VPDN 그룹 및 TACACS+를 사용한 다이얼 인 VPDN 컨피그레이션

목차

소개

이 문서에서는 VPDN 그룹 및 TACACS+(Terminal Access Controller Access Control System Plus)를 사용하는 VPDN(Dial-in Virtual Private Dialup Networks)에 대한 샘플 컨피그레이션을 제공합니다.

사전 요구 사항

요구 사항

이 구성을 시도하기 전에 다음 요구 사항을 충족해야 합니다.

다음과 같은 기능이 필요합니다.

- 클라이언트 액세스를 위한 Cisco 라우터(NAS/LAC), 네트워크 액세스를 위한 Cisco 라우터(HGW/LNS), IP 연결을 지원하는 Cisco 라우터
- 라우터의 호스트 이름 또는 VPDN 그룹에서 사용할 로컬 이름입니다.
- 사용할 터널링 프로토콜입니다.이는 L2T(Layer 2 Tunneling) 프로토콜 또는 L2F(Layer 2 Forwarding) 프로토콜일 수 있습니다.
- 라우터가 터널을 인증하기 위한 비밀번호입니다.
- 터널링 기준입니다.도메인 이름 또는 DNIS(Dialed Number Identification Service)일 수 있습니다.

- 사용자의 사용자 이름 및 암호(클라이언트 전화 걸기)입니다.
- TACACS+ 서버의 IP 주소 및 키

사용되는 구성 요소

이 문서는 특정 소프트웨어 및 하드웨어 버전으로 한정되지 않습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다.이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다.현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 표기 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

배경 정보

VPDN(Virtual Private Dialup Networks) 및 VPDN 그룹에 대한 자세한 개요는 VPDN 이해를 참조하십시오.이 문서는 VDPN 컨피그레이션에서 확장되며 TACACS+(Terminal Access Controller Access Control System Plus)를 추가합니다.

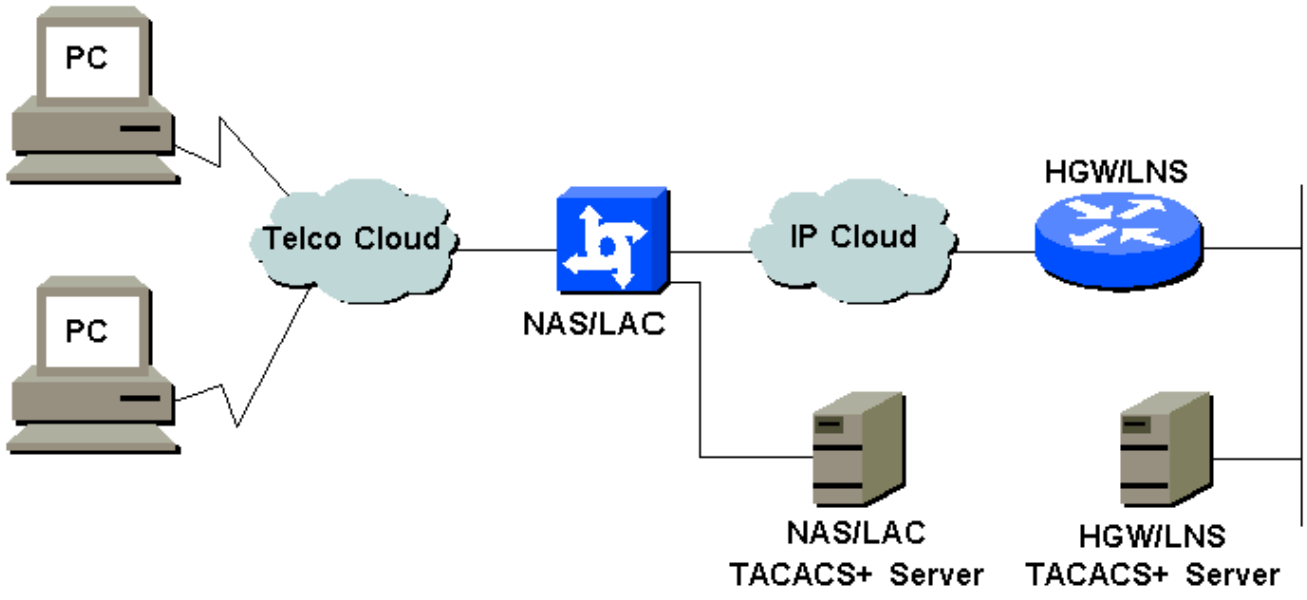
구성

이 섹션에서는 이 문서에 설명된 기능을 구성하는 정보를 제공합니다.

참고: 이 문서에 사용된 명령에 대한 추가 정보를 찾으려면 명령 조회 도구(등록된 고객만 해당)를 사용합니다.

네트워크 다이어그램

이 문서에서는 다음 네트워크 설정을 사용합니다.



구성

이 문서에서는 다음 구성을 사용합니다.

- NAS/LAC
- HGW/LNS
- NAS/LAC TACACS+ 구성 파일
- HGW/LNS TACACS+ 구성 파일

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+ 구성 파일

```
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+ 구성 파일

```
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 { }
      }
```

다음을 확인합니다.

이 섹션에서는 컨피그레이션이 제대로 작동하는지 확인하는 데 사용할 수 있는 정보를 제공합니다.

일부 **show 명령은** 출력 인터프리터 툴 에서 지원되는데(등록된 고객만), 이 툴을 사용하면 **show 명령 출력의 분석 결과를 볼 수 있습니다.**

- **show vpdn tunnel all** - 모든 활성 터널의 세부 정보를 표시합니다.
- **show user**—연결된 사용자의 이름을 표시합니다.
- **show interface virtual-access #**—HGW/LNS에서 특정 가상 인터페이스의 상태를 확인할 수 있습니다.

문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

문제 해결 명령

참고: debug 명령을 실행하기 전에 디버그 명령에 대한 중요 정보를 참조하십시오.

- **debug vpdn l2x-events** - 터널 또는 세션 생성을 위한 NAS/LAC와 HGW/LNS 간의 대화 상자를 표시합니다.
- **debug ppp authentication**—클라이언트가 인증을 통과하는지 확인할 수 있습니다.
- **debug ppp negotiation**—클라이언트가 PPP 협상을 통과하고 있는지 확인할 수 있습니다.어떤 옵션(예: 콜백, MLP 등)과 협상 중인 프로토콜(예: IP, IPX 등)을 확인할 수 있습니다.
- **debug ppp error**—PPP 연결 협상 및 작업과 관련된 프로토콜 오류 및 오류 통계를 표시합니다.
- **debug vtemplate**—HGW/LNS에서 가상 액세스 인터페이스의 복제를 표시합니다.다이얼업 연결 시작 시 인터페이스가 생성된 시점(가상 템플릿에서 복제)과 연결이 종료될 때 인터페이스가 제거되는 시기를 확인할 수 있습니다.
- **debug aaa authentication**—사용자 또는 터널이 AAA(authentication, authorization, and accounting) 서버에서 인증되는지 확인할 수 있습니다.
- **debug aaa authorization**—AAA 서버에서 사용자의 권한을 부여하는지 여부를 확인할 수 있습니다.
- **debug aaa per-user**—인증된 각 사용자에게 적용되는 사항을 확인할 수 있습니다.이는 위에 나열된 일반 디버그와 다릅니다.

관련 정보

- 기술 지원 페이지 - 다이얼
- Technical Support - Cisco Systems