

Configuración de VPDN del dial-in usando los grupos de VPDN y el TACACS+

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Convenciones](#)

[Antecedentes](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Verificación](#)

[Troubleshooting](#)

[Comandos para resolución de problemas](#)

[Información Relacionada](#)

Introducción

Este documento proporciona una configuración de muestra para los Virtual Private Dialup Networks del dial-in (VPDN), usando los grupos de VPDN y el Terminal Access Controller Access Control System más (TACACS+).

prerrequisitos

Requisitos

Antes de utilizar esta configuración, asegúrese de que cumple con estos requisitos:

Usted necesita tener:

- Un router Cisco para el acceso al cliente (NAS/LAC), y un router Cisco para el acceso a la red (HGW/LNS) con la conectividad del IP entre ellos.
- Nombres del host del Routers, o nombres locales a utilizar en los grupos de VPDN.
- El Tunneling Protocol a utilizar. Éste puede ser o protocolo del Tunelización de la capa 2 (L2T), o acode 2 el protocolo de envío (L2F).
- Una contraseña para que el Routers autentique el túnel.
- Un criterio del Tunelización. Éste podía ser el Domain Name, o el Dialed Number Identification Service (DNIS).

- Nombres de usuario y contraseñas para el usuario (cliente que marca adentro).
- IP Addresses y claves para sus servidores TACACS+.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

Antecedentes

Para una introducción detallada a los Virtual Private Dialup Networks (VPDN) y a los grupos de VPDN, vea [comprensión del VPDN](#). Este documento se amplía en la configuración VPDN, y agrega el Terminal Access Controller Access Control System más (TACACS+).

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Nota: Para obtener información adicional sobre los comandos que se utilizan en este documento, use la Command Lookup Tool (solo para clientes [registrados](#)).

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Configuraciones

En este documento, se utilizan estas configuraciones:

- NAS/LAC
- HGW/LNS
- Archivo de configuración NAS/LAC TACACS+
- Archivo de configuración HGW/LNS TACACS+

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-Templat1  
  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

```

Archivo de configuración NAS/LAC TACACS+

```

key = 2easy

# Use L2TP tunnel to 172.16.186.1 when 4085555100 is
dialled
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
dialled
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
}

```

Archivo de configuración HGW/LNS TACACS+

```

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 { }
}

```

Verificación

En esta sección encontrará información que puede utilizar para confirmar que su configuración esté funcionando correctamente.

La herramienta [Output Interpreter](#) (sólo para clientes [registrados](#)) permite utilizar algunos

comandos “show” y ver un análisis del resultado de estos comandos.

- **show vpdn tunnel all** — detalles de las visualizaciones de todos los túneles activos.
- **usuario de la demostración** — visualiza el nombre del usuario que está conectado.
- **show interface virtual-access -** — le permite para marcar el estatus de una interfaz virtual determinada en el HGW/LNS.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

Comandos para resolución de problemas

Nota: [Antes de ejecutar un comando de depuración, consulte Información importante sobre comandos de depuración.](#)

- **debug vpdn l2x-events** — visualiza el diálogo entre el NAS/LAC y el HGW/LNS para el túnel o la creación de sesión.
- **autenticación PPP del debug** — le permite para marcar si un cliente está pasando la autenticación.
- **negociación ppp del debug** — le permite para marcar si un cliente está pasando la negociación PPP. Usted podría ver qué opciones (por ejemplo, servicio repetido, MLP, y así sucesivamente), y qué protocolos (por ejemplo, IP, IPX, y así sucesivamente) se están negociando.
- **debug ppp error** — errores del protocolo y estadística de errores de las visualizaciones, asociados a la negociación de la conexión PPP y a la operación.
- **debug vtemplate** — visualiza la reproducción de las interfaces de acceso virtual en el HGW/LNS. Usted puede ver cuando la interfaz se crea (reproducido de la plantilla virtual) al principio de la conexión de marcación manual, y cuando se destruye la interfaz cuando la conexión termina.
- **autenticación aaa del debug** — le permite para marcar si el servidor del Authentication, Authorization, and Accounting (AAA) está autenticando al usuario o el túnel.
- **debug aaa authorization** — le permite para marcar si al servidor de AAA está autorizando al usuario.
- **el debug aaa por usuario** — le permite para marcar qué se aplica a cada usuario se autentique que. Esto es diferente de los debugs generales enumerados arriba.

Información Relacionada

- [Páginas de soporte de la tecnología - Dial](#)
- [Soporte Técnico - Cisco Systems](#)