Konfigurieren benutzerspezifischer VPDNs ohne Domänen- oder DNIS-Informationen

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für benutzerspezifische VPDNs ohne Domänen- oder DNIS-Informationen.

Voraussetzungen

Anforderungen

Für dieses Dokument bestehen keine speziellen Anforderungen.

Verwendete Komponenten

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

- Cisco IOS® Softwareversion 12.1(4) oder höher
- Cisco IOS Software, Version 12.1(4)T oder 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 unter Cisco Technical Tips Conventions.

Hintergrundinformationen

In VPDN-Szenarien (Virtual Private Dial-up Network) stellt der Netzwerkzugriffsserver (NAS) (ein L2TP-Zugriffskonzentrator oder LAC) den VPDN-Tunnel zum Home Gateway (LNS) auf der Grundlage benutzerspezifischer Informationen her. Dieser VPDN-Tunnel kann Level-2-Forwarding (L2F) oder Layer-2-Tunneling-Protokoll (L2TP) sein. Um zu bestimmen, ob ein Benutzer einen VPDN-Tunnel verwenden soll, überprüfen Sie:

- Legt fest, ob der Domänenname als Teil des Benutzernamens enthalten ist. Mit dem Benutzernamen tunnelme@cisco.com leitet das NAS diesen Benutzer zum Tunnel für cisco.com weiter.
- Der Dienst für Informationen zur gewählten Rufnummer (Dialed Number Information Service, DNIS). Dies ist die Anrufweiterleitung basierend auf der angerufenen Nummer. Das bedeutet, dass das NAS-Gerät alle Anrufe mit einer bestimmten angerufenen Nummer an den entsprechenden Tunnel weiterleiten kann. Wenn beispielsweise ein eingehender Anruf die angerufene Nummer 5551111 hat, kann der Anruf an den VPDN-Tunnel weitergeleitet werden, während ein Anruf an 552222 nicht weitergeleitet wird. Für diese Funktion muss das Telco-Netzwerk Informationen zur angerufenen Nummer bereitstellen.

Weitere Informationen zur VPDN-Konfiguration finden Sie unter VPDN-Verständnis.

In einigen Fällen müssen Sie möglicherweise einen VPDN-Tunnel für jeden Benutzernamen initiieren, mit oder ohne dass ein Domänenname erforderlich ist. Der Benutzer **ciscouser** kann beispielsweise auf **cisco.com** getunnelt werden, während andere Benutzer lokal auf dem NAS terminiert werden können.

Hinweis: Dieser Benutzername enthält nicht die Domäneninformationen wie im vorherigen Beispiel.

Die VPDN-Konfigurationsfunktion pro Benutzer sendet beim ersten Kontakt des Routers mit dem AAA-Server den gesamten strukturierten Benutzernamen an den AAA-Server (Authentication, Authorization, Accounting). So kann die Cisco IOS-Software Tunnelattribute für einzelne Benutzer anpassen, die einen gemeinsamen Domänennamen oder DNIS verwenden.

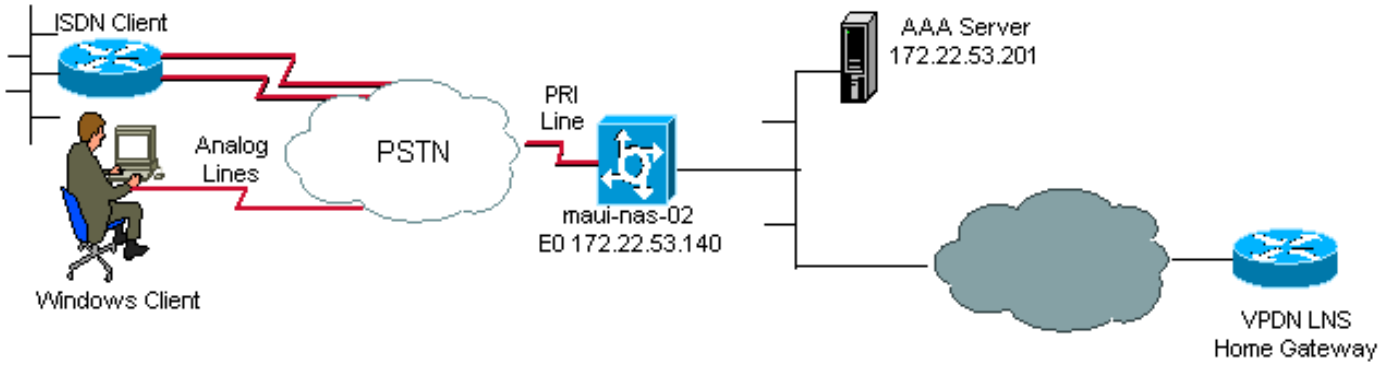
Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

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 folgende Netzwerkeinrichtung verwendet:



Konfigurationen

Die einzigen VPDN-Befehle, die auf dem NAS (LAC) für die Unterstützung von VPDNs pro Benutzer erforderlich sind, sind die globalen Konfigurationsbefehle **vpdn enable** und **vpdn authen-before-forward**. Der Befehl **vpdn authen-before-forward** weist das NAS (LAC) an, den vollständigen Benutzernamen zu authentifizieren, bevor eine Weiterleitungsentscheidung getroffen wird. Anschließend wird anhand der vom AAA-Server für diesen einzelnen Benutzer zurückgegebenen Informationen ein VPDN-Tunnel erstellt. Wenn keine VPDN-Informationen vom AAA-Server zurückgegeben werden, wird der Benutzer lokal terminiert. Die Konfiguration in diesem Abschnitt zeigt die Befehle, die zur Unterstützung von Tunneln ohne die Domäneninformationen im Benutzernamen erforderlich sind.

Hinweis: Diese Konfiguration ist nicht vollständig. Enthalten sind nur die relevanten VPDN-, Schnittstellen- und AAA-Befehle.

Hinweis: Es geht nicht um dieses Dokument, jedes mögliche Tunnelprotokoll und AAA-Protokoll zu besprechen. Daher wird bei dieser Konfiguration ein L2TP-Tunnel mit AAA RADIUS-Server implementiert. Passen Sie die hier beschriebenen Prinzipien und Konfigurationen an, um andere Tunneltypen oder AAA-Protokolle zu konfigurieren.

In diesem Dokument wird diese Konfiguration verwendet:

- VPDN NAS (LAC)

VPDN NAS (LAC)

```
aaa new-model
aaa authentication ppp default group radius
!--- Use RADIUS authentication for PPP authentication.
aaa authorization network default group radius !---
Obtain authorization information from the Radius server.
!--- This command is required for the AAA server to
provide VPDN attributes. ! vpdn enable !--- VPDN is
enabled. vpdn authen-before-forward !--- Authenticate
the complete username before making a forwarding
decision. !--- The LAC sends the username to the AAA
server for VPDN attributes. ! controller E1 0 pri-group
timeslots 1-31 ! interface Serial0:15 dialer rotary-
group 1 !--- D-channel for E1 0 is a member of the
dialer rotary group 1. ! interface Dialer1 !--- Logical
```

```
interface for dialer rotary group 1. ip unnumbered
Ethernet0 encapsulation ppp dialer in-band dialer-group
1 ppp authentication chap pap callin ! radius-server
host 172.22.53.201 !--- The IP address of the RADIUS
server host. !--- This AAA server will supply the
NAS(LAC) with the VPDN attributes for the user. radius-
server key cisco !--- The RADIUS server key.
```

RADIUS-Serverkonfiguration

Hier einige Benutzerkonfigurationen auf einem RADIUS-Server von Cisco Secure for Unix (CSU):

1. Ein Benutzer, der lokal auf dem NAS terminiert werden soll:
   ```
   user1 Password = "cisco"
   Service-Type = Framed-User
   ```
2. Ein Benutzer, für den eine VPDN-Sitzung eingerichtet werden soll:
   ```
   user2           Password = "cisco"
   Service-Type = Framed-User,
   Cisco-AVPair = "vpdn:ip-addresses=172.22.53.141",
   Cisco-AVPair = "vpdn:l2tp-tunnel-password=cisco",
   Cisco-AVPair = "vpdn:tunnel-type=l2tp"
   ```

Das NAS (LAC) verwendet die mit dem Cisco-AVPair-VPDN angegebenen Attribute, um den VPDN-Tunnel zum Home Gateway zu initiieren. Stellen Sie sicher, dass Sie das Home Gateway so konfigurieren, dass VPDN-Tunnel vom NAS akzeptiert werden.

Überprüfen

Dieser Abschnitt enthält Informationen, mit denen Sie überprüfen können, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom Output Interpreter Tool unterstützt (nur registrierte Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **Anzeige des Anruferbenutzers** - Zeigt Parameter für einen bestimmten Benutzer an, z. B. verwendete TTY-Leitung, asynchrone Schnittstelle (Gehäuse, Steckplatz oder Port), DS0-Kanalnummer, Modemnummer, zugewiesene IP-Adresse, PPP- und PPP-Paketparameter usw. Wenn Ihre Version der Cisco IOS-Software diesen Befehl nicht unterstützt, verwenden Sie den Befehl **show user**.
- **show vpdn**: Zeigt Informationen über aktive L2F- und L2TP-Protokoll-Tunnel und Nachrichtenbezeichner in einem VPDN an.

Beispiel für die Ausgabe von Befehlen

Wenn die Verbindung hergestellt wird, verwenden Sie den **Befehl show caller user *username* sowie den** Befehl **show vpdn**, um zu überprüfen, ob der Anruf erfolgreich war. Nachstehend ist eine Beispielausgabe dargestellt:

```
maui-nas-02#show caller user vpdn_authen

  User: vpdn_authen, line tty 12, service Async
        Active time 00:09:01, Idle time 00:00:05
  Timeouts:           Absolute  Idle      Idle
```

```
                                Session   Exec
      Limits:           -       -         00:10:00
      Disconnect in:    -       -         -
  TTY: Line 12, running PPP on As12
  DS0: (slot/unit/channel)=0/0/5
  Line: Baud rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits
  Status: Ready, Active, No Exit Banner, Async Interface Active
          HW PPP Support Active
  Capabilities: Hardware Flowcontrol In, Hardware Flowcontrol Out
                Modem Callout, Modem RI is CD,
                Line is permanent async interface, Integrated Modem
  Modem State: Ready

  User: vpdn_authen, line As12, service PPP
        Active time 00:08:58, Idle time 00:00:05
  Timeouts:             Absolute  Idle
      Limits:           -         -
      Disconnect in:    -         -
  PPP: LCP Open, CHAP (<- AAA)
  IP: Local 172.22.53.140
  VPDN: NAS , MID 4, MID Unknown
        HGW , NAS CLID 0, HGW CLID 0, tunnel open
  !--- The VPDN tunnel is open. Counts: 85 packets input, 2642 bytes, 0 no buffer 0 input
errors, 0 CRC, 0 frame, 0 overrun 71 packets output, 1577 bytes, 0 underruns 0 output errors, 0
collisions, 0 interface resets maui-nas-02#show vpdn

L2TP Tunnel and Session Information Total tunnels 1 sessions 1

LocID RemID Remote Name   State  Remote Address  Port  Sessions
6318  3     HGW           est    172.22.53.141   1701  1

LocID RemID TunID Intf       Username      State  Last Chg Fastswitch
4     3     6318  As12       vpdn_authen   est    00:09:33 enabled
!--- The tunnel for user vpdn_authen is in established state. %No active L2F tunnels %No active
PPTP tunnels %No active PPPoE tunnel
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Befehle zur Fehlerbehebung

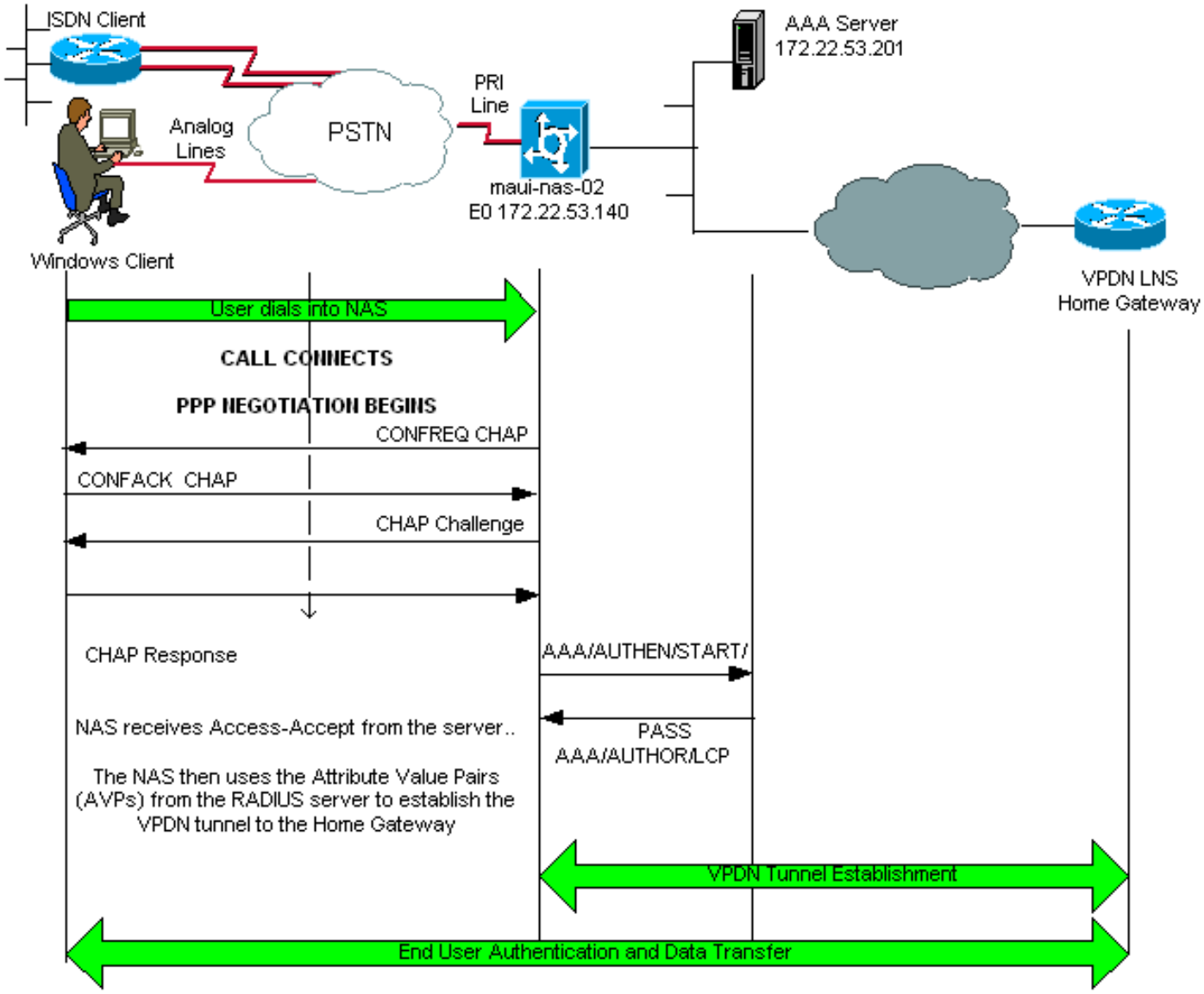
Hinweis: Bevor Sie **Debugbefehle** ausgeben, lesen Sie Wichtige Informationen über Debug-Befehle.

- **debug ppp authentication**: Zeigt Meldungen des PPP-Authentifizierungsprotokolls an und enthält den CHAP-Paketaustausch (Challenge Handshake Authentication Protocol) und den Austausch von PAP (Password Authentication Protocol).
- **debug aaa authentication**: Zeigt Informationen zur AAA-/RADIUS-Authentifizierung an.
- **debug aaa authorization**: Zeigt Informationen über die AAA-/RADIUS-Autorisierung an.
- **debug radius**: Zeigt detaillierte Debuginformationen an, die dem RADIUS zugeordnet sind. Verwenden Sie das Output Interpreter Tool (nur registrierte Kunden), um die Debug-Radius-Meldungen zu decodieren. Weitere Informationen finden Sie z. B. im Abschnitt Beispiel **debug** Output. Verwenden Sie die Informationen aus dem **Debugradius**, um zu bestimmen, welche Attribute ausgehandelt werden.
- **debug tacacs**: Zeigt detaillierte Debuginformationen für TACACS+ an.
- **debug vpdn event**: Zeigt L2x-Fehler und -Ereignisse an, die Teil der normalen

Tunneleinrichtung oder -abschaltung für VPDNs sind.
- **debug vpdn error**: Zeigt VPDN-Protokollfehler an.
- **debug vpdn l2x-event**: Zeigt detaillierte L2x-Fehler und -Ereignisse an, die Teil der normalen Tunneleinrichtung oder -abschaltung für VPDNs sind.
- **debug vpdn l2x-error**: Zeigt VPDN L2x-Protokollfehler an.

Beispielausgabe für Debugging

Hier ist die **Debug-**Ausgabe für einen erfolgreichen Aufruf. Beachten Sie in diesem Beispiel, dass das NAS die Attribute für den VPDN-Tunnel vom Radius-Server abruft.




```
maui-nas-02#show debug
General OS:
  AAA Authentication debugging is on
  AAA Authorization debugging is on
PPP:
  PPP authentication debugging is on
VPN:
  L2X protocol events debugging is on
  L2X protocol errors debugging is on
  VPDN events debugging is on
  VPDN errors debugging is onRadius protocol debugging is on
```

```
maui-nas-02#
*Jan 21 19:07:26.752: %ISDN-6-CONNECT: Interface Serial0:5 is now connected
to N/A N/A
!--- Incoming call. *Jan 21 19:07:55.352: %LINK-3-UPDOWN: Interface Async12, changed state to up
*Jan 21 19:07:55.352: As12 PPP: Treating connection as a dedicated line *Jan 21 19:07:55.352:
As12 AAA/AUTHOR/FSM: (0): LCP succeeds trivially *Jan 21 19:07:55.604: As12 CHAP: O CHALLENGE id
1 len 32 from "maui-nas-02" *Jan 21 19:07:55.732: As12 CHAP: I RESPONSE id 1 len 32 from
"vpdn_authen"
!--- Incoming CHAP response from user vpdn_authen. *Jan 21 19:07:55.732: AAA: parse name=Async12
idb type=10 tty=12 *Jan 21 19:07:55.732: AAA: name=Async12 flags=0x11 type=4 shelf=0 slot=0
adapter=0 port=12 channel=0 *Jan 21 19:07:55.732: AAA: parse name=Serial0:5 idb type=12 tty=-1
*Jan 21 19:07:55.732: AAA: name=Serial0:5 flags=0x51 type=1 shelf=0 slot=0 adapter=0 port=0
channel=5 *Jan 21 19:07:55.732: AAA/ACCT/DS0: channel=5, ds1=0, t3=0, slot=0, ds0=5 *Jan 21
19:07:55.732: AAA/MEMORY: create_user (0x628C79EC) user='vpdn_authen' ruser='' port='Async12'
rem_addr='async/81560' authen_type=CHAP service=PPP priv=1 *Jan 21 19:07:55.732:
AAA/AUTHEN/START (4048817807): port='Async12' list='' action=LOGIN service=PPP *Jan 21
19:07:55.732: AAA/AUTHEN/START (4048817807): using "default" list *Jan 21 19:07:55.732:
AAA/AUTHEN/START (4048817807): Method=radius (radius) *Jan 21 19:07:55.736: RADIUS: ustruct
sharecount=1 *Jan 21 19:07:55.736: RADIUS: Initial Transmit Async12 id
6 172.22.53.201:1645, Access-Request, len 89
*Jan 21 19:07:55.736:         Attribute 4 6 AC16358C
*Jan 21 19:07:55.736:         Attribute 5 6 0000000C
*Jan 21 19:07:55.736:         Attribute 61 6 00000000
*Jan 21 19:07:55.736:         Attribute 1 13 7670646E
*Jan 21 19:07:55.736:         Attribute 30 7 38313536
*Jan 21 19:07:55.736:         Attribute 3 19 014CF9D6
*Jan 21 19:07:55.736:         Attribute 6 6 00000002
*Jan 21 19:07:55.736:         Attribute 7 6 00000001
*Jan 21 19:07:55.740: RADIUS: Received from id 6 172.22.53.201:1645,
Access-Accept, len 136
*Jan 21 19:07:55.740:         Attribute 6 6 00000002
*Jan 21 19:07:55.740:         Attribute 26 40 0000000901227670
*Jan 21 19:07:55.740:         Attribute 26 40 0000000901227670
*Jan 21 19:07:55.740:         Attribute 26 30 0000000901187670
```

Die für den VPDN-Tunnel erforderlichen Attributwertpaare (AVPs) werden vom RADIUS-Server heruntergefahren. Der **Debugradius** erzeugt jedoch eine codierte Ausgabe, die die AVPs und deren Werte angibt. Sie können die oben in **Fettschrift** dargestellte Ausgabe im Output Interpreter Tool einfügen (nur registrierte Kunden). Die folgende fettgedruckte Ausgabe ist die vom Tool erhaltene dekodierte Ausgabe:

```
Access-Request 172.22.53.201:1645 id 6
Attribute Type 4:  NAS-IP-Address is 172.22.53.140
Attribute Type 5:  NAS-Port is 12
Attribute Type 61: NAS-Port-Type is Asynchronous
Attribute Type 1:  User-Name is vpdn
Attribute Type 30: Called-Station-ID(DNIS) is 8156
Attribute Type 3:  CHAP-Password is (encoded)
Attribute Type 6:  Service-Type is Framed
Attribute Type 7:  Framed-Protocol is PPP
        Access-Accept 172.22.53.201:1645 id 6
Attribute Type 6:  Service-Type is Framed
Attribute Type 26: Vendor is Cisco
Attribute Type 26: Vendor is Cisco
Attribute Type 26: Vendor is Cisco
*Jan 21 19:07:55.740: AAA/AUTHEN (4048817807): status = PASS
...
...
...
```

```
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:ip-addresses=172.22.53.141"
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:l2tp-tunnel-password=cisco"
*Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:tunnel-type=l2tp"
*Jan 21 19:07:55.744: AAA/AUTHOR (733932081): Post authorization status = PASS_REPL
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV service=ppp
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV ip-addresses=172.22.53.141
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV l2tp-tunnel-password=cisco
*Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp
 !--- Tunnel information. !--- The VPDN Tunnel will now be established and the call will be
authenticated. !--- Since the debug information is similar to that for a normal VPDN call, !---
the VPDN tunnel establishment debug output is omitted.
```

Zugehörige Informationen

- VPDN im Überblick
- Konfigurieren von Virtual Private Dialup Networks
- Konfigurieren der Layer-2-Tunnelprotokollauthentifizierung mit RADIUS
- Konfigurieren der Layer-2-Tunnelprotokollauthentifizierung mit TACACS+
- Support-Seiten für Technologien aufrufen
- Technischer Support - Cisco Systems