco.com » avec le mot de passe cisco pour le bothplain et LE GERCEZ. C'est le nom d'utilisateur qui est utilisé pour les attributs de tunnel.
3. Cliquez sur en fonction le bouton de **configuration de groupe** dans la barre de navigation gauche. Sélectionnez le groupe que l'utilisateur appartient à et cliquez sur Edit les **configurations**. Faites descendre l'écran à la section de **RAYON IETF** et sélectionnez le **type de service de l'**attribut 6 comme **sortant**.*Si toutes les options vérifiables n'apparaissent pas, entrez dans la **configuration d'interface** et vérifiez les diverses cases pour les faire apparaître dans la zone de groupe.*
4. Dans la section d'attributs RADIUS de Cisco IOS/PIX au bas, cochez la case pour les Cisco-poids du commerce-**paires 009\001**, et introduisez au clavier ceci la case :`vpdn:tunnel-id=DEFGH`
   `vpdn:tunnel-type=l2tp`
   `vpdn:ip-addresses=10.31.1.9`
   `vpdn:l2tp-tunnel-password=ABCDE`Pour plus d'informations sur la configuration RADIUS sur le LAC, référez-vous au profil RADIUS à l'usage de la section de LAC dans le tunnel Protocol de la couche
   2.



Configuration RADIUS LNS - Cisco Secure ACS pour Windows

Procédez comme suit :

1. Configurez l'user-id **janedoe@rtp.cisco.com** et entrez n'importe quel mot de passe pour la brute et le CHAP.
2. Cliquez sur en fonction le bouton de **Group Setup** dans la barre gauche. Sélectionnez le groupe que l'utilisateur appartient à et cliquez sur Edit les **configurations**.
3. Dans la section pour des attributs RADIUS de l'Internet Engineering Task Force (IETF), **type de service** choisi **(attribut 6) = vue** et **protocole tramé (attribut 7)=PPP du** menu déroulant.**Remarque:** Vous devez également cliquer sur la case à cocher située à côté des attributs sélectionnés **type de service** et **protocole tramé**.

Configuration RADIUS de LAC - Merit RADIUS

Remarque: Des serveurs de Livingston et de mérite doivent fréquemment être modifiés pour prendre en charge des poids du commerce-paires de constructeur-particularité.

```
rtp.cisco.com   Password = "cisco"
        Service-Type = Outbound-User,
    cisco-avpair = "vpdn:tunnel-id=DEFGH",
    cisco-avpair = "vpdn:tunnel-type=l2tp",
    cisco-avpair = "vpdn:ip-addresses=10.31.1.9",
    cisco-avpair = "vpdn:l2tp-tunnel-password=ABCDE"
```

Pour plus d'informations sur la configuration RADIUS sur le LAC, référez-vous au profil RADIUS à l'usage de la section de LAC dans le tunnel Protocol de la couche 2.

Configuration RADIUS LNS - Merit RADIUS

```
janedoe@rtp.cisco.com   Password = "rtp",
                Service-Type = Framed,
                Framed-Protocol = PPP
```

Configurations de routeur

Ce document utilise les configurations suivantes.

- Configuration de routeur de LAC
- Configuration de routeur LNS

Configuration de routeur de LAC

```
LAC#show run Building configuration... Current
configuration: ! version 12.0 service timestamps debug
datetime service timestamps log uptime no service
password-encryption ! hostname LAC ! !--- AAA commands
needed to authenticate the user and obtain !--- VPDN
tunnel information. aaa new-model aaa authentication
login default local aaa authentication ppp default if-
needed radius aaa authorization network default radius
aaa accounting exec default start-stop radius aaa
accounting network default start-stop radius enable
secret level 7 5 $1$Dj3K$9jkyuJR6fJV2JO./Qt0lC1 enable
password ww ! username cse password 0 csecse username
john password 0 doe ip subnet-zero no ip domain-lookup !
jnj00=tfdfr vpdn enable ! !--- VPDN tunnel authorization
is based on the domain name !--- (the default is DNIS).
vpdn search-order domain ! ! ! interface Loopback0 no ip
address no ip directed-broadcast ! interface Ethernet0
ip address 10.31.1.6 255.255.255.0 no ip directed-
broadcast ! interface Serial0 no ip address no ip
directed-broadcast no ip mroute-cache shutdown !
interface Serial1 no ip address no ip directed-broadcast
shutdown ! interface Async1 ip unnumbered Ethernet0 no
ip directed-broadcast ip tcp header-compression passive
encapsulation ppp async mode dedicated peer default ip
address pool async no cdp enable ppp authentication chap
! interface Group-Async1 physical-layer async no ip
address no ip directed-broadcast ! ip local pool default
10.5.5.5 10.5.5.50 ip local pool async 10.7.1.1 10.7.1.5
ip classless ip route 0.0.0.0 0.0.0.0 10.31.1.1 ! !---
RADIUS server host and key. radius-server host
171.68.118.101 auth-port 1645 acct-port 1646 radius-
server key cisco ! line con 0 transport input none line
1 session-timeout 20 exec-timeout 0 0 password ww
```

```
autoselect during-login autoselect ppp modem InOut
transport preferred none transport output none stopbits
1 speed 38400 flowcontrol hardware line 2 16 modem InOut
transport input all speed 38400 flowcontrol hardware
line aux 0 line vty 0 4 password ww ! end
```

Configuration de routeur LNS

```
LNS#show run Building configuration... Current
configuration: ! ! Last configuration change at 12:17:54
UTC Sun Feb 7 1999 !==m6knr5yui6yt6egv2wr25nfd1rsion
12.0=4rservice exec-callback service timestamps debug
datetime service timestamps log uptime no service
password-encryption ! hostname LNS ! aaa new-model aaa
authentication login default local aaa authentication
ppp default radius local aaa authorization network
default radius local aaa accounting exec default start-
stop radius aaa accounting network default start-stop
radius enable secret 5 $1$pnYM$B.FveZjZpgA3C9ZPq/cma/
enable password ww ! username john password 0 doe !---
User the_LNS is used to authenticate the tunnel. !---
The password used here must match the vpdn:l2tp-tunnel-
password !--- configured in the LAC RADIUS server.
username the_LNS password 0 ABCDE ip subnet-zero ! !---
Enable VPDN on the LNS. vpdn enable ! !--- VPDN group
for connection from the LAC. vpdn-group 1 !--- This
command specifies that the router uses !--- virtual-
template 1 for tunnel-id DEFGH (which matches the
tunnel-id !--- configured in the LAC RADIUS server).
accept dialin l2tp virtual-template 1 remote DEFGH !---
The username used to authenticate this tunnel !--- is
the_LNS (configured above). local name the_LNS !
interface Ethernet0 ip address 10.31.1.9 255.255.255.0
no ip directed-broadcast ! !--- Virtual-template that is
used for the incoming connection. interface Virtual-
Template1 ip unnumbered Ethernet0 no ip directed-
broadcast peer default ip address pool default ppp
authentication chap ! interface Serial0 no ip address no
ip directed-broadcast no ip mroute-cache shutdown no
fair-queue ! interface Serial1 no ip address no ip
directed-broadcast shutdown ! interface Async1 ip
unnumbered Ethernet0 no ip directed-broadcast
encapsulation ppp async mode interactive peer default ip
address pool async ppp authentication chap ! ip local
pool default 10.6.1.1 10.6.1.5 ip local pool async
10.8.100.100 10.8.100.110 ip classless ip route 0.0.0.0
0.0.0.0 10.31.1.1 ! !--- RADIUS server host and key
information. radius-server host 171.68.120.194 auth-port
1645 acct-port 1646 radius-server key cisco ! line con 0
transport input none line 1 session-timeout 20 exec-
timeout 5 0 password ww autoselect during-login
autoselect ppp modem InOut transport input all escape-
character BREAK stopbits 1 speed 38400 flowcontrol
hardware line 2 8 line aux 0 line vty 0 4 password ww !
end
```

Vérifiez

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** — Affiche des informations au sujet de tout l'expédition actif de la couche 2 et tunnels L2TP dans le format de style du résumé.
- **IP de show caller** — Affiche une récapitulation d'informations sur l'appelant pour l'adresse IP que vous fournissez.

Dépannez

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

Dépannage des commandes

Remarque: Avant d'exécuter les commandes **debug**, référez-vous à la section **Informations importantes sur les commandes Debug**.

- **debug aaa authentication** — Affiche des informations sur l'authentification AAA/TACACS+.
- **autorisation de debug aaa** — Affiche des informations sur l'autorisation AAA/TACACS+.
- **debug aaa accounting** — Affiche des informations sur des événements imputables comme ils se produisent. L'information affichée par cette commande est indépendant du protocole de traçabilité utilisé pour virer l'information de comptabilité sur un serveur.
- **debug radius** — Affiche les informations de débogage détaillées associées avec le RAYON.
- **debug vtemplate** — Les informations de clonage d'affichages pour une interface d'accès virtuelle du temps où elle est copiée d'un modèle virtuel au temps l'interface d'accès virtuelle descend quand l'appel finit.
- **erreur de debug vpdn** — Affiche les erreurs qui empêchent un tunnel de PPP d'être établi ou les erreurs qui causent un tunnel établi d'être fermé.
- **événements de debug vpdn** — Affiche des messages au sujet des événements qui font partie d'établissement normal de tunnel de PPP ou arrêt.
- **debug vpdn l2x-errors** — Les affichages posent 2 erreurs de protocole qui empêchent l'établissement de la couche 2 ou empêchent son fonctionnement normal.
- **debug vpdn l2x-events** — Affiche des messages au sujet des événements qui font partie d'établissement normal de tunnel de PPP ou arrêt pour la couche 2.
- **l2tp sequencing de debug vpdn** — Affiche des messages au sujet de L2TP.

Sortie de débogage

Pour la description détaillée du L2TP met au point, se rapporte à l'installation et à la désinstallation de tunnel L2TP.

Bon debug de routeur de LAC

```
LAC#show debug General OS: AAA Authentication debugging is on AAA Authorization debugging is on
AAA Accounting 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 on L2TP data sequencing
debugging is on VTEMPLATE: Virtual Template debugging is on Radius protocol debugging is on LAC#
Feb 7 12:22:16: As1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially 2d18h: %LINK-3-UPDOWN: Interface
Async1, changed state to up Feb 7 12:22:17: As1 VPDN: Looking for tunnel -- rtp.cisco.com -- Feb
7 12:22:17: AAA: parse name=Async1 idb type=10 tty=1 Feb 7 12:22:17: AAA: name=Async1 flags=0x11
```

type=4 shelf=0 slot=0 adapter=0 port=1 channel=0 Feb 7 12:22:17: AAA/AUTHEN: create_user (0x25BA84) user='rtp.cisco.com' ruser='' port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0 Feb 7 12:22:17: AAA/AUTHOR/VPDN (6239469): Port='Async1' list='default' service=NET Feb 7 12:22:17: AAA/AUTHOR/VPDN: (6239469) user='rtp.cisco.com' Feb 7 12:22:17: AAA/AUTHOR/VPDN: (6239469) send AV service=ppp Feb 7 12:22:17: AAA/AUTHOR/VPDN: (6239469) send AV protocol=vpdn Feb 7 12:22:17: AAA/AUTHOR/VPDN (6239469) found list "default" Feb 7 12:22:17: AAA/AUTHOR/VPDN: (6239469) Method=RADIUS Feb 7 12:22:17: RADIUS: authenticating to get author data Feb 7 12:22:17: RADIUS: ustruct sharecount=2 Feb 7 12:22:17: RADIUS: Initial Transmit Async1 id 66 171.68.118.101:1645, Access-Request, len 77 Feb 7 12:22:17: Attribute 4 6 0A1F0106 Feb 7 12:22:17: Attribute 5 6 00000001 Feb 7 12:22:17: Attribute 61 6 00000000 Feb 7 12:22:17: Attribute 1 15 7274702E Feb 7 12:22:17: Attribute 2 18 6AB5A2B0 Feb 7 12:22:17: Attribute 6 6 00000005 Feb 7 12:22:17: RADIUS: Received from id 66 171.68.118.101:1645, Access-Accept, len 158 Feb 7 12:22:17: Attribute 6 6 00000005 Feb 7 12:22:17: Attribute 26 28 0000000901167670 Feb 7 12:22:17: Attribute 26 29 0000000901177670 Feb 7 12:22:17: Attribute 26 36 00000009011E7670 Feb 7 12:22:17: Attribute 26 39 0000000901217670 Feb 7 12:22:17: RADIUS: saved authorization data for user 25BA84 at 24C488 *!--- RADIUS server supplies the VPDN tunnel attributes.* **Feb 7 12:22:17: RADIUS: cisco AVPair "vpdn:tunnel-id=DEFGH" Feb 7 12:22:17: RADIUS: cisco AVPair "vpdn:tunnel-type=l2tp" Feb 7 12:22:17: RADIUS: cisco AVPair "vpdn:ip-addresses=10.31.1.9," Feb 7 12:22:17: RADIUS: cisco AVPair "vpdn:l2tp-tunnel-password=ABCDE"** Feb 7 12:22:17: AAA/AUTHOR (6239469): Post authorization status = PASS_ADD Feb 7 12:22:17: AAA/AUTHOR/VPDN: Processing AV service=ppp Feb 7 12:22:17: AAA/AUTHOR/VPDN: Processing AV protocol=vpdn Feb 7 12:22:17: AAA/AUTHOR/VPDN: Processing AV tunnel-id=DEFGH Feb 7 12:22:17: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp Feb 7 12:22:17: AAA/AUTHOR/VPDN: Processing AV ip-addresses=10.31.1.9, Feb 7 12:22:17: AAA/AUTHOR/VPDN: Processing AV l2tp-tunnel-password=ABCDE Feb 7 12:22:17: As1 VPDN: Get tunnel info for rtp.cisco.com with LAC DEFGH, IP 10.31.1.9 Feb 7 12:22:17: AAA/AUTHEN: free_user (0x25BA84) user='rtp.cisco.com' ruser='' port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0 **Feb 7 12:22:17: As1 VPDN: Forward to address 10.31.1.9** Feb 7 12:22:17: As1 VPDN: Forwarding... Feb 7 12:22:17: AAA: parse name=Async1 idb type=10 tty=1 Feb 7 12:22:17: AAA: name=Async1 flags=0x11 type=4 shelf=0 slot=0 adapter=0 port=1 channel=0 Feb 7 12:22:17: AAA/AUTHEN: create_user (0xB7918) user='janedoe@rtp.cisco.com' ruser='' port='Async1' rem_addr='async' authen_type=CHAP service=PPP priv=1 Feb 7 12:22:17: As1 VPDN: Bind interface direction=1 Feb 7 12:22:17: Tnl/Cl 51/1 L2TP: Session FS enabled Feb 7 12:22:17: Tnl/Cl 51/1 L2TP: Session state change from idle to wait-for-tunnel Feb 7 12:22:17: As1 51/1 L2TP: Create session Feb 7 12:22:17: Tnl 51 L2TP: SM State idle Feb 7 12:22:17: Tnl 51 L2TP: O SCCRQ Feb 7 12:22:17: Tnl 51 L2TP: Tunnel state change from idle to wait-ctl-reply Feb 7 12:22:17: Tnl 51 L2TP: SM State wait-ctl-reply **Feb 7 12:22:17: As1 VPDN: janedoe@rtp.cisco.com is forwarded** Feb 7 12:22:17: Tnl 51 L2TP: I SCCRP from the_LNS *!--- Tunnel authentication is successful.* **Feb 7 12:22:17: Tnl 51 L2TP: Got a challenge from remote peer, the_LNS Feb 7 12:22:17: Tnl 51 L2TP: Got a response from remote peer, the_LNS Feb 7 12:22:17: Tnl 51 L2TP: Tunnel Authentication success** Feb 7 12:22:17: Tnl 51 L2TP: Tunnel state change from wait-ctl-reply to established Feb 7 12:22:17: Tnl 51 L2TP: O SCCCN to the_LNS tnlid 38 Feb 7 12:22:17: Tnl 51 L2TP: SM State established Feb 7 12:22:17: As1 51/1 L2TP: O ICRQ to the_LNS 38/0 Feb 7 12:22:17: As1 51/1 L2TP: Session state change from wait-for-tunnel to wait-reply Feb 7 12:22:17: As1 51/1 L2TP: O ICCN to the_LNS 38/1 Feb 7 12:22:17: As1 51/1 L2TP: Session state change from wait-reply to established 2d18h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state to up LAC#

Bon debug de routeur LNS

LNS#**show debug** General OS: AAA Authentication debugging is on AAA Authorization debugging is on AAA Accounting 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 on L2TP data sequencing debugging is on VTEMPLATE: Virtual Template debugging is on Radius protocol debugging is on LNS# Feb 7 12:22:16: L2TP: I SCCRQ from DEFGH tnl 51 **Feb 7 12:22:16: Tnl 38 L2TP: New tunnel created for remote DEFGH, address 10.31.1.6** Feb 7 12:22:16: Tnl 38 L2TP: Got a challenge in SCCRQ, DEFGH Feb 7 12:22:16: Tnl 38 L2TP: O SCCRP to DEFGH tnlid 51 Feb 7 12:22:16: Tnl 38 L2TP: Tunnel state change from idle to wait-ctl-reply Feb 7 12:22:16: Tnl 38 L2TP: I SCCCN from DEFGH tnl 51 Feb 7 12:22:16: Tnl 38 L2TP: Got a Challenge Response in SCCCN from DEFGH Feb 7 12:22:16: Tnl 38 L2TP: Tunnel Authentication success Feb 7 12:22:16: Tnl 38 L2TP: Tunnel state change from wait-ctl-reply to established Feb 7 12:22:16: Tnl 38 L2TP: SM State established Feb 7 12:22:17: Tnl 38 L2TP: I ICRQ from DEFGH tnl 51 Feb 7 12:22:17: Tnl/Cl 38/1 L2TP: Session FS enabled Feb 7 12:22:17: Tnl/Cl 38/1 L2TP: Session state change from idle to wait-for-tunnel Feb 7 12:22:17: Tnl/Cl 38/1 L2TP: New session created Feb 7 12:22:17: Tnl/Cl 38/1 L2TP: O ICRP to DEFGH 51/1 Feb 7 12:22:17: Tnl/Cl 38/1 L2TP: Session state change from wait-for-tunnel to wait-connect Feb 7 12:22:17: Tnl/Cl 38/1 L2TP: I ICCN from DEFGH tnl 51, cl 1 Feb 7 12:22:17: Tnl/Cl 38/1 L2TP:

Session state change from wait-connect to established Feb 7 12:22:17: Vi1 VTEMPLATE: Reuse Vi1, recycle queue size 0 Feb 7 12:22:17: Vi1 VTEMPLATE: Hardware address 00e0.1e68.942c *!--- Use Virtual-template 1 for this user.* **Feb 7 12:22:17: Vi1 VPDN: Virtual interface created for janedoe@rtp.cisco.com Feb 7 12:22:17: Vi1 VPDN: Set to Async interface Feb 7 12:22:17: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking** Feb 7 12:22:17: Vi1 VTEMPLATE: Has a new cloneblk vtemplate, now it has vtemplate Feb 7 12:22:17: Vi1 VTEMPLATE: ********** CLONE VACCESS1 ********** Feb 7 12:22:17: Vi1 VTEMPLATE: Clone from Virtual-Template1 interface Virtual-Access1 default ip address no ip address encap ppp ip unnum eth 0 no ip directed-broadcast peer default ip address pool default ppp authen chap end Feb 7 12:22:18: janedoe@rtp.cisco.com 38/1 L2TP: Session with no hwidb 02:23:59: %LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up Feb 7 12:22:19: Vi1 AAA/AUTHOR/FSM: (0): LCP succeeds trivially Feb 7 12:22:19: Vi1 VPDN: Bind interface direction=2 Feb 7 12:22:19: Vi1 VPDN: PPP LCP accepted rcv CONFACK Feb 7 12:22:19: Vi1 VPDN: PPP LCP accepted sent CONFACK Feb 7 12:22:19: Vi1 L2X: Discarding packet because of no mid/session Feb 7 12:22:19: AAA: parse name=Virtual-Access1 idb type=21 tty=-1 Feb 7 12:22:19: AAA: name=Virtual-Access1 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=1 channel=0 Feb 7 12:22:19: AAA/AUTHEN: create_user (0x2462A0) user='janedoe@rtp.cisco.com' ruser='' port='Virtual-Access1' rem_addr='' authen_type=CHAP service=PPP priv=1 Feb 7 12:22:19: AAA/AUTHEN/START (2229277178): port='Virtual-Access1' list='' action=LOGIN service=PPP Feb 7 12:22:19: AAA/AUTHEN/START (2229277178): using "default" list Feb 7 12:22:19: AAA/AUTHEN/START (2229277178): Method=RADIUS Feb 7 12:22:19: RADIUS: ustruct sharecount=1 Feb 7 12:22:19: RADIUS: Initial Transmit Virtual-Access1 id 78 171.68.120.194:1645, Access-Request, len 92 Feb 7 12:22:19: Attribute 4 6 0A1F0109 Feb 7 12:22:19: Attribute 5 6 00000001 Feb 7 12:22:19: Attribute 61 6 00000005 Feb 7 12:22:19: Attribute 1 23 6464756E Feb 7 12:22:19: Attribute 3 19 34A66389 Feb 7 12:22:19: Attribute 6 6 00000002 Feb 7 12:22:19: Attribute 7 6 00000001 Feb 7 12:22:19: RADIUS: Received from id 78 171.68.120.194:1645, Access-Accept, len 32 Feb 7 12:22:19: Attribute 6 6 00000002 Feb 7 12:22:19: Attribute 7 6 00000001 Feb 7 12:22:19: AAA/AUTHEN (2229277178): status = PASS Feb 7 12:22:19: Vi1 AAA/AUTHOR/LCP: Authorize LCP Feb 7 12:22:19: AAA/AUTHOR/LCP Vi1 (1756915964): Port='Virtual-Access1' list='' service=NET Feb 7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964) user='janedoe@rtp.cisco.com' Feb 7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964) send AV service=ppp Feb 7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964) send AV protocol=lcp Feb 7 12:22:19: AAA/AUTHOR/LCP (1756915964) found list "default" Feb 7 12:22:19: AAA/AUTHOR/LCP: Vi1 (1756915964) Method=RADIUS Feb 7 12:22:19: AAA/AUTHOR (1756915964): Post authorization status = PASS_REPL Feb 7 12:22:19: Vi1 AAA/AUTHOR/LCP: Processing AV service=ppp Feb 7 12:22:19: AAA/ACCT/NET/START User janedoe@rtp.cisco.com, Port Virtual-Access1, List "" Feb 7 12:22:19: AAA/ACCT/NET: Found list "default" Feb 7 12:22:19: Vi1 AAA/AUTHOR/FSM: (0): Can we start IPCP? Feb 7 12:22:19: AAA/AUTHOR/FSM Vi1 (1311872588): Port='Virtual-Access1' list='' service=NET Feb 7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588) user='janedoe@rtp.cisco.com' Feb 7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588) send AV service=ppp Feb 7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588) send AV protocol=ip Feb 7 12:22:19: AAA/AUTHOR/FSM (1311872588) found list "default" Feb 7 12:22:19: AAA/AUTHOR/FSM: Vi1 (1311872588) Method=RADIUS Feb 7 12:22:19: AAA/AUTHOR (1311872588): Post authorization status = PASS_REPL Feb 7 12:22:19: Vi1 AAA/AUTHOR/FSM: We can start IPCP Feb 7 12:22:19: RADIUS: ustruct sharecount=2 Feb 7 12:22:19: RADIUS: Initial Transmit Virtual-Access1 id 79 171.68.120.194:1646, Accounting-Request, len 101 Feb 7 12:22:19: Attribute 4 6 0A1F0109 Feb 7 12:22:19: Attribute 5 6 00000001 Feb 7 12:22:19: Attribute 61 6 00000005 Feb 7 12:22:19: Attribute 1 23 6464756E Feb 7 12:22:19: Attribute 40 6 00000001 Feb 7 12:22:19: Attribute 45 6 00000001 Feb 7 12:22:19: Attribute 6 6 00000002 Feb 7 12:22:19: Attribute 44 10 30303030 Feb 7 12:22:19: Attribute 7 6 00000001 Feb 7 12:22:19: Attribute 41 6 00000000 Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want 0.0.0.0 Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want 0.0.0.0 Feb 7 12:22:19: RADIUS: Received from id 79 171.68.120.194:1646, Accounting-response, len 20 Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Start. Her address 0.0.0.0, we want 10.6.1.1 Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Authorization succeeded Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Done. Her address 0.0.0.0, we want 10.6.1.1 Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Start. Her address 10.6.1.1, we want 10.6.1.1 Feb 7 12:22:19: AAA/AUTHOR/IPCP Vi1 (2909132255): Port='Virtual-Access1' list='' service=NET Feb 7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255) user='janedoe@rtp.cisco.com' Feb 7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255) send AV service=ppp Feb 7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255) send AV protocol=ip Feb 7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255) send AV addr*10.6.1.1 Feb 7 12:22:19: AAA/AUTHOR/IPCP (2909132255) found list "default" Feb 7 12:22:19: AAA/AUTHOR/IPCP: Vi1 (2909132255) Method=RADIUS Feb 7 12:22:19: AAA/AUTHOR (2909132255): Post authorization status = PASS_REPL Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Reject 10.6.1.1, using 10.6.1.1 Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing AV service=ppp Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Processing AV addr*10.6.1.1 Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Authorization

```
succeeded Feb 7 12:22:19: Vi1 AAA/AUTHOR/IPCP: Done. Her address 10.6.1.1, we want 10.6.1.1
02:24:00: %LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1, changed state to up
LNS#
```

Ce qui peut aller mal - Mauvais debug de LAC

```
LAC#show debug General OS: AAA Authentication debugging is on AAA Authorization debugging is on
AAA Accounting 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 on L2TP data sequencing
debugging is on VTEMPLATE: Virtual Template debugging is on Radius protocol debugging is on
```

L'utilisateur entre comme janedoe@sj.cisco.com (au lieu de janedoe@rtp.cisco.com), mais le serveur de RAYON de LAC n'identifie pas ce domaine.

```
Feb 7 13:26:48: RADIUS: Received from id 86 171.68.118.101:1645, Access-Reject, len 46 Feb 7
13:26:48: Attribute 18 26 41757468 Feb 7 13:26:48: RADIUS: failed to get authorization data:
authen status = 2 %VPDN-6-AUTHORFAIL: L2F NAS LAC, AAA authorization failure for As1 user
janedoe@sj.cisco.com
```

Ceux-ci met au point l'exposition une situation où les informations de tunnel sont reçues, mais avec une adresse IP incorrect pour l'autre extrémité du tunnel. Les tentatives d'utilisateur d'établir une session, mais ne peuvent pas se connecter.

```
Feb 7 13:32:45: As1 VPDN: Forward to address 1.1.1.1 Feb 7 13:32:45: As1 VPDN: Forwarding... Feb
7 13:32:45: Tnl 56 L2TP: Tunnel state change from idle to wait-ctl-reply Feb 7 13:32:46: As1
56/1 L2TP: Discarding data packet because tunnel is not open
```

Ceux-ci met au point l'exposition une situation quand il y a une non-concordance de mot de passe de tunnel. Sur le LNS, « le mot de passe ABCDE de the_LNS de nom d'utilisateur » est changé « aux déchets de mot de passe de the_LNS de nom d'utilisateur » de sorte que l'authentification de tunnel échoue une fois tentée.

```
Feb 7 13:39:35: Tnl 59 L2TP: Tunnel Authentication fails for the_LNS Feb 7 13:39:35: Tnl 59
L2TP: Expected E530DA13B826685C678589250C0BF525 Feb 7 13:39:35: Tnl 59 L2TP: Got
E09D90E8A91CF1014C91D56F65BDD052 Feb 7 13:39:35: Tnl 59 L2TP: O StopCCN to the_LNS tnlid 44 Feb
7 13:39:35: Tnl 59 L2TP: Tunnel state change from wait-ctl-reply to shutting-down Feb 7
13:39:35: Tnl 59 L2TP: Shutdown tunnel
```

Ce qui peut aller mal - Mauvais debug de LNS

```
LNS#show debug General OS: AAA Authentication debugging is on AAA Authorization debugging is on
AAA Accounting 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 on L2TP data sequencing
debugging is on VTEMPLATE: Virtual Template debugging is on Radius protocol debugging is on LNS#
```

Dans cet exemple, « recevez le virtual-template de composition 1 l2tp DEFGH que distant » est changé « reçoit l'ordure distante du virtual-template 1 du dialin l2tp ». Le LNS peut plus ne trouver le tunnel DEFGH (c'est « ordure » à la place).

```
Feb 7 13:45:32: L2TP: I SCCRQ from DEFGH tnl 62 Feb 7 13:45:32: L2X: Never heard of DEFGH Feb 7
13:45:32: L2TP: Could not find info block for DEFGH
```

Enregistrements des comptes LNS

```
10.31.1.9 janedoe@rtp.cisco.com 1 - start
    server=rtp-cherry time=09:23:53
    date=02/ 6/1999 task_id=0000001C
Sat Feb 6 12:23:53 1999
        Client-Id = 10.31.1.9
        Client-Port-Id = 1
```

```
        NAS-Port-Type = Virtual
        User-Name = "janedoe@rtp.cisco.com"
        Acct-Status-Type = Start
        Acct-Authentic = RADIUS
        User-Service-Type = Framed-User
        Acct-Session-Id = "0000001C"
        Framed-Protocol = PPP
        Acct-Delay-Time = 0


10.31.1.9 janedoe@rtp.cisco.com 1 - stop
    server=rtp-cherry time=09:24:46
    date=02/ 6/1999 task_id=0000001C
Sat Feb  6 12:24:46 1999
        Client-Id = 10.31.1.9
        Client-Port-Id = 1
        NAS-Port-Type = Virtual
        User-Name = "janedoe@rtp.cisco.com"
        Acct-Status-Type = Stop
        Acct-Authentic = RADIUS
        User-Service-Type = Framed-User
        Acct-Session-Id = "0000001C"
        Framed-Protocol = PPP
        Framed-Address = 10.6.1.1
        Acct-Terminate-Cause = Lost-Carrier
        Acct-Input-Octets = 678
        Acct-Output-Octets = 176
        Acct-Input-Packets = 17
        Acct-Output-Packets = 10
        Acct-Session-Time = 53
        Acct-Delay-Time = 0
```

Informations connexes

- Accès distant d'Access VPDN utilisant L2TP
- Tunnel Protocol de la couche 2
- Page d'assistance RADIUS
- Cisco Secure ACS pour la page d'assistance de Windows
- Cisco Secure ACS pour la page de support UNIX
- Demandes de commentaires (RFC)
- Support technique - Cisco Systems