Configuración de VPDN de Marcado Usando Grupos VPDN y TACACS+

Contenido

Introducción

Este documento proporciona una configuración de ejemplo para redes de marcado privadas virtuales (VPDN), utilizando grupos VPDN y Terminal Access Controller Access Control System Plus (TACACS+).

Prerequisites

Requirements

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

Necesita tener:

- Un router Cisco para el acceso de cliente (NAS/LAC) y un router Cisco para el acceso a la red (HGW/LNS) con conectividad IP entre ellos.
- Nombres de host de los routers o nombres locales que se utilizarán en los grupos de VPDN.
- Protocolo de tunelización que se utilizará. Puede ser protocolo de tunelación de capa 2 (L2T) o protocolo de reenvío de capa 2 (L2F).
- Una contraseña para que los routers autentiquen el túnel.
- Un criterio de tunelización. Puede ser el nombre de dominio o el servicio de identificación de número marcado (DNIS).

- Nombres de usuario y contraseñas del usuario (marcación de cliente).
- Direcciones IP y claves para sus servidores TACACS+.

Componentes Utilizados

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

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Antecedentes

Para obtener una introducción detallada de las redes de marcado privadas virtuales (VPDN) y los grupos de VPDN, vea Comprensión de VPDN. Este documento se expande en la configuración VDPN y agrega Terminal Access Controller Access Control System Plus (TACACS+).

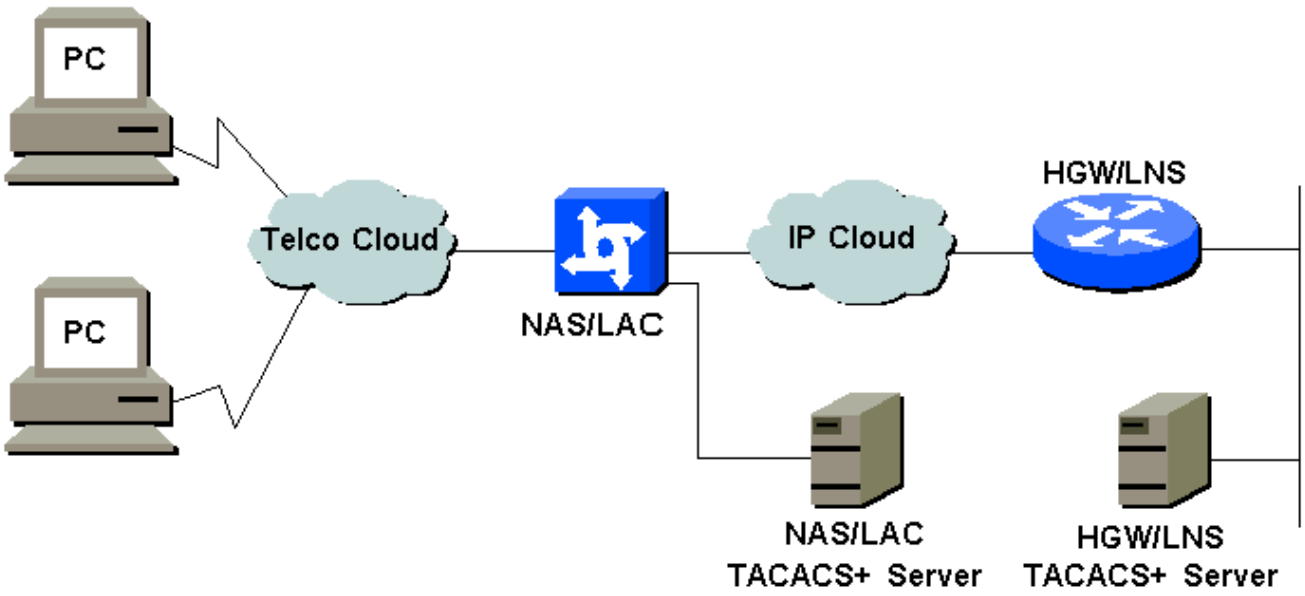
Configurar

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

Nota: Para encontrar información adicional sobre los comandos usados en este documento, utilice la Command Lookup Tool (sólo 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 TACACS+ NAS/LAC
- Archivo de configuración TACACS+ de HGW/LNS

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
```

Archivo de configuración TACACS+ NAS/LAC

```
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
       }
```

Archivo de configuración TACACS+ de HGW/LNS

```
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**: muestra los detalles de todos los túneles activos.
- **show user**: muestra el nombre del usuario que está conectado.
- **show interface virtual-access #**—permite verificar el estado de una interfaz virtual determinada en el HGW/LNS.

Troubleshoot

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

Comandos para resolución de problemas

Nota: Antes de ejecutar un comando **debug**, consulte Información Importante sobre Comandos Debug.

- **debug vpdn l2x-events**: muestra el diálogo entre NAS/LAC y HGW/LNS para la creación de túnel o sesión.
- **debug ppp authentication**: permite verificar si un cliente está pasando la autenticación.
- **debug ppp negotiation**: permite verificar si un cliente está pasando la negociación PPP. Podría ver qué opciones (como devolución de llamada, MLP, etc.) y qué protocolos (como IP, IPX, etc.) se están negociando.
- **debug ppp error**: muestra los errores de protocolo y las estadísticas de error asociadas con la negociación y operación de conexión PPP.
- **debug vtemplate**: muestra la clonación de interfaces de acceso virtual en el HGW/LNS. Puede ver cuándo se crea la interfaz (clonada a partir de la plantilla virtual) al principio de la conexión de marcación manual y cuándo se destruye la interfaz cuando se termina la conexión.
- **debug aaa authentication**: permite comprobar si el usuario o el túnel está siendo autenticado por el servidor de autenticación, autorización y contabilidad (AAA).
- **debug aaa authorization**: permite verificar si el usuario está siendo autorizado por el servidor AAA.
- **debug aaa per-user**: permite comprobar qué se aplica a cada usuario autenticado. Esto es diferente de las depuraciones generales enumeradas anteriormente.

Información Relacionada

- Páginas de soporte de tecnología - Marcar
- Soporte Técnico - Cisco Systems