Configuration de l'authentification TACACS+ pour les réseaux VPDN

Contenu

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]). Quand un client de Protocole point à point (PPP) introduit dans un LAC, le LAC détermine qu'il devrait expédier cette session PPP en fonction à un serveur de réseau L2TP (LNS) pour ce client, qui alors authentifie l'utilisateur et commence la négociation PPP. Une fois que l'installation de PPP s'est terminée, toutes les trames sont envoyées par le LAC au client et au LNS.

Cette configuration d'échantillon te permet pour utiliser l'authentification TACACS+ avec des réseaux commutés de connexion privée virtuelle (VPDNs). Le LAC questionne le serveur TACACS+, détermine quel LNS pour expédier l'utilisateur, et établit le tunnel approprié.

Pour plus d'informations sur VPDNs, référez-vous compréhension derrière VPDN.

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 :

- Cisco Secure ACS pour la version 2.x.x et ultérieures d'UNIX ou le logiciel gratuit TACACS+
- Version de logiciel 11.2 et ultérieures de Cisco IOS®

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 de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Cette section présente les informations requises pour configurer les caractéristiques décrites dans ce document.

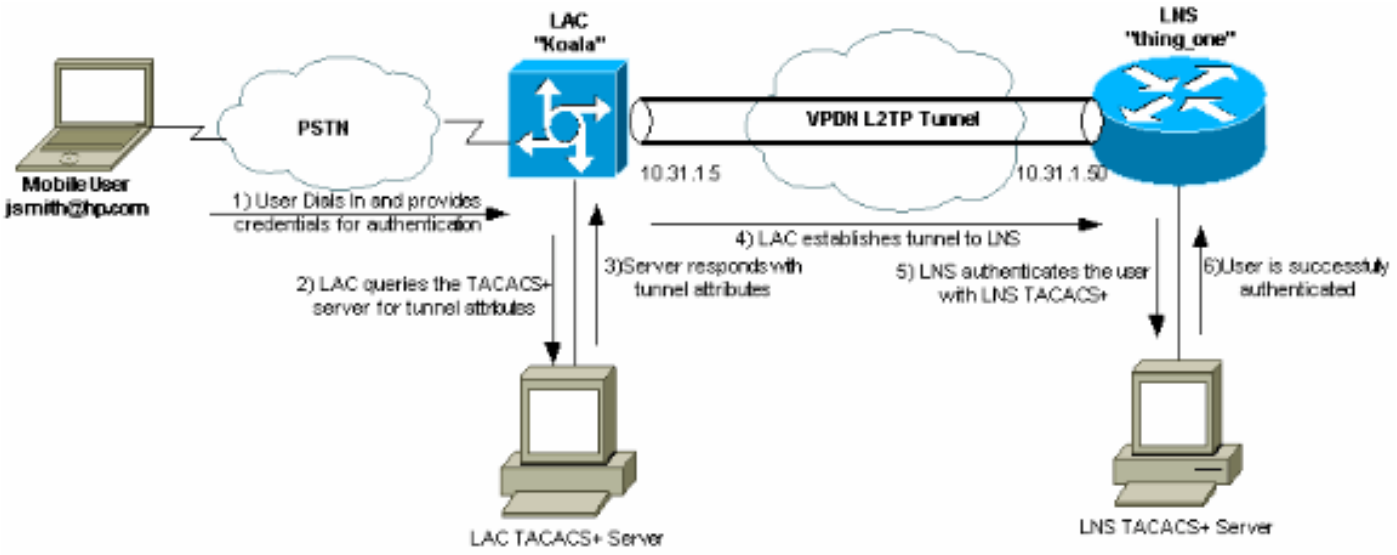
Dans cet exemple, l'utilisateur est « jsmith@hp.com » avec le mot de passe « test ». Quand « jsmith@hp.com » introduit dans le routeur de l'ISP, le routeur de l'ISP envoie l'ID utilisateur « hp.com » au serveur ISP TACACS+. Le serveur ISP trouve l'ID utilisateur « hp.com » et envoie son tunnel-id (« fournisseur d'accès internet »), l'adresse IP du routeur de la passerelle domestique (HGW) (10.31.1.50), le mot de passe de serveur d'accès à distance (NAS) (« bonjour »), et le mot de passe de la passerelle (« là ») de nouveau au routeur de l'ISP.

Le routeur de l'ISP initie un tunnel et se connecte au routeur HGW, qui en avant les mots de passe pour l'ID utilisateur « HP-gw » (« là ») et puis l'ID utilisateur « fournisseur d'accès internet » (« bonjour ») au serveur HGW TACACS+. Une fois que les tunnels est établis, le routeur de l'ISP en avant au routeur HGW l'ID utilisateur ("jsmith@hp.com ") et mot de passe (« test ») de l'utilisateur qui se connecte. Cet utilisateur est authentifié sur le serveur HGW. Dans les configurations d'échantillon dans ce document, le nom d'hôte de routeur de l'ISP est « koala » et le nom de hôte du routeur HGW est « thing_one ».

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.



Configurations du serveur TACACS+

Ce document utilise les configurations du serveur affichées 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 address !--- of the Peer (10.31.1.50), !--- and the passwords used to authenticate the
tunnel. !--- The ISP uses these attibutes to establish the tunnel. 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 the LAC !--- during tunnel initialization. # ./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 de routeur

Ce document utilise les configurations indiquées ici.

- Routeur de l'ISP
- Routeur HGW

Configuration de routeur de l'ISP

```
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
```

Configuration de routeur HGW

```
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 the home gateway) to use
to authenticate. !--- Also specify the virtual template
to use. !--- The local name and the remote host name
must match !--- the ones in the TACACS server. 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
```

Vérifiez

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

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 de l'Authentification, autorisation et comptabilité (AAA) /TACACS+.
- **autorisation de debug aaa** — Affiche des informations sur l'autorisation AAA/TACACS+.
- **debug ppp negotiation** — Paquets PPP d'affichages transmis pendant le startup de PPP, où des options PPP sont négociées.
- **mettez au point tacacs+** — Affiche les informations de débogage détaillées associées avec TACACS+.
- **erreurs de debug vpdn** — Affiche les erreurs qui empêchent un tunnel de PPP d'être établi ou les erreurs qui font fermer un tunnel établi.
- **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 l2f-errors** — Les affichages posent 2 erreurs de protocole qui empêchent l'établissement de la couche 2 ou empêchent son fonctionnement normal.
- **debug vpdn l2f-events** — Affiche des messages au sujet des événements qui font partie d'établissement normal de tunnel de PPP ou arrêt pour la couche 2.
- **debug vpdn l2f-packets** — Messages d'affichages au sujet des en-têtes et d'état de protocole de transfert de couche 2.
- **paquets de debug vpdn** — Les affichages posent 2 erreurs et événements de protocol (L2TP) de tunnel qui sont une partie de l'établissement normal d'un tunnel ou un arrêt pour VPDNs.
- **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.

Exemple de sortie de débogage

Ceux-ci met au point sont donnés pour la référence.

- Bon debug de routeur de l'ISP
- Debug de routeur HGW bon
- Debugs pour la connexion défectueuse sur le routeur de l'ISP
- Debugs pour des connexions Failed sur le routeur HGW

Bon debug de routeur de l'ISP

```
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-id is "ISP" and the IP address of HGW is 10.31.1.50.* 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#

Debug de routeur HGW bon

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#

Debugs pour la connexion défectueuse sur le routeur de l'ISP

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 has not gone that far.* **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 !--- because the call has not gone that far.* **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**

Debugs pour des connexions Failed sur le routeur HGW

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

- Cisco Secure ACS pour la page de support UNIX
- Page d'assistance TACACS+
- Support et documentation techniques - Cisco Systems