Configuración de Capa 2 de autenticación de protocolo de túnel mediante servidor RADIUS

Contenido

Introducción

Este documento muestra cómo configurar un escenario de Virtual Private Dialup Network (VPDN) de Layer 2 Tunnel Protocol (L2TP) usando atributos de túnel descargados de un servidor RADIUS. En este ejemplo, el L2TP Access Concentrator (LAC) recibe la conexión entrante y entra en contacto con el servidor RADIUS LAC. El servidor RADIUS busca los atributos del túnel para el dominio del usuario (por ejemplo, cisco.com) y pasa los atributos del túnel al LAC. Según estos atributos, el LAC inicia un túnel con el Servidor de Red L2TP (LNS). Una vez que se establece el túnel, el LNS autentica al usuario final usando su propio servidor RADIUS.

Nota: Este documento asume que el NAS (LAC) se ha configurado para el acceso general del dial. Para más información sobre cómo configurar el dial, refiera a configurar el Basic AAA

RADIUS para los clientes dial in.

Para más información sobre el L2TP y los VPDN, refiera a estos documentos:

- Introducción a VPDN'
- Configurar las Redes privadas virtuales
- Protocolo de túnel de capa 2

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Dos Cisco 2511 Router
- Versión 12.0(2)T del software del IOS de Cisco
- Cisco Secure ACS para UNIX, Cisco Secure ACS para Windows o Merit RADIUS

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

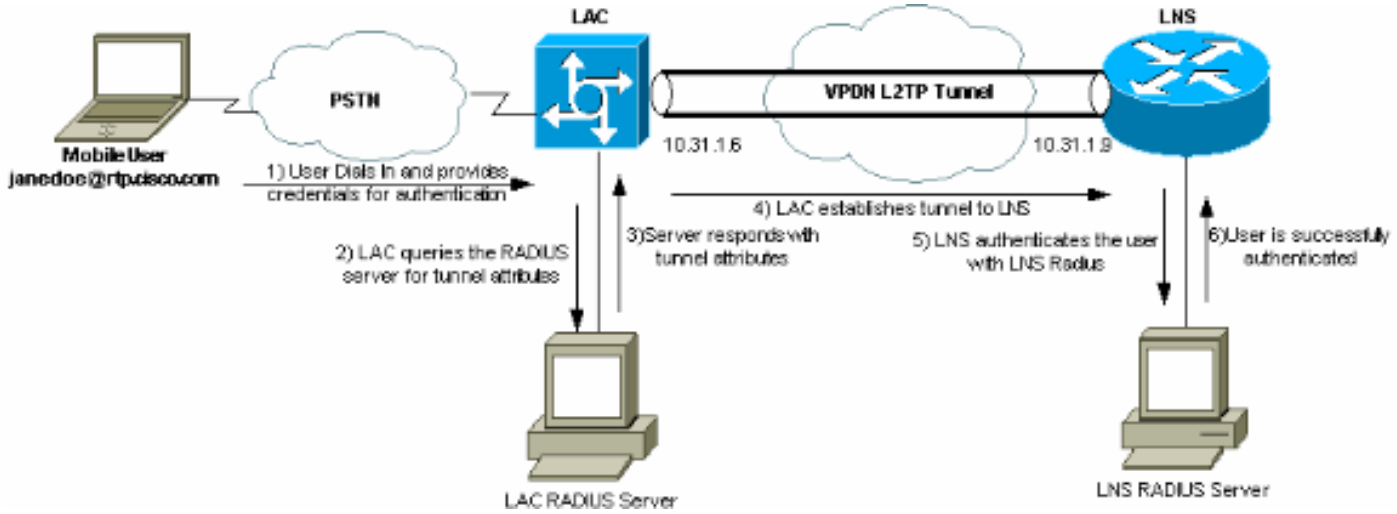
Configuración del servidor de RADIUS

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes registrados).

Diagrama de la red

Este documento utiliza la configuración de red que se muestra en el siguiente diagrama.



Configuración de RADIUS LAC - Cisco Secure ACS para UNIX

La configuración de RADIUS LAC incluye al usuario “rtp.cisco.com” (que es el dominio usado por el cliente). La contraseña para este usuario debe ser 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"
}
}
}
```

Para más información sobre la configuración de RADIUS en el LAC, refiera al perfil de RADIUS para uso de la sección LAC dentro del Tunnel Protocol de la capa 2.

Configuración de RADIUS LNS - Cisco Secure ACS para UNIX

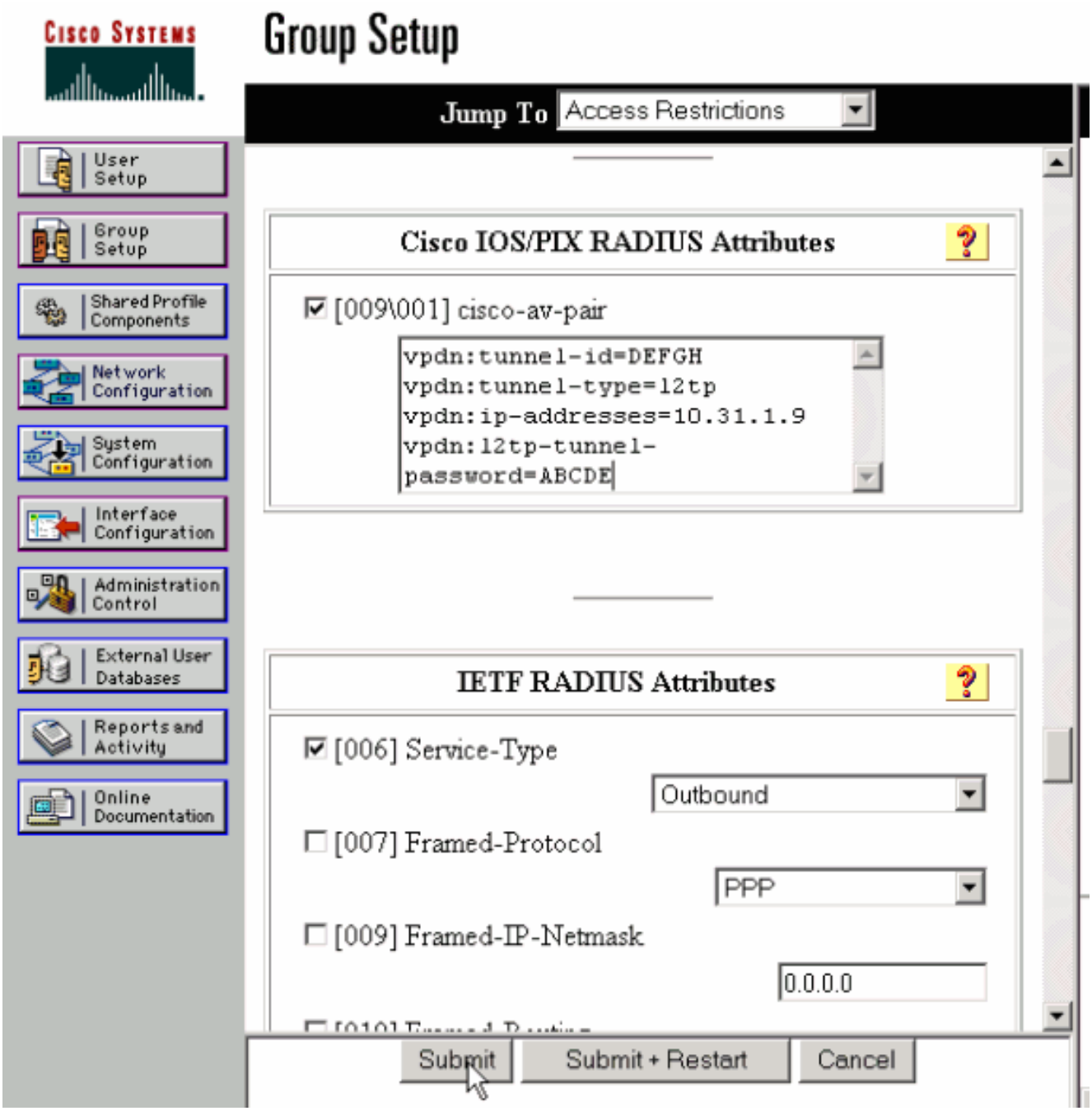
```
# ./ViewProfile -p 9900 -u janedoe@rtp.cisco.com
user = janedoe@rtp.cisco.com{
radius=Cisco {
check_items= {
2="rtp"
}
reply_attributes= {
6=2
7=1
}
}

}
```

Configuración de RADIUS LAC - Cisco Secure ACS for Windows

Complete estos pasos:

1. En el área de la configuración de red, configure la autenticación del LAC Network Access Server (NAS) para utilizar **RADIUS (Cisco IOS/PIX)**.
2. Configure al usuario “rtp.cisco.com” con la palabra clave Cisco para el bothplain y AGRIÉTELO. Éste es el nombre de usuario que se utiliza para los atributos del túnel.
3. Haga clic en el botón de la **configuración de grupo** en la barra de navegación izquierda. Seleccione al grupo que el usuario pertenece a y el tecleo **edita las configuraciones**. Navegue hacia abajo a la sección del **IETF RADIUS** y seleccione el **tipo de servicio del** atributo 6 como **saliente**.*Si no aparece toda la opciones que pueden marcar, entre la* ***configuración de la interfaz*** *y marque los diversos cuadros para hacer que aparecen en el área del grupo.*
4. En la sección de los atributos de RADIUS de Cisco IOS/PIX en la parte inferior, marque el cuadro para el **Cisco-av-pair 009\001**, y teclee esto en el cuadro:`vpdn:tunnel-id=DEFGH`
   `vpdn:tunnel-type=l2tp`
   `vpdn:ip-addresses=10.31.1.9`
   `vpdn:l2tp-tunnel-password=ABCDE`Para más información sobre la configuración de RADIUS en el LAC, refiera al perfil de RADIUS para uso de la sección LAC dentro del Tunnel Protocol de la capa
   2.



Configuración de RADIUS LNS - Cisco Secure ACS for Windows

Complete estos pasos:

1. Configure la identificación del usuario **janedoe@rtp.cisco.com** y entre cualquier contraseña para el llano y la GRIETA.
2. Haga clic en el **botón Group Setup Button** en la barra izquierda. Seleccione al grupo que el usuario pertenece a y el tecleo **edita las configuraciones**.
3. En la sección para los atributos de RADIUS de la Fuerza de tareas de ingeniería en Internet (IETF) (IETF), **tipo de servicio** selecto **(atributo 6) = Framed** y **Protocolo Entramado (atributo 7)=PPP del** menú desplegable.**Nota:** Usted debe también hacer clic el checkbox situado al lado de los atributos seleccionados **tipo de servicio** y **Protocolo Entramado**.

Configuración de LAC RADIUS – Merit RADIUS

Nota: Los servidores de Livingston y del Merit se deben modificar con frecuencia para soportar los AV-pares específicos del vendedor.

```
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"
```

Para más información sobre la configuración de RADIUS en el LAC, refiera al perfil de RADIUS para uso de la sección LAC dentro del Tunnel Protocol de la capa 2.

Configuración de LNS RADIUS - Merit RADIUS

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

Configuración del router

Este documento usa estas configuraciones.

- Configuración del router LAC
- Configuración del router LNS

Configuración del router 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
```

Configuración del router 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
```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta Output Interpreter (sólo para clientes registrados) permite utilizar algunos

comandos “show” y ver un análisis del resultado de estos comandos.

- **muestre el túnel del vpdn** — La información de las visualizaciones sobre toda la expedición de la capa activa 2 y L2TP hace un túnel en el formato resumido.
- show caller ip: Muestra un resumen de la información de la parte llamadora para la dirección de IP proporcionada.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

Nota: Antes de ejecutar un comando debug, consulte Información Importante sobre Comandos Debug.

- debug aaa authentication — Muestra información sobre autenticación de AAA/TACACS+.
- **debug aaa authorization** — Visualiza la información sobre la autorización AAA/TACACS+.
- debug aaa accounting — Muestra información sobre todos los eventos que se puedan registrar a medida que ocurren. La información mostrada por este comando es independiente del protocolo de la cuenta utilizado para transferir la información de la cuenta al servidor.
- debug radius - Muestra información detallada de depuración asociada con el RADIUS.
- debug vtemplate - Muestra información de clonación para una interfaz de acceso virtual desde el momento en que se clona desde una plantilla virtual hasta el momento en que la interfaz de acceso virtual se cae al finalizar la llamada.
- debug vpdn error — Muestra errores que evitan que se establezca un túnel PPP o errores que provocan que un túnel establecido se cierre.
- debug vpdn events — Muestra mensajes relativos a eventos que forman parte del establecimiento o cierre normal del túnel PPP.
- **debug vpdn l2x-errors** — Visualiza los errores del protocolo de la capa 2 que previenen el establecimiento de la capa 2 o previenen su funcionamiento normal.
- **debug vpdn l2x-events** — Visualiza los mensajes sobre los eventos que son establecimiento del túnel normal de la parte de PPP o apagan para la capa 2.
- **debug vpdn l2tp-sequencing** — Visualiza los mensajes sobre el L2TP.

‘Resultado de debug’

Para la descripción detallada de los debugs L2TP, refiera a la configuración de túnel y al desmontaje L2TP.

Depuración correcta del router 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#

Depuración correcta del router 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#
```

'Lo que puede salir mal – mala depuración desde 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
```

El usuario entra como janedoe@sj.cisco.com (en vez de janedoe@rtp.cisco.com), pero el servidor de RADIUS LAC no reconoce este dominio.

```
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
```

Estos debugs muestran una situación donde se recibe la información del túnel, pero con una dirección IP no válida para el otro extremo del túnel. El usuario intenta establecer una sesión, pero no puede conectar.

```
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
```

Estos debugs muestran una situación cuando hay una discordancía de la contraseña del túnel. En el LNS, "la contraseña ABCDE del the_LNS del nombre de usuario" se cambia "al password garbage del the_LNS del nombre de usuario" de modo que la autenticación de túnel falle cuando esté intentada.

```
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
```

Lo que puede salir mal – Mala depuración desde 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#
```

En este ejemplo, el "accept dialing l2tp virtual-template 1 remote defgh" se cambia al "accept dialin l2tp virtual-template 1 remote junk". El LNS puede encontrar no más el túnel DEFGH (es "desperdicios" en lugar de otro).

```
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
```

Registros contables 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
```

Información Relacionada

- Dial-in del acceso VPDN usando el L2TP
- Protocolo de túnel de capa 2
- Página de soporte de RADIUS
- Página de soporte de Cisco Secure ACS para Windows
- Página de soporte de Cisco Secure ACS para Windows
- Solicitudes de Comentarios (RFC)
- Soporte Técnico - Cisco Systems