Configuration de l'authentification TACACS+ pour les réseaux VPDN

Table des matières

Introduction

Un réseau privé virtuel à accès commuté (VPDN) permet à un réseau privé en service de se répartir sur des serveurs à accès distant (définis comme concentrateur L2TP Access [LAC]). Lorsqu'un client PPP (Point-to-Point Protocol) compose un numéro dans un LAC, le LAC détermine qu'il doit transférer cette session PPP sur un serveur de réseau L2TP (LNS) pour ce client, qui authentifie ensuite l'utilisateur et lance la négociation PPP. Une fois la configuration PPP terminée, toutes les trames sont envoyées via la LAC au client et au LNS.

Cet exemple de configuration vous permet d'utiliser l'authentification TACACS+ avec des réseaux commutés privés virtuels (VPDN). La LAC interroge le serveur TACACS+, détermine le LNS à transférer à l'utilisateur et établit le tunnel approprié.

Pour plus d'informations sur les VPDN, référez-vous à Présentation des VPDN.

Conditions préalables

Exigences

Aucune exigence spécifique n'est associée à ce document.

Composants utilisés

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

- Cisco Secure ACS pour UNIX version 2.x.x et ultérieure ou logiciel gratuit TACACS+
- Logiciel Cisco IOS® versions 11.2 et ultérieures

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 utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurer

Cette section présente les informations nécessaires à la configuration des fonctionnalités décrites dans ce document.

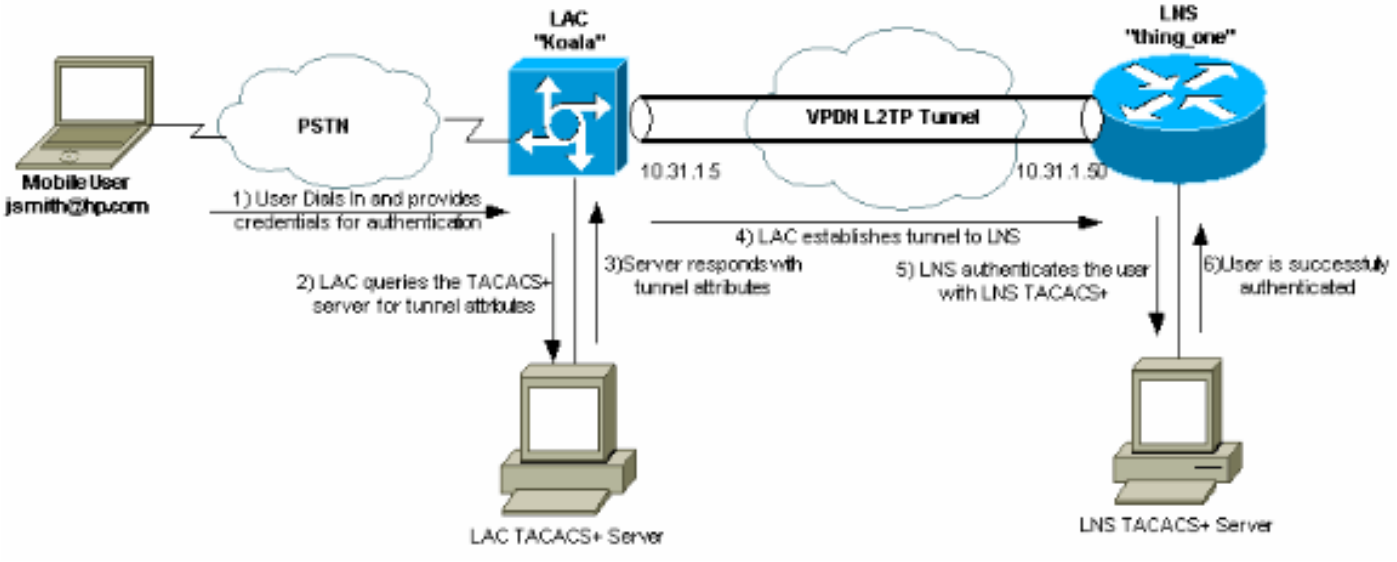
Dans cet exemple, l'utilisateur est "jsmith@hp.com" avec le mot de passe "test". Lorsque « jsmith@hp.com » compose un numéro sur le routeur ISP, ce dernier envoie l'ID utilisateur « hp.com » au serveur TACACS+ ISP. Le serveur du FAI trouve l'ID utilisateur « hp.com » et renvoie son ID de tunnel (« isp »), l'adresse IP du routeur de la passerelle d'accueil (HGW) (10.31.1.50), le mot de passe du serveur d'accès réseau (NAS) (« hello ») et le mot de passe de la passerelle (« there ») au routeur du FAI.

Le routeur ISP initie un tunnel et se connecte au routeur HGW, qui transfère les mots de passe pour l'ID d'utilisateur « hp-gw » (« there »), puis l'ID d'utilisateur « isp » (« hello ») au serveur HGW TACACS+. Une fois les tunnels établis, le routeur ISP transfère au routeur HGW l'ID utilisateur (« jsmith@hp.com ») et le mot de passe (« test ») de l'utilisateur qui compose le numéro. Cet utilisateur est authentifié sur le serveur HGW. Dans les exemples de configuration de ce document, le nom d'hôte du routeur ISP est « koala » et le nom d'hôte du routeur HGW est « thing_one ».

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 indiquée dans le diagramme suivant.



Configurations du serveur TACACS+

Ce document utilise les configurations de serveur indiquées ici.

- Logiciel gratuit TACACS+
- Cisco Secure ACS pour UNIX 2.x.x

Logiciel gratuit TACACS+

```
!--- This user is on the ISP TACACS+ server. !--- The profile includes the Tunnel ID ("isp"), the IP ad

user = hp.com {
service = ppp protocol = vpdn {
tunnel-id = isp
ip-addresses = "10.31.1.50"
nas-password = "hello"
gw-password = "there"
}
}


!--- The next three users are on the HGW server.

user = isp {
chap = cleartext "hello"
service = ppp protocol = ip {
default attribute = permit
}
}

user = hp-gw {
chap = cleartext "there"
service = ppp protocol = ip {
default attribute = permit
}
}
```

```
user = jsmith@hp.com {
chap = cleartext "test"
service = ppp protocol = ip {
default attribute = permit
}
}
```

Cisco Secure ACS pour UNIX 2.x.x

```
!--- This user is on the ISP server.

# ./ViewProfile -p 9900 -u hp.com
User Profile Information
user = hp.com{
profile_id = 83
profile_cycle = 1
service=ppp {
protocol=vpdn {
set tunnel-id=isp
set ip-addresses="10.31.1.50"
set nas-password="hello"
set gw-password="there"
}
protocol=lcp {
}
}

}


!--- The next three users are on the HGW server. !--- The next two usernames are used to authenticate t

# ./ViewProfile -p 9900 -u isp
User Profile Information
user = isp{
profile_id = 84
profile_cycle = 1
password = chap "********"
service=ppp {
protocol=ip {
default attribute=permit
}
protocol=lcp {
}
}

}

# ./ViewProfile -p 9900 -u hp-gw
User Profile Information
user = hp-gw{
profile_id = 82
profile_cycle = 1
password = chap "********"
service=ppp {
```

```
protocol=ip {
default attribute=permit
}
protocol=lcp {
}
}

}

!--- This username is used to authenticate the end user !--- after the tunnel is established.

# ./ViewProfile -p 9900 -u jsmith@hp.com
User Profile Information
user = jsmith@hp.com{
profile_id = 85
profile_cycle = 1
password = chap "********"
service=ppp {
protocol=ip {
default attribute=permit
}
protocol=lcp {
}
}

}
```

Configurations des routeurs

Ce document utilise les configurations indiquées ici.

- Routeur ISP
- Routeur HGW

Configuration du routeur ISP

```
<#root>

koala#

show running config

Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname koala
!
aaa new-model
aaa authentication ppp default tacacs+ none
aaa authorization network tacacs+ none
```

```
aaa accounting network start-stop tacacs+

enable password ww
!

!--- VPDN is enabled.


vpdn enable

!
interface Ethernet0
ip address 10.31.1.5 255.255.255.0
!
interface Serial0
shutdown
!
interface Serial1
shutdown
!
interface Async1
ip unnumbered Ethernet0
encapsulation ppp
async mode dedicated
no cdp enable
ppp authentication chap
!
ip default-gateway 10.31.1.1
no ip classless
ip route 0.0.0.0 0.0.0.0 10.31.1.1
!

!--- Specify the TACACS server information on the NAS.


tacacs-server host 171.68.120.194

tacacs-server key cisco

no tacacs-server directed-request
snmp-server community public RW
snmp-server enable traps config
!
line con 0
password ww
line 1 16
password ww
autoselect ppp
modem InOut
transport input all
stopbits 1
rxspeed 115200
txspeed 115200
flowcontrol hardware
line aux 0
line vty 0 4
exec-timeout 0 0
password ww
!
end
```

```
<#root>

thing_one#

show running config

Building configuration...

Current configuration:
!
version 11.2
no service password-encryption
no service udp-small-servers
no service tcp-small-servers
!
hostname thing_one
!
aaa new-model
aaa authentication ppp default tacacs+ none
aaa authorization network tacacs+ none
enable password ww
!

!--- Enable VPDN.


vpdn enable


!--- Specify the remote host ("isp" on the network access server) !--- and the local name ("hp-gw" on

vpdn incoming isp hp-gw virtual-template 1

!
interface Loopback0
shutdown
!
interface Ethernet0
ip address 10.31.1.50 255.255.255.0
!
interface Virtual-Template1


!--- Create a virtual template interface.


ip unnumbered Ethernet0


!--- Un-number the Virtual interface to an available LAN interface.


peer default ip address pool async


!--- Use the pool "async" to assign the IP address for incoming connections.


ppp authentication chap
```

```
!--- Use CHAP authentication for the incoming connection.

!
interface Serial0
shutdown
!
interface Serial1
shutdown
!
ip local pool async 15.15.15.15
no ip classless
ip route 0.0.0.0 0.0.0.0 10.31.1.1
!
tacacs-server host 171.68.118.101

no tacacs-server directed-request

tacacs-server key cisco


!--- Specify the TACACS+ server information on the NAS.

!
line con 0
exec-timeout 0 0
line 1 8
line aux 0
line vty 0 4
!
end
```

Vérifier

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannage

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

Dépannage des commandes

Remarque : avant d'émettre des commandes debug, consultez Informations importantes sur les commandes de débogage.

- debug aaa authentication : affiche des informations sur l'authentification AAA (authentication, authorization, and accounting)/TACACS+.
- debug aaa authorization : affiche des informations sur l'autorisation AAA/TACACS+.
- debug ppp negotiation : affiche les paquets PPP transmis lors du démarrage de PPP, où les options PPP sont négociées.

- debug tacacs+ : affiche des informations de débogage détaillées associées à TACACS+.
- debug vpdn errors : affiche les erreurs qui empêchent l'établissement d'un tunnel PPP ou celles qui entraînent la fermeture d'un tunnel établi.
- debug vpdn events : affiche des messages sur les événements qui font partie de l'établissement ou de l'arrêt normal du tunnel PPP.
- debug vpdn l2f-errors : affiche les erreurs de protocole de couche 2 qui empêchent l'établissement de la couche 2 ou son fonctionnement normal.
- debug vpdn l2f-events : affiche des messages sur les événements qui font partie de l'établissement ou de l'arrêt normal du tunnel PPP pour la couche 2.
- debug vpdn l2f-packets : affiche des messages sur les en-têtes et l'état du protocole de transfert de couche 2.
- debug vpdn packets : affiche les erreurs et les événements L2TP (Layer 2 Tunnel Protocol) qui font partie de l'établissement ou de l'arrêt normal du tunnel pour les VPDN.
- debug vtemplate : affiche les informations de clonage d'une interface d'accès virtuelle, du moment où elle est clonée à partir d'un modèle virtuel jusqu'au moment où l'interface d'accès virtuelle s'arrête lorsque l'appel se termine.

Exemple de sortie de débogage

Ces débogages sont fournis à titre de référence.

- Débogage correct du routeur ISP
- Débogage correct du routeur HGW
- Débogages pour échec de connexion sur le routeur ISP
- Débogages pour les échecs de connexion sur le routeur HGW

Débogage correct du routeur ISP

<#root>

```
koala#
```

show debug

```
General OS:
AAA Authentication debugging is on
AAA Authorization debugging is on
AAA Accounting debugging is on
VPN:
VPN events debugging is on
VPN errors debugging is on
koala#
```

```
%LINK-3-UPDOWN: Interface Async1, changed state to up
15:04:47: VPDN: Looking for tunnel -- hp.com --
15:04:47: AAA/AUTHEN: create_user (0x15FA80) user='hp.com' ruser=''
   port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0
15:04:47: AAA/AUTHOR/VPDN: : (2445181346): user='hp.com'
15:04:47: AAA/AUTHOR/VPDN: : (2445181346): send AV service=ppp
15:04:47: AAA/AUTHOR/VPDN: : (2445181346): send AV protocol=vpdn
15:04:47: AAA/AUTHOR/VPDN: : (2445181346): Method=TACACS+
15:04:47: AAA/AUTHOR/TAC+: (2445181346): user=hp.com
15:04:47: AAA/AUTHOR/TAC+: (2445181346): send AV service=ppp
15:04:47: AAA/AUTHOR/TAC+: (2445181346): send AV protocol=vpdn
15:04:47: TAC+: (2445181346): received author response status = PASS_ADD

15:04:47: AAA/AUTHOR (2445181346): Post authorization status = PASS_ADD
15:04:47: AAA/AUTHOR/VPDN: Processing AV service=ppp

15:04:47: AAA/AUTHOR/VPDN: Processing AV protocol=vpdn
15:04:47: AAA/AUTHOR/VPDN: Processing AV tunnel-id=isp
15:04:47: AAA/AUTHOR/VPDN: Processing AV ip-addresses=10.31.1.50
15:04:47: AAA/AUTHOR/VPDN: Processing AV nas-password=hello
15:04:47: AAA/AUTHOR/VPDN: Processing AV gw-password=there

15:04:47: VPDN: Get tunnel info with NAS isp GW hp.com, IP 10.31.1.50


!--- The TACACS+ server returns the attributes the !--- NAS should use for the tunnel. !--- The tunnel-

15:04:47: AAA/AUTHEN: free_user (0x15FA80) user='hp.com' ruser=''
   port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0
15:04:47: VPDN: Forward to address 10.31.1.50
15:04:47: As1 VPDN: Forwarding...
15:04:47: AAA/AUTHEN: create_user (0x118008) user='jsmith@hp.com' ruser=''
   port='Async1' rem_addr='async' authen_type=CHAP service=PPP priv=1
15:04:47: As1 VPDN: Bind interface direction=1

15:04:47: As1 VPDN: jsmith@hp.com is forwarded

%LINEPROTO-5-UPDOWN: Line protocol on Interface Async1, changed state to up
15:04:49: AAA/ACCT: NET acct start. User jsmith@hp.com, Port Async1: Async1

!--- User finishes and disconnects.

%LINEPROTO-5-UPDOWN: Line protocol on Interface Async1,
   changed state to down
%LINK-5-CHANGED: Interface Async1, changed state to reset
15:05:27: As1 VPDN: Cleanup
15:05:27: As1 VPDN: Reset
15:05:27: As1 VPDN: Reset
15:05:27: As1 VPDN: Unbind interface
15:05:27: AAA/ACCT: Network acct stop. User jsmith@hp.com, Port Async1:
task_id=2 timezone=UTC service=vpdn bytes_in=1399 bytes_out=150 paks_in=27
   paks_out=9 elapsed_time=38
%LINK-3-UPDOWN: Interface Async1, changed state to down
15:05:30: AAA/AUTHEN: free_user (0x118008) user='jsmith@hp.com' ruser=''
   port='Async1' rem_addr='async' authen_type=CHAP service=PPP priv=1
koala#
```

Débogage correct du routeur HGW

<#root>

thing_one#

show debug

General OS:
AAA Authentication debugging is on
AAA Authorization debugging is on
AAA Accounting debugging is on
VPN:
VPN events debugging is on
VPN errors debugging is on
VTEMPLATE:
Virtual Template debugging is on
thing_one#

15:04:46: AAA/AUTHEN: create_user (0x15E6E0) user='isp' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
15:04:46: TAC+: ver=192 id=969200103 received AUTHEN status = PASS
15:04:46: AAA/AUTHEN: free_user (0x15E6E0) user='isp' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
15:04:46: AAA/AUTHEN (3252085483): status = PASS
15:04:46: AAA/AUTHEN: free_user (0x15CBEC) user='isp' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
15:04:46: AAA/AUTHEN: create_user (0x15F1B8) user='isp' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
15:04:46: AAA/AUTHEN/START (3897539709): port='' list='default'
   action=LOGIN service=PPP
15:04:46: AAA/AUTHEN/START (3897539709): found list default
15:04:46: AAA/AUTHEN/START (3897539709): Method=TACACS+
15:04:46: TAC+: send AUTHEN/START packet ver=193 id=3897539709
15:04:46: TAC+: ver=192 id=3897539709 received AUTHEN status = GETPASS
15:04:46: AAA/AUTHEN: create_user (0x15E6F0) user='isp' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
15:04:46: TAC+: ver=192 id=2306139011 received AUTHEN status = PASS
15:04:46: AAA/AUTHEN: free_user (0x15E6F0) user='isp' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
15:04:46: AAA/AUTHEN (3897539709): status = PASS

15:04:46: VPDN: Chap authentication succeeded for isp

!--- The LAC ("ISP") is succesfully authenticated.

15:04:46: AAA/AUTHEN: free_user (0x15F1B8) user='isp' ruser='' port=''
rem_addr='' authen_type=CHAP service=PPP priv=1
15:04:46: Vi1 VTEMPLATE: Reuse Vi1, recycle queue size 0
15:04:46: Vi1 VTEMPLATE: Set default settings with no ip address
15:04:47: Vi1 VTEMPLATE: Hardware address 00e0.1e68.942c
15:04:47: Vi1 VPDN: Virtual interface created for jsmith@hp.com
15:04:47: Vi1 VPDN: Set to Async interface
15:04:47: Vi1 VPDN: Clone from Vtemplate 1 filterPPP=0 blocking
15:04:47: Vi1 VTEMPLATE: Has a new cloneblk vtemplate, now it has vtemplate
15:04:47: Vi1 VTEMPLATE: Undo default settings
15:04:47: Vi1 VTEMPLATE: ********** CLONE VACCESS1 **********
15:04:47: Vi1 VTEMPLATE: Clone from vtemplate1
interface Virtual-Access1
no ip address
encap ppp
ip unnum eth 0
peer default ip address pool async
ppp authen chap
end

```
%LINK-3-UPDOWN: Interface Virtual-Access1, changed state to up
15:04:48: Vi1 VPDN: Bind interface direction=2
15:04:48: Vi1 VPDN: PPP LCP accepted sent & rcv CONFACK
15:04:48: Vi1 VPDN: Virtual interface iteration
15:04:48: AAA/AUTHEN: create_user (0x161688) user='jsmith@hp.com' ruser=''
   port='Virtual-Access1' rem_addr='async' authen_type=CHAP service=PPP priv=1
15:04:48: AAA/AUTHEN/START (580760432): port='Virtual-Access1' list=''
   action=LOGIN service=PPP
15:04:48: AAA/AUTHEN/START (580760432): using "default" list
15:04:48: AAA/AUTHEN/START (580760432): Method=TACACS+
15:04:48: TAC+: send AUTHEN/START packet ver=193 id=580760432
15:04:48: Vi1 VPDN: Virtual interface iteration
15:04:49: TAC+: ver=192 id=580760432 received AUTHEN status = GETPASS

!--- Authenticate user jsmith@hp.com with the TACACS+ server.


15:04:49: AAA/AUTHEN: create_user (0x1667C0) user='jsmith@hp.com' ruser=''
 port='Virtual-Access1' rem_addr='async' authen_type=CHAP service=PPP priv=1
15:04:49: TAC+: ver=192 id=2894253624 received AUTHEN status = PASS

15:04:49: AAA/AUTHEN: free_user (0x1667C0) user='jsmith@hp.com' ruser=''
 port='Virtual-Access1' rem_addr='async' authen_type=CHAP service=PPP priv=1
15:04:49: AAA/AUTHEN (580760432): status = PASS
15:04:49: AAA/AUTHOR/LCP Vi1: Authorize LCP
15:04:49: AAA/AUTHOR/LCP: Virtual-Access1: (687698354): user='jsmith@hp.com'
15:04:49: AAA/AUTHOR/LCP: Virtual-Access1: (687698354): send AV service=ppp
15:04:49: AAA/AUTHOR/LCP: Virtual-Access1: (687698354): send AV protocol=lcp
15:04:49: AAA/AUTHOR/LCP: Virtual-Access1: (687698354): Method=TACACS+
15:04:49: AAA/AUTHOR/TAC+: (687698354): user=jsmith@hp.com
15:04:49: AAA/AUTHOR/TAC+: (687698354): send AV service=ppp
15:04:49: AAA/AUTHOR/TAC+: (687698354): send AV protocol=lcp
15:04:49: TAC+: (687698354): received author response status = PASS_ADD
15:04:49: AAA/AUTHOR (687698354): Post authorization status = PASS_ADD
15:04:49: AAA/ACCT: NET acct start. User jsmith@hp.com, Port Virtual-Access1:
 Virtual-Access1
15:04:49: AAA/AUTHOR/FSM Vi1: (0): Can we start IPCP?
15:04:49: AAA/AUTHOR/FSM: Virtual-Access1: (3562892028): user='jsmith@hp.com'
15:04:49: AAA/AUTHOR/FSM: Virtual-Access1: (3562892028): send AV service=ppp
15:04:49: AAA/AUTHOR/FSM: Virtual-Access1: (3562892028): send AV protocol=ip
15:04:49: AAA/AUTHOR/FSM: Virtual-Access1: (3562892028): Method=TACACS+
15:04:49: AAA/AUTHOR/TAC+: (3562892028): user=jsmith@hp.com
15:04:49: AAA/AUTHOR/TAC+: (3562892028): send AV service=ppp
15:04:49: AAA/AUTHOR/TAC+: (3562892028): send AV protocol=ip
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
   changed state to up
15:04:49: TAC+: (3562892028): received author response status = PASS_ADD
15:04:49: AAA/AUTHOR (3562892028): Post authorization status = PASS_ADD

!--- IPCP negotiation begins.

15:04:49: AAA/AUTHOR/FSM Vi1: We can start IPCP
15:04:50: AAA/AUTHOR/IPCP Vi1: Start. Her address 0.0.0.0, we want 0.0.0.0
15:04:50: AAA/AUTHOR/IPCP Vi1: Processing AV service=ppp
15:04:50: AAA/AUTHOR/IPCP Vi1: Processing AV protocol=ip
15:04:50: AAA/AUTHOR/IPCP Vi1: Authorization succeeded
15:04:50: AAA/AUTHOR/IPCP Vi1: Done. Her address 0.0.0.0, we want 0.0.0.0
15:04:51: AAA/AUTHOR/IPCP Vi1: Start. Her address 0.0.0.0,
   we want 15.15.15.15
15:04:51: AAA/AUTHOR/IPCP Vi1: Processing AV service=ppp
15:04:51: AAA/AUTHOR/IPCP Vi1: Processing AV protocol=ip
15:04:51: AAA/AUTHOR/IPCP Vi1: Authorization succeeded
```

```
15:04:51: AAA/AUTHOR/IPCP Vi1: Done. Her address 0.0.0.0,
   we want 15.15.15.15
15:04:51: AAA/AUTHOR/IPCP Vi1: Start. Her address 15.15.15.15,
   we want 15.15.15.15
15:04:51: AAA/AUTHOR/IPCP: Virtual-Access1: (3193852847):
   user='jsmith@hp.com'
15:04:51: AAA/AUTHOR/IPCP: Virtual-Access1: (3193852847):
   send AV service=ppp
15:04:51: AAA/AUTHOR/IPCP: Virtual-Access1: (3193852847):
   send AV protocol=ip
15:04:51: AAA/AUTHOR/IPCP: Virtual-Access1: (3193852847):
   send AV addr*15.15.15.15
15:04:51: AAA/AUTHOR/IPCP: Virtual-Access1: (3193852847):
   Method=TACACS+
15:04:51: AAA/AUTHOR/TAC+: (3193852847): user=jsmith@hp.com
15:04:51: AAA/AUTHOR/TAC+: (3193852847): send AV service=ppp
15:04:51: AAA/AUTHOR/TAC+: (3193852847): send AV protocol=ip
15:04:51: AAA/AUTHOR/TAC+: (3193852847): send AV addr*15.15.15.15
15:04:51: TAC+: (3193852847): received author response status = PASS_ADD
15:04:51: AAA/AUTHOR (3193852847): Post authorization status = PASS_ADD
15:04:51: AAA/AUTHOR/IPCP Vi1: Processing AV service=ppp
15:04:51: AAA/AUTHOR/IPCP Vi1: Processing AV protocol=ip
15:04:51: AAA/AUTHOR/IPCP Vi1: Processing AV addr*15.15.15.15
15:04:51: AAA/AUTHOR/IPCP Vi1: Authorization succeeded
15:04:51: AAA/AUTHOR/IPCP Vi1: Done. Her address 15.15.15.15,
   we want 15.15.15.15

!--- User finishes and disconnects.

15:05:24: Vi1 VPDN: Reset
15:05:24: Vi1 VPDN: Reset
%LINK-3-UPDOWN: Interface Virtual-Access1, changed state to down
15:05:24: Vi1 VPDN: Cleanup
15:05:24: Vi1 VPDN: Reset
15:05:24: Vi1 VPDN: Reset
15:05:24: Vi1 VPDN: Unbind interface
15:05:24: Vi1 VTEMPLATE: Free vaccess
15:05:24: Vi1 VPDN: Reset
15:05:24: Vi1 VPDN: Reset
15:05:24: AAA/ACCT: Network acct stop. User jsmith@hp.com,
   Port Virtual-Access1:
task_id=2 timezone=UTC service=ppp protocol=ip addr=15.15.15.15
   bytes_in=564
bytes_out=142 paks_in=15 paks_out=8 elapsed_time=35
15:05:24: AAA/AUTHEN: free_user (0x161688) user='jsmith@hp.com' ruser=''
   port='Virtual-Access1' rem_addr='async'
   authen_type=CHAP service=PPP priv=1
%LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1,
 changed state to down
15:05:25: VTEMPLATE: Clean up dirty vaccess queue, size 1
15:05:25: Vi1 VTEMPLATE: Found a dirty vaccess clone with vtemplate
15:05:25: Vi1 VTEMPLATE: ************ UNCLONE VACCESS1 **************
15:05:25: Vi1 VTEMPLATE: Unclone to-be-freed command#5
interface Virtual-Access1
default ppp authen chap
default peer default ip address pool async
default ip unnum eth 0
default encap ppp
default ip address
end

15:05:26: Vi1 VTEMPLATE: Set default settings with no ip address
```

```
15:05:26: Vi1 VTEMPLATE: Remove cloneblk vtemplate with vtemplate
15:05:26: Vi1 VTEMPLATE: Add vaccess to recycle queue, queue size=1
thing_one#
```

Débogages pour échec de connexion sur le routeur ISP

<#root>

```
koala#
```

show debug

```
General OS:
AAA Authentication debugging is on
AAA Authorization debugging is on
AAA Accounting debugging is on
VPN:
VPN events debugging is on
VPN errors debugging is on
koala#
```

!---

Problem 1:

```
 !--- The ISP TACACS+ server is down. !--- There is no output on the HGW router !--- because the call ha
```

```
AAA/AUTHOR (3015476150): Post authorization status = ERROR
AAA/AUTHOR/VPDN: : (3015476150): Method=NOT_SET
AAA/AUTHOR/VPDN: : (3015476150): no methods left to try
AAA/AUTHOR (3015476150): Post authorization status = ERROR
VPDN: (hp.com) Authorization failed, could not talk to AAA server or
 local tunnel problem
```

!---

Problem 2:

```
 !--- Userid hp.com is not in the ISP server. !--- There is no output on the Gateway router !--- becaus
```

```
TAC+: (894828802): received author response status = PASS_ADD
AAA/AUTHOR (894828802): Post authorization status = PASS_ADD
VPDN: (hp.com) Authorization failed, had talked to AAA server;
   but both Tunnel ID and IP address are missing
AAA/AUTHEN: free_user (0x16A6E4) user='hp.com' ruser=''
   port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0
AAA/AUTHEN: create_user (0x16CA8C) user='jsmith@hp.com' ruser=''
   port='Async1' rem_addr='async' authen_type=CHAP service=PPP priv=1
AAA/AUTHEN/START (1904487288): port='Async1' list=''
   action=LOGIN service=PPP
AAA/AUTHEN/START (1904487288): using "default" list
AAA/AUTHEN (1904487288): status = UNKNOWN
AAA/AUTHEN/START (1904487288): Method=TACACS+
TAC+: send AUTHEN/START packet ver=193 id=1904487288
TAC+: ver=193 id=1904487288 received AUTHEN status = FAIL
AAA/AUTHEN (1904487288): status = FAIL
```

Débogages pour les échecs de connexion sur le routeur HGW

<#root>

```
thing_one#

show debug

General OS:
AAA Authentication debugging is on
AAA Authorization debugging is on
AAA Accounting debugging is on
VPN:
VPN events debugging is on
VPN errors debugging is on
VTEMPLATE:
Virtual Template debugging is on
thing_one#

!---

Problem 1:

 !--- The problem is in the tunnel definition on HGW router. !--- In the HGW configuration,

vpdn incoming hp-gw isp virtual-template 1

 !--- is inserted instead of

vpdn incoming isp hp-gw virtual-template 1

 !--- The

debug vpdn l2f-errors

 command displays.


L2F: Couldn't find tunnel named isp
L2F: Couldn't find tunnel named isp


!---

Problem 2:

 !--- This message appears when User hp-gw is not in the HGW server.


TAC+: ver=192 id=1920941753 received AUTHEN status = FAIL
AAA/AUTHEN: free_user (0x138C34) user='hp-gw' ruser=''
   port='' rem_addr='' authen_type=CHAP service=PPP priv=1
AAA/AUTHEN (3006335673): status = FAIL
VPDN: authentication failed, couldn't find user information for hp-gw


!---

Problem 3:

 !--- This appears when user isp is not in the HGW server.


TAC+: ver=192 id=1917558147 received AUTHEN status = FAIL
AAA/AUTHEN: free_user (0x15F20C) user='isp' ruser=''
```

```
   port='' rem_addr='' authen_type=CHAP service=PPP priv=1
AAA/AUTHEN (1949507921): status = FAIL
VPDN: authentication failed, couldn't find user information for isp


!---
```

Problem 4:

```
 !--- This message appears when User jsmith@hp.com is !--- not in the HGW server:


TAC+: ver=192 id=755036341 received AUTHEN status = FAIL
AAA/AUTHEN: free_user (0x15F89C) user='jsmith@hp.com' ruser=''
   port='Virtual-Access1' rem_addr='async' authen_type=CHAP service=PPP priv=1
AAA/AUTHEN (2606986667): status = FAIL
```

Informations connexes

- Page d'assistance Cisco Secure ACS pour UNIX
- Page d'assistance TACACS+
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.