Конфигурация коммутируемой VPDN с использованием групп VPDN и TACACS+

Содержание

Введение

Этот документ предоставляет пример конфигурации для Виртуальных частных коммутируемых сетей (VPDN) наборного (телефонный) доступа, с помощью групп VPDN и Terminal Access Controller Access Control System (TACACS) Плюс (TACACS +).

Предварительные условия

Требования

Прежде чем использовать эту конфигурацию, убедитесь, что выполняются эти требования:

Вы должны иметь:

- Маршрутизатор Cisco для доступа клиента (NAS/LAC) и маршрутизатор Cisco для доступа к сети (HGW/LNS) с возможностью подключения с помощью IP-адреса между ними.
- Имена хоста маршрутизаторов или локальные имена для использования на группах VPDN.
- Протокол туннелирования для использования. Это может быть или протоколом Туннелирования уровня 2 (L2T) или протоколом переадресации уровня 2 (L2F).
- Пароль для маршрутизаторов для аутентификации туннеля.

- Туннелирующий критерий. Это могло быть или доменным именем, или Dialed Number Identification Service (DNIS).
- Имена пользователя и пароли для пользователя (клиент, набирающий в).
- IP-адреса и ключи для вашего TACACS + серверы.

Используемые компоненты

Настоящий документ не имеет жесткой привязки к каким-либо конкретным версиям программного обеспечения и оборудования.

Сведения, представленные в этом документе, были получены от устройств, работающих в специальной лабораторной среде. Все устройства, описанные в этом документе, были запущены с чистой (стандартной) конфигурацией. В рабочей сети необходимо изучить потенциальное воздействие всех команд до их использования.

Условные обозначения

Дополнительные сведения об условных обозначениях в документах см. Cisco Technical Tips Conventions.

Общие сведения

Для подробного введения к Виртуальным частным коммутируемым сетям (VPDN) и группам VPDN, посмотрите VPDN Понимания. Этот документ подробно останавливается на конфигурации VDPN и добавляет Terminal Access Controller Access Control System (TACACS) Плюс (TACACS +).

Настройка

В этом разделе содержатся сведения о настройке функций, описанных в этом документе.

Примечание: Поиск дополнительной информации о командах в данном документе можно выполнить с помощью средства "Command Lookup" (Поиск команд) (только для зарегистрированных клиентов).

Схема сети

В настоящем документе используется следующая схема сети:

Конфигурации

Эти конфигурации используются в данном документе:

- NAS/LAC
- HGW/LNS
- TACACS NAS/LAC + Файл config
- TACACS HGW/LNS + Файл config

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
```

TACACS NAS/LAC + Файл config

```
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
       }
```

TACACS HGW/LNS + Файл config

```
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 { }
       }
```

Проверка

В этом разделе содержатся сведения, которые помогают убедиться в надлежащей работе

конфигурации.

Некоторые команды show поддерживаются Средством интерпретации выходных данных(только зарегистрированные клиенты), которое позволяет просматривать аналитику выходных данных команды show.

- **show vpdn tunnel all** — отображает подробные данные всех активных туннелей.
- **show user** — отображает имя пользователя, который связан.
- **virtual-access show interface #** — позволяет вам проверить статус отдельного виртуального интерфейса на HGW/LNS.

Устранение неполадок

В этом разделе описывается процесс устранения неполадок конфигурации.

Команды для устранения неполадок

Примечание: Прежде чем вызывать команды debug, обратитесь к разделу Важные сведения о командах отладки.

- **debug vpdn l2x-event** — отображают диалоговое окно между NAS/LAC и HGW/LNS для туннеля или создания сеанса.
- **debug ppp authenticaion** — позволяет вам проверить, передает ли клиент аутентификацию.
- **debug ppp negotiation** — позволяет вам проверить, передает ли клиент согласование PPP. Вы видели, какие опции (такой как, обратный вызов, MLP, и так далее), и о каких протоколах (такой как, IP, IPX, и так далее) выполняют согласование.
- **debug ppp error – отображает ошибки протокола и статистику ошибок, связанных с согласованием и функционированием PPP-соединения.**
- **debug vtemplate** — отображает клонирование интерфейсов виртуального доступа на HGW/LNS. Вы видите, когда интерфейс создан (клонированный от виртуального шаблона) в начале подключения удаленного доступа, и когда интерфейс уничтожен, когда соединение является termitated.
- **debug aaa authentication** — позволяет вам проверить, аутентифицируются ли пользователь или туннель аутентификацией, авторизацией и учетом (AAA).
- **debug aaa authorization** — позволяет вам проверить, авторизуется ли пользователь AAA-сервером.
- **debug aaa per-user** — позволяет вам проверить то, что применено к каждому пользователю, который аутентифицируется. Это отличается от общих упомянутых выше отладок.

Дополнительные сведения

- Страницы поддержки технологии - набор
- Техническая поддержка - Cisco Systems