تكوين مصادقة TACACS+ لشبكات VPDN

المحتويات

المقدمة
المتطلبات الأساسية
المتطلبات
المكونات المستخدمة
الاصطلاحات
التكوين
الرسم التخطيطي للشبكة
تكوينات خادم TACACS+
تكوينات الموجه
التحقق من الصحة
استكشاف الأخطاء وإصلاحها
أوامر استكشاف الأخطاء وإصلاحها
إخراج تصحيح الأخطاء للعينة
معلومات ذات صلة

المقدمة

تسمح شبكة الطلب الهاتفي الخاصة الظاهرية (VPDN) لأي طلب شبكة خاصة في الخدمة بالمرور عبر خوادم الوصول عن بعد (المحددة باسم مركز الوصول إلى L2TP [LAC]). عندما يتصل عميل بروتوكول الاتصال من نقطة إلى نقطة (PPP) بوحدة التحكم في الوصول (LAC)، تحدد وحدة التحكم في الوصول أنه يجب إعادة توجيه جلسة عمل بروتوكول الاتصال من نقطة إلى نقطة (LNS) لذلك العميل، والذي يقوم بعد ذلك بمصادقة المستخدم وبدء التفاوض على بروتوكول الاتصال من نقطة إلى نقطة (PPP). بمجرد اكتمال إعداد بروتوكول الاتصال من نقطة إلى نقطة (PPP)، يتم إرسال جميع الإطارات من خلال وحدة التحكم في الوصول (LAC) إلى العميل و LNS.

يتيح لك نموذج التكوين هذا إستخدام مصادقة TACACS+ مع شبكات الطلب الهاتفي الخاصة الظاهرية (VPDNs). تستعلم LAC عن خادم TACACS+، وتحدد LNS لإعادة توجيه المستخدم، وتنشئ النفق المناسب.

أحلت ل كثير معلومة على VPDNs، يفهم VPDN.

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- مصدر المحتوى الإضافي الآمن من Cisco ل UNIX الإصدار x.x.2 والإصدارات الأحدث أو البرامج المجانية ل TACACS+
- برنامج Cisco IOS® الإصدار 11.2 والإصدارات الأحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

الاصطلاحات

للحصول على مزيد من المعلومات حول اصطلاحات المستندات، ارجع إلى اصطلاحات تلميحات Cisco التقنية.

التكوين

يعرض هذا القسم المعلومات اللازمة لتكوين الميزات الموضحة في هذا المستند.

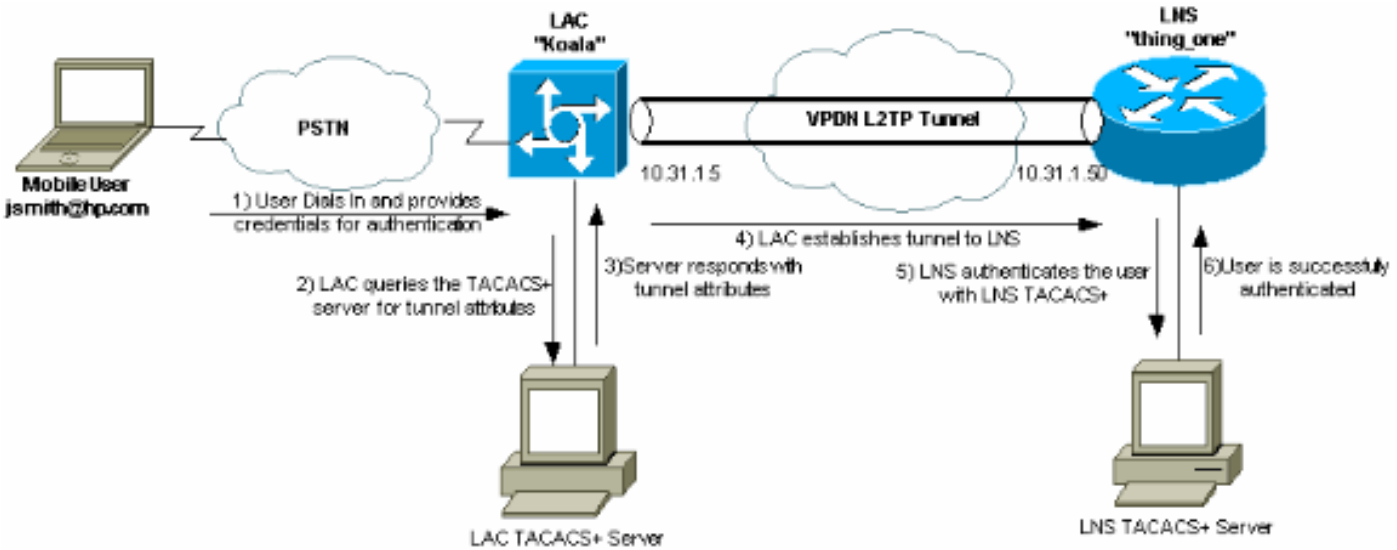
في هذا المثال، المستخدم هو "jsmith@hp.com" بكلمة مرور "test". عندما يدخل "jsmith@hp.com" إلى موجه ISP، يرسل موجه ISP معرف المستخدم "hp.com" إلى خادم ISP TACACS+. يعثر خادم ISP على معرف المستخدم "hp.com" ويرسل معرف النفق الخاص به ("isp")، وعنوان IP الخاص بموجه العبارة الرئيسية ((HGW 10.31.1.50))، وكلمة مرور خادم الوصول إلى الشبكة ("hello") (NAS")، وكلمة مرور العبارة ("هناك") مرة أخرى إلى موجه ISP.

يقوم موجه ISP بتهيئة نفق والاتصال بموجه HGW، والذي يقوم بإعادة توجيه كلمات مرور معرف المستخدم "hp-gw" ("هناك") ثم معرف المستخدم "hello" ("isp") إلى خادم HGW TACACS+. بمجرد إنشاء الأنفاق، يقوم موجه ISP بإعادة التوجيه إلى موجه HGW معرف المستخدم ("jsmith@hp.com") وكلمة المرور ("test") الخاصة بالمستخدم الذي يتم إدخاله. تمت مصادقة هذا المستخدم على خادم HGW. في نموذج التكوينات الواردة في هذا المستند، يكون اسم مضيف موجه ISP هو "koala" واسم مضيف موجه HGW هو "thing_one".

ملاحظة: للعثور على معلومات إضافية حول الأوامر المستخدمة في هذا المستند، أستخدم أداة بحث الأوامر (للعملاء المسجلين فقط).

الرسم التخطيطي للشبكة

يستخدم هذا المستند إعداد الشبكة الموضح في هذا الرسم التخطيطي.



تكوينات خادم TACACS+

يستخدم هذا المستند تكوينات الخادم الموضحة هنا.

- TACACS+ البرمجيات المجانية
- UNIX 2.x.x ل Cisco Secure ACS

TACACS+ البرمجيات المجانية

```
   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
                                                                                        { {
```

UNIX 2.x.x ل Cisco Secure ACS

```
 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
```

تكوينات الموجه

يستخدم هذا المستند التكوينات الموضحة هنا.

- موجه ISP
- الموجه HGW

تكوين موجه 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
```

تکوین موجه 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
```

التحقق من الصحة

لا يوجد حاليًا إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

أوامر استكشاف الأخطاء وإصلاحها

ملاحظة: قبل إصدار أوامر **تصحيح الأخطاء**، يرجى الاطلاع على المعلومات المهمة في أوامر تصحيح الأخطاء.

- **تصحيح الأخطاء لمصادقة AAA**— يعرض معلومات حول المصادقة والتخويل والمحاسبة (AAA)/مصادقة TACACS+.
- **تصحيح أخطاء تفويض المصادقة والتفويض والمحاسبة (AAA)**—يعرض معلومات حول تفويض

AAA/TACACS+.

- **debug ppp negotiation**—يعرض حزم PPP المرسلة أثناء بدء تشغيل PPP، حيث يتم التفاوض حول خيارات PPP.
- **debug tacacs+**—يعرض معلومات تصحيح الأخطاء التفصيلية المرتبطة ب TACACS+.
- **debug vpdn** -يعرض أخطاء تمنع إنشاء نفق PPP أو أخطاء تتسبب في إغلاق نفق تم إنشاؤه.
- **debug vpdn events**— يعرض رسائل حول الأحداث التي تعد جزءا من إنشاء نفق PPP العادي أو إيقاف تشغيله.
- **debug vpdn l2f-errors**—يعرض أخطاء بروتوكول الطبقة 2 التي تمنع إنشاء الطبقة 2 أو تمنع تشغيلها الطبيعي.
- **debug vpdn l2f-events**—يعرض رسائل حول الأحداث التي هي جزء من إنشاء نفق PPP العادي أو إيقاف تشغيله للطبقة 2.
- **debug vpdn l2f-packet**—يعرض رسائل حول رؤوس بروتوكول إعادة توجيه الطبقة 2 وحالته.
- **debug vpdn packet**— يعرض أخطاء بروتوكول نفق الطبقة 2 (L2TP) والأحداث التي تعد جزءا من إنشاء النفق العادي أو إيقاف تشغيله لشبكات VPDN.
- **debug vtemplate**— يعرض معلومات النسخ لواجهة الوصول الظاهري من الوقت الذي يتم إستنساخها فيه من قالب ظاهري إلى الوقت الذي يتم فيه إيقاف واجهة الوصول الظاهري عند انتهاء المكالمة.

إخراج تصحيح الأخطاء للعينة

يتم توفير عمليات تصحيح الأخطاء هذه للرجوع إليها.

- تصحيح أخطاء موجه ISP الجيد
- تصحيح أخطاء موجه HGW الجيد
- تصحيح أخطاء الاتصال الفاشل على موجه ISP
- تصحيح أخطاء الاتصالات الفاشلة على موجه HGW

تصحيح أخطاء موجه ISP الجيد

```
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%
-- VPDN: Looking for tunnel -- hp.com :15:04:47
''=AAA/AUTHEN: create_user (0x15FA80) user='hp.com' ruser :15:04:47
port='Async1' rem_addr='' authen_type=NONE service=LOGIN priv=0
'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 :15:04:47
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% AAA/ACCT: NET acct start. User jsmith@hp.com, Port Async1: Async1 :15:04:49
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

تصحيح أخطاء موجه HGW الجيد

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

''=AAA/AUTHEN: create_user (0x15E6E0) user='isp' ruser='' port :15:04:46
rem_addr='' authen_type=CHAP service=PPP priv=1
TAC+: ver=192 id=969200103 received AUTHEN status = PASS :15:04:46
''=AAA/AUTHEN: free_user (0x15E6E0) user='isp' ruser='' port :15:04:46
rem_addr='' authen_type=CHAP service=PPP priv=1
AAA/AUTHEN (3252085483): status = PASS :15:04:46
''=AAA/AUTHEN: free_user (0x15CBEC) user='isp' ruser='' port :15:04:46
rem_addr='' authen_type=CHAP service=PPP priv=1
''=AAA/AUTHEN: create_user (0x15F1B8) user='isp' ruser='' port :15:04:46
rem_addr='' authen_type=CHAP service=PPP priv=1
'AAA/AUTHEN/START (3897539709): port='' list='default :15:04:46
action=LOGIN service=PPP
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 :15:04:46
rem_addr='' authen_type=CHAP service=PPP priv=1
TAC+: ver=192 id=2306139011 received AUTHEN status = PASS :15:04:46
''=AAA/AUTHEN: free_user (0x15E6F0) user='isp' ruser='' port :15:04:46
rem_addr='' authen_type=CHAP service=PPP priv=1
AAA/AUTHEN (3897539709): status = PASS :15:04:46
VPDN: Chap authentication succeeded for isp :15:04:46
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 TAC+: ver=192 id=2894253624 received AUTHEN status = PASS :15:04:49** ''=AAA/AUTHEN: free_user (0x1667C0) user='jsmith@hp.com' ruser :15:04:49 port='Virtual-Access1' rem_addr='async' authen_type=CHAP service=PPP priv=1 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 :15:04:49 Virtual-Access1 ?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 :15:04:49 ,LINEPROTO-5-UPDOWN: Line protocol on Interface Virtual-Access1% changed state to up TAC+: (3562892028): received author response status = PASS_ADD :15:04:49 AAA/AUTHOR (3562892028): Post authorization status = PASS_ADD :15:04:49 *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
```

تصحيح أخطاء الاتصال الفاشل على موجه 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
```

تصحيح أخطاء الاتصالات الفاشلة على موجه 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**. **Problem 2:** !--- 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
```

معلومات ذات صلة

- مصدر المحتوى الإضافي الآمن من Cisco لصفحة دعم UNIX
- صفحة دعم TACACS+
- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).