Konfigurieren der TACACS+-Authentifizierung für VPDNs

Inhalt

Einführung

Ein Virtual Private Dial-up-Netzwerk (VPDN) ermöglicht es einem privaten Netzwerk, eine Einwahl in den Dienst über Remote-Zugriffsserver (definiert als L2TP Access Concentrator [LAC]) zu führen. Wenn sich ein PPP-Client (Point-to-Point Protocol) in eine LAC einwählt, legt die LAC fest, dass diese PPP-Sitzung an einen L2TP-Netzwerkserver (LNS) für diesen Client weitergeleitet werden soll, der dann den Benutzer authentifiziert und die PPP-Aushandlung startet. Nach Abschluss der PPP-Einrichtung werden alle Frames über die LAC an den Client und das LNS gesendet.

Mit dieser Beispielkonfiguration können Sie die TACACS+-Authentifizierung mit Virtual Private Dial-Up Networks (VPDNs) verwenden. Die LAC fragt den TACACS+-Server ab, bestimmt, welches LNS den Benutzer weiterleiten soll, und erstellt den entsprechenden Tunnel.

Weitere Informationen zu VPDNs finden Sie unter VPDN-Verständnis.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Secure ACS für UNIX Version 2.x.x und höher oder für TACACS+-Freeware
- Cisco IOS® Softwareversion 11.2 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions.

Konfigurieren

In diesem Abschnitt werden die Informationen beschrieben, die zum Konfigurieren der in diesem Dokument beschriebenen Funktionen erforderlich sind.

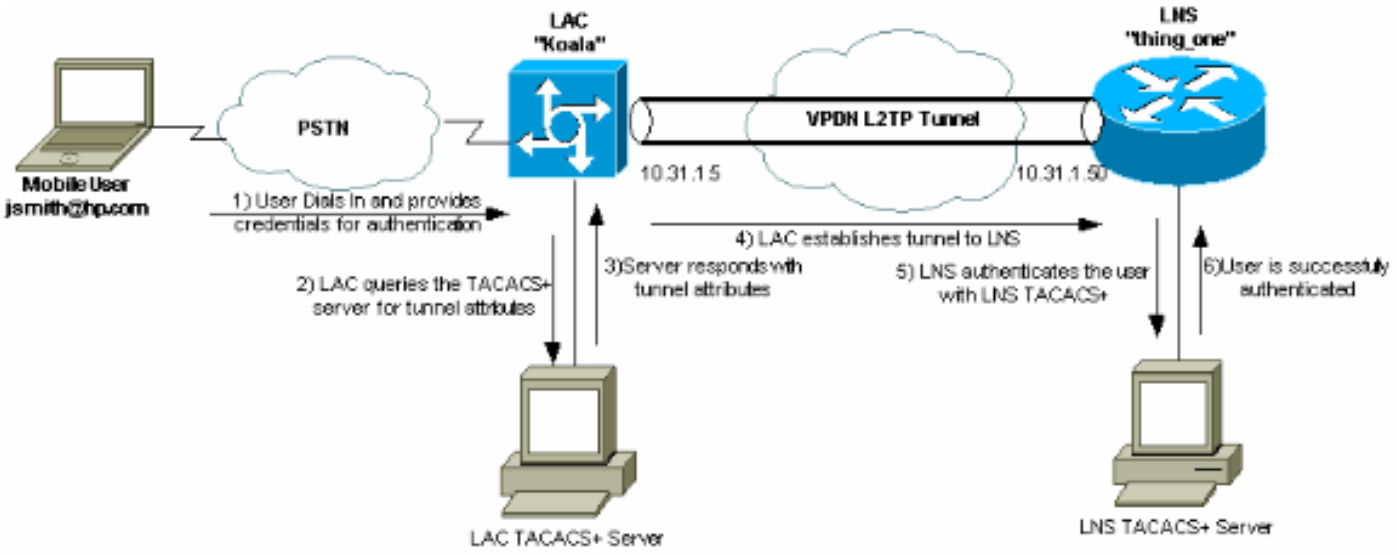
In diesem Beispiel lautet der Benutzer "jsmith@hp.com" mit dem Kennwort "test". Wenn sich "jsmith@hp.com" beim ISP-Router anwählt, sendet der ISP-Router die Benutzer-ID "hp.com" an den ISP TACACS+-Server. Der ISP-Server findet die "hp.com"-Benutzer-ID und sendet seine Tunnel-ID ("isp"), die IP-Adresse des HGW-Routers (10.31.1.50), das Network Access Server (NAS)-Kennwort ("hello") und das Gateway-Kennwort ("dorthin") zurück an den ISP-Router.

Der ISP-Router initiiert einen Tunnel und stellt eine Verbindung zum HGW-Router her, der die Passwörter für die Benutzer-ID "hp-gw" ("dorthin") und anschließend die Benutzerid "isp" ("hello") an den HGW TACACS+-Server weiterleitet. Sobald die Tunnel eingerichtet sind, leitet der ISP-Router die Benutzer-ID ("jsmith@hp.com") und das Kennwort ("test") des Benutzers, der sich einwählt, an den HGW-Router weiter. Dieser Benutzer wird auf dem HGW-Server authentifiziert. In den Beispielkonfigurationen in diesem Dokument lautet der Hostname des ISP-Routers "koala" und der Hostname des HGW-Routers "thing_one".

Hinweis: Um weitere Informationen zu den in diesem Dokument verwendeten Befehlen zu erhalten, verwenden Sie das Command Lookup Tool (nur registrierte Kunden).

Netzwerkdiagramm

In diesem Dokument wird die in diesem Diagramm dargestellte Netzwerkeinrichtung verwendet.



TACACS+-Serverkonfigurationen

In diesem Dokument werden die hier gezeigten Serverkonfigurationen verwendet.

- TACACS+-Freeware
- Cisco Secure ACS für UNIX 2.x.x

TACACS+-Freeware

```
!--- 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 für 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 { } } }
```

Router-Konfigurationen

In diesem Dokument werden die hier gezeigten Konfigurationen verwendet.

- ISP-Router
- HGW-Router

ISP-Router-Konfiguration

```
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
```

Konfiguration des HGW-Routers

```
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
```

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle.

- **debug aaa authentication**: Zeigt Informationen zur AAA-/TACACS+-Authentifizierung (Authentication, Authorization, Accounting) und TACACS+-Authentifizierung an.
- **debug aaa autorization**: Zeigt Informationen zur AAA/TACACS+-Autorisierung an.
- **debug ppp negotiation**: Zeigt PPP-Pakete an, die während des PPP-Starts übertragen werden und über die PPP-Optionen ausgehandelt werden.
- **debug tacacs+**: Zeigt detaillierte Debuginformationen zu TACACS+ an.
- **debug vpdn errors** (**vpdn-Fehler debuggen**): Zeigt Fehler an, die verhindern, dass ein PPP-Tunnel erstellt wird, oder Fehler, die das Schließen eines erstellten Tunnels verursachen.
- **debug vpdn events**: Zeigt Meldungen über Ereignisse an, die Teil der normalen PPP-Tunneleinrichtung oder des normalen Herunterfahrens sind.
- **debug vpdn l2f-errors**: Zeigt Layer-2-Protokollfehler an, die eine Layer-2-Einrichtung verhindern oder deren normalen Betrieb verhindern.
- **debug vpdn l2f-events**: Zeigt Meldungen über Ereignisse an, die zum normalen PPP-Tunnelaufbau oder -Herunterfahren für Layer 2 gehören.
- **debug vpdn l2f-pakete**: Zeigt Meldungen über Header und Status des Layer-2-Forwarding-Protokolls an.
- **debug vpdn pakete**: Zeigt Layer 2 Tunnel Protocol (L2TP)-Fehler und -Ereignisse an, die Teil der normalen Tunneleinrichtung oder -abschaltung für VPDNs sind.
- **debug vtemplate**: Zeigt Informationen zum Klonen einer virtuellen Zugriffsschnittstelle an, vom Zeitpunkt des Klonens von einer virtuellen Vorlage bis hin zum Zeitpunkt des Abbruchs der virtuellen Zugriffsschnittstelle beim Beenden des Anrufs.

Beispielausgabe für Debugging

Diese Debuggen werden als Referenz bereitgestellt.

- ISP-Router - gute Fehlerbehebung
- HGW-Router Gute Fehlersuche
- Debugger für fehlgeschlagene Verbindung auf ISP-Router
- Debugger für fehlgeschlagene Verbindungen auf dem HGW-Router

ISP-Router - gute Fehlerbehebung

```
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#
```

HGW-Router Gute Fehlersuche

```
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#
```

Debugger für fehlerhafte Verbindung auf ISP-Router

```
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
```

Debugger für fehlgeschlagene Verbindungen auf dem HGW-Router

```
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
```

Zugehörige Informationen

- Support-Seite für Cisco Secure ACS für UNIX
- Support-Seite für TACACS+
- Technischer Support und Dokumentation - Cisco Systems