Einwahl-VPDN-Konfiguration mithilfe von VPDN-Gruppen und TACACS+

Inhalt

Einführung

Dieses Dokument enthält eine Beispielkonfiguration für Virtual Private Dialup Networks (VPDN) mit VPDN-Gruppen und Terminal Access Controller Access Control System Plus (TACACS+).

Voraussetzungen

Anforderungen

Stellen Sie vor dem Versuch dieser Konfiguration sicher, dass Sie die folgenden Anforderungen erfüllen:

Sie benötigen Folgendes:

- Ein Cisco Router für den Client-Zugriff (NAS/LAC) und ein Cisco Router für den Netzwerkzugriff (HGW/LNS) mit IP-Konnektivität zwischen ihnen.
- Hostnamen der Router oder lokale Namen, die in den VPDN-Gruppen verwendet werden sollen.
- Das zu verwendende Tunneling-Protokoll. Dabei kann es sich entweder um das Layer 2 Tunneling (L2T)-Protokoll oder das Layer 2 Forwarding (L2F)-Protokoll handeln.
- Ein Passwort für die Router zur Authentifizierung des Tunnels.
- Ein Tunneling-Kriterium. Dabei kann es sich um den Domänennamen oder den Dienst für die

Identifizierung gewählter Rufnummern (Dialed Number Identification Service, DNIS) handeln.
- Benutzernamen und Kennwörter für den Benutzer (Einwahl des Clients).
- IP-Adressen und -Schlüssel für Ihre TACACS+-Server.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

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

Eine ausführliche Einführung in Virtual Private Dialup Networks (VPDN)- und VPDN-Gruppen finden Sie unter Understanding VPDN. Dieses Dokument wird in der VDPN-Konfiguration erweitert und fügt das Terminal Access Controller Access Control System Plus (TACACS+) hinzu.

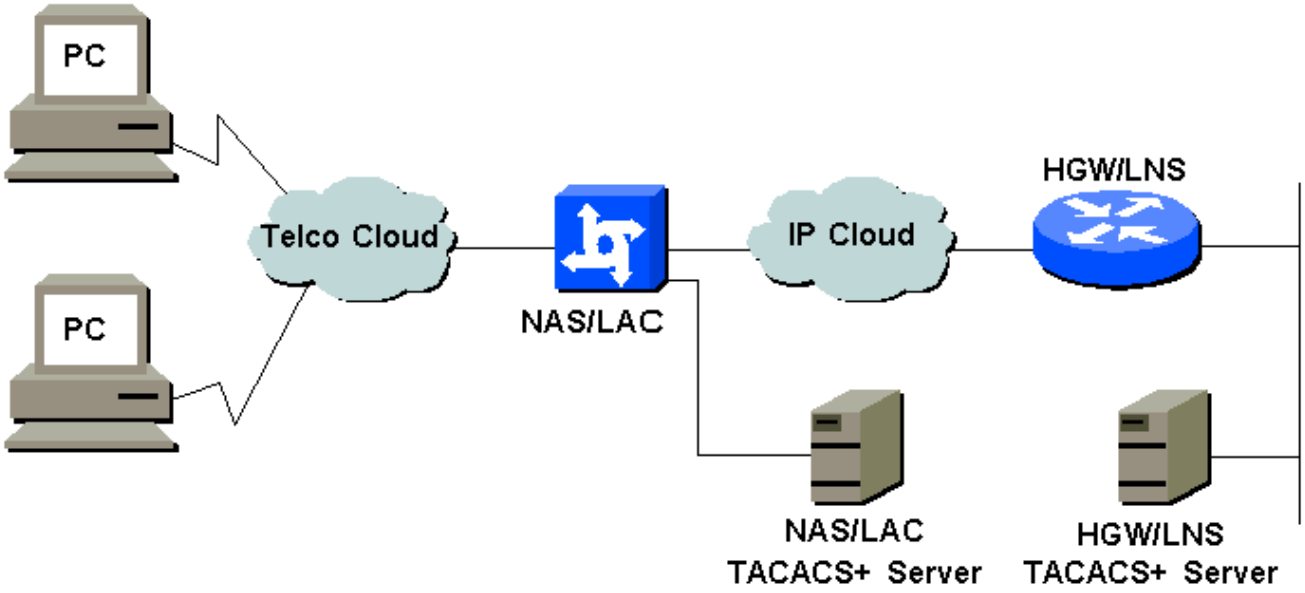
Konfigurieren

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

In diesem Dokument werden folgende Konfigurationen verwendet:

- NAS/LAC
- HGW/LNS
- NAS/LAC TACACS+-Konfigurationsdatei
- HGW/LNS TACACS+-Konfigurationsdatei

NAS/LAC

```
!
version 12.0
service timestamps debug datetime msec
service timestamps log datetime msec
!
hostname as5300
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
enable password somethingSecret
!
username john password 0 secret4me
!
ip subnet-zero
!
vpdn enable
!
isdn switch-type primary-5ess
!
controller T1 0
 framing esf
 clock source line primary
 linecode b8zs
 pri-group timeslots 1-24
!
```

```
controller T1 1
 framing esf
 clock source line secondary 1
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 2
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
controller T1 3
 framing esf
 linecode b8zs
 pri-group timeslots 1-24
!
interface Ethernet0
 ip address 172.16.186.52 255.255.255.240
 no ip directed-broadcast
!
interface Serial023
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 ip tcp header-compression passive
 dialer rotary-group 1
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no cdp enable
!
interface Serial123
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 ip tcp header-compression passive
 dialer rotary-group 1
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no cdp enable
!
interface Serial223
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 ip tcp header-compression passive
 dialer rotary-group 1
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no cdp enable
!
interface Serial323
 no ip address
 no ip directed-broadcast
 encapsulation ppp
 ip tcp header-compression passive
 dialer rotary-group 1
 isdn switch-type primary-5ess
 isdn incoming-voice modem
 no cdp enable
!
interface FastEthernet0
 no ip address
 no ip directed-broadcast
 shutdown
```

```
!
interface Group-Async1
 ip unnumbered Ethernet0
 no ip directed-broadcast
 encapsulation ppp
 ip tcp header-compression passive
 async mode interactive
 peer default ip address pool IPaddressPool
 no cdp enable
 ppp authentication chap
 group-range 1 96
!
interface Dialer1
 ip unnumbered Ethernet0
 no ip directed-broadcast
 encapsulation ppp
 ip tcp header-compression passive
 dialer-group 1
 peer default ip address pool IPaddressPool
 no cdp enable
 ppp authentication chap
!
ip local pool IPaddressPool 10.10.10.1 10.10.10.254
no ip http server
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.186.49
!
tacacs-server host 172.16.171.9
tacacs-server key 2easy
!
line con 0
 login authentication CONSOLE
 transport input none
line 1 96
 autoselect during-login
 autoselect ppp
 modem Dialin
line aux 0
line vty 0 4
!
end
```

HGW/LNS

```
!
version 12.0
service timestamps debug uptime
service timestamps log uptime
!
hostname access-9
!
aaa new-model
aaa authentication login default local
aaa authentication login CONSOLE none
aaa authentication ppp default if-needed group tacacs+
aaa authorization network default group tacacs+
enable password somethingSecret
!
ip subnet-zero
!
vpdn enable
!
```

```
vpdn-group DEFAULT
! Default L2TP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
 local name LNS
 lcp renegotiation always
 l2tp tunnel password 0 not2tell
!
vpdn-group POP1
 accept-dialin
  protocol l2tp
  virtual-template 2
 terminate-from hostname LAC
 local name LNS
 l2tp tunnel password 0 2secret
!
vpdn-group POP2
 accept-dialin
  protocol l2f
  virtual-template 3
 terminate-from hostname NAS
 local name HGW
 lcp renegotiation always
!
interface FastEthernet0/0
 ip address 172.16.186.1 255.255.255.240
 no ip directed-broadcast
!
interface Virtual-Template1
 ip unnumbered FastEthernet0/0
 no ip directed-broadcast
 ip tcp header-compression passive
 peer default ip address pool IPaddressPool
 ppp authentication chap
!
interface Virtual-Template2
 ip unnumbered Ethernet0/0
 no ip directed-broadcast
 ip tcp header-compression passive
 peer default ip address pool IPaddressPoolPOP1
 compress stac
 ppp authentication chap
!
interface Virtual-Template3
 ip unnumbered Ethernet0/0
 no ip directed-broadcast
 ip tcp header-compression passive
 peer default ip address pool IPaddressPoolPOP2
 ppp authentication pap
 ppp multilink
!
ip local pool IPaddressPool 10.10.10.1 10.10.10.254
ip local pool IPaddressPoolPOP1 10.1.1.1 10.1.1.254
ip local pool IPaddressPoolPOP2 10.1.2.1 10.1.2.254
ip classless
no ip http server
!
tacacs-server host 172.16.186.9
tacacs-server key not2difficult
!
line con 0

login authentication CONSOLE
```

```
transport input none
line 97 120
line aux 0
line vty 0 4
!
!
end
```

NAS/LAC TACACS+-Konfigurationsdatei

```
key = 2easy

# Use L2TP tunnel to 172.16.186.1 when 4085555100 is
dialed
user = dnis:4085555100 {
         service = ppp protocol = vpdn {
           tunnel-id = anonymous
           ip-addresses = 172.16.186.1
           tunnel-type = l2tp
         }
       }

# Password for tunnel authentication
user = anonymous {
         chap = cleartext not2tell
       }

###

# Use L2TP tunnel to 172.16.186.1 when 4085555200 is
dialed
user = dnis:4085555200 {
         service = ppp protocol = vpdn {
           tunnel-id = LAC
           ip-addresses = 172.16.186.1
           tunnel-type = l2tp
         }
       }

# Password for tunnel authentication
user = LAC {
         chap = cleartext 2secret
       }

###

# Use L2F tunnel to 172.16.186.1 when user authenticates
with cisco.com domain
user = cisco.com {
         service = ppp protocol = vpdn {
           tunnel-id = NAS
           ip-addresses = 172.16.186.1
           tunnel-type = l2f
         }
       }

# Password for tunnel authentication
user = NAS {
         chap = cleartext cisco
       }

# Password for tunnel authentication
```

```
user = HGW {
         chap = cleartext cisco
       }
```

HGW/LNS TACACS+-Konfigurationsdatei

```
key = not2difficult

# Password for tunnel authentication
user = NAS {
         chap = cleartext cisco
       }

# Password for tunnel authentication
user = HGW {
         chap = cleartext cisco
       }

user = santiago {
         chap = cleartext letmein

         service = ppp protocol = lcp { }
         service = ppp protocol = ip { }
       }

user = santiago@cisco.com {
         global = cleartext letmein

         service = ppp protocol = lcp { }
         service = ppp protocol = multilink { }
         service = ppp protocol = ip { }
       }
```

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.

- **show vpdn tunnel all** - Zeigt Details aller aktiven Tunnel an.
- **show user** (Benutzer anzeigen): Zeigt den Namen des Benutzers an, der verbunden ist.
- **show interface virtual-access #** - Ermöglicht Ihnen, den Status einer bestimmten virtuellen Schnittstelle im HGW/LNS zu überprüfen.

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 vpdn l2x-events** - Zeigt den Dialog zwischen NAS/LAC und HGW/LNS für die Tunnel- oder Sitzungserstellung an.
- **debug ppp authentication**: Ermöglicht Ihnen zu überprüfen, ob ein Client die Authentifizierung übergibt.
- **debug ppp negotiation**: Ermöglicht Ihnen zu überprüfen, ob ein Client PPP-Aushandlung übergibt. Sie können sehen, welche Optionen (z. B. Callback, MLP usw.) und welche Protokolle (z. B. IP, IPX usw.) ausgehandelt werden.
- **debug ppp error** (**ppp-Fehler debuggen**): Zeigt Protokollfehler und Fehlerstatistiken an, die mit der Aushandlung und Ausführung von PPP-Verbindungen verknüpft sind.
- **debug vtemplate**: Zeigt das Klonen von virtuellen Zugriffsschnittstellen auf dem HGW/LNS an. Sie können sehen, wann die Schnittstelle erstellt wird (aus der virtuellen Vorlage geklont), und wann die Schnittstelle bei Beendigung der Verbindung zerstört wird.
- **debug aaa authentication**: Ermöglicht Ihnen zu überprüfen, ob der Benutzer oder Tunnel vom AAA-Server (Authentication, Authorization, Accounting) authentifiziert wird.
- **debug aaa authorized** (**debug aaa-Autorisierung**) - Hiermit können Sie überprüfen, ob der Benutzer vom AAA-Server autorisiert wird.
- **debug aaa per user** - Ermöglicht es Ihnen zu überprüfen, was auf jeden authentifizierten Benutzer angewendet wird. Dies unterscheidet sich von allgemeinen Debuggen, die oben aufgeführt sind.

Zugehörige Informationen

- Support-Seiten für Technologie - Wählen
- Technischer Support - Cisco Systems