Configuração de VPDN do discado usando grupos de VPDN e TACACS+

Índice

Introdução

Este documento fornece uma configuração de exemplo para o Virtual Private Dialup Networks do discado (VPDN), usando os grupos de VPDN e o protocolo tacacs+ (TACACS+).

Pré-requisitos

Requisitos

Antes de tentar esta configuração, verifique se estes requisitos são atendidos:

Você precisa de ter:

- Um roteador Cisco para o acesso do cliente (NAS/LAC), e um roteador Cisco para o acesso de rede (HGW/LNS) com conectividade IP entre eles.
- Nomes de host do Roteadores, ou nomes locais a usar-se nos grupos de VPDN.
- O protocolo de tunelamento a usar-se. Este pode ser ou protocolo do Tunelamento da camada 2 (L2T), ou mergulhe 2 o protocolo (L2F) de transmissão.
- Uma senha para que o Roteadores autentique o túnel.
- Um critério do Tunelamento. Este podia ser o Domain Name, ou o Dialed Number Identification Service (DNIS).
- Nomes de usuário e senhas para o usuário (cliente que disca dentro).

- Endereços IP de Um ou Mais Servidores Cisco ICM NT e chaves para seus server TACACS+.

Componentes Utilizados

Este documento não se restringe a versões de software e hardware específicas.

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Convenções

Para obter mais informações sobre convenções de documento, consulte as Convenções de dicas técnicas Cisco.

Informações de Apoio

Para uma introdução detalhada ao Virtual Private Dialup Networks (VPDN) e aos grupos de VPDN, veja compreendendo o VPDN. Este documento expande na configuração VDPN, e adiciona o protocolo tacacs+ (TACACS+).

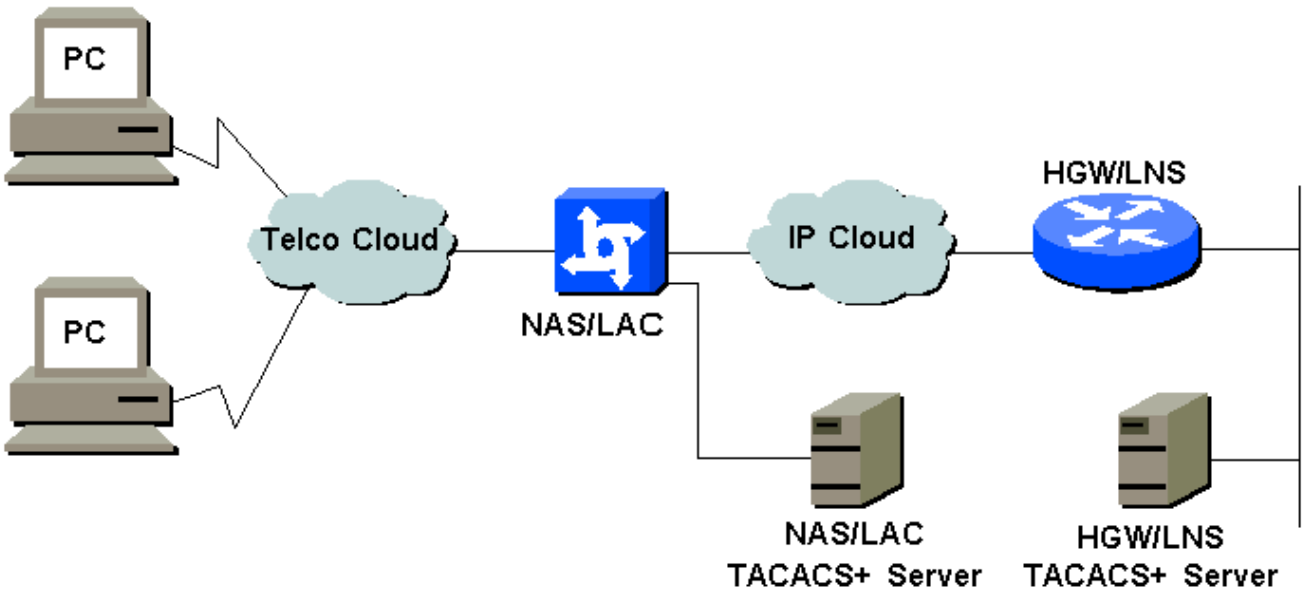
Configurar

Nesta seção, você encontrará informações para configurar os recursos descritos neste documento.

Nota: Para localizar informações adicionais sobre os comandos usados neste documento, utilize a Ferramenta Command Lookup (somente clientes registrados).

Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



Configurações

Este documento utiliza as seguintes configurações:

- NAS/LAC
- HGW/LNS
- Arquivo de configuração NAS/LAC TACACS+
- Arquivo de configuração 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-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
```

Arquivo de configuração NAS/LAC TACACS+

```
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
       }
```

Arquivo de configuração 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 { }
       }
```

Verificar

Esta seção fornece informações que você pode usar para confirmar se sua configuração está funcionando adequadamente.

A Output Interpreter Tool (somente clientes registrados) oferece suporte a determinados comandos show, o que permite exibir uma análise da saída do comando show.

- **show vpdn tunnel all** — detalhes dos indicadores de todos os túneis ativo.
- **usuário da mostra** — indica o nome do usuário que é conectado.
- **show interface virtual-access -** — permite-o de verificar o estado de uma interface particular virtual no HGW/LNS.

Troubleshooting

Esta seção fornece informações que podem ser usadas para o troubleshooting da sua configuração.

Comandos para Troubleshooting

Nota: Antes de emitir comandos de depuração, consulte as informações importantes sobre eles.

- **debug vpdn l2x-events** — indica o diálogo entre o NAS/LAC e o HGW/LNS para o túnel ou a criação de sessão.
- **debugar a autenticação de PPP** — permite-o de verificar se um cliente esteja passando a

autenticação.

- **debugar a negociação ppp** — permite-o de verificar se um cliente esteja passando a negociação de PPP. Você poderia ver que opções (como, rechamada, MLP, e assim por diante), e que protocolos (como, IP, IPX, e assim por diante) estão sendo negociados.
- **debug ppp error** — erros de protocolo e estatísticas de erros dos indicadores, associados com a negociação da conexão PPP e a operação.
- **debug vtemplate** — indica a clonagem das interfaces de acesso virtual no HGW/LNS. Você pode ver quando a relação está criada (clonado do molde virtual) no início da conexão dialup, e quando a relação está destruída quando a conexão termitated.
- **debugar a autenticação aaa** — permite-o de verificar se o usuário ou o túnel estejam sendo autenticados pelo server do Authentication, Authorization, and Accounting (AAA).
- **debug aaa authorization** — permite-o de verificar se o usuário esteja sendo autorizado pelo servidor AAA.
- **debugar o aaa por usuário** — permite-o de verificar o que é aplicado a cada usuário que é autenticado. Isto é diferente do general debuga listado acima.

Informações Relacionadas

- Páginas de suporte de tecnologia - Seletor
- Suporte Técnico - Cisco Systems