Configuration d'un réseau VPDN initié par accès téléphonique en utilisant des groupes VPDN et TACACS+

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour les réseaux de connexion privée virtuelle d'accès distant (VPDN), utilisant les groupes VPDN et le Terminal Access Controller Access Control System Plus (TACACS+).

Conditions préalables

Conditions requises

Avant de tenter cette configuration, assurez-vous que vous répondez à ces exigences :

Vous devez avoir :

- Un routeur de Cisco pour l'accès client (NAS/LAC), et un routeur de Cisco pour l'accès au réseau (HGW/LNS) avec la connectivité IP entre eux.
- Noms d'hôte des Routeurs, ou locaux names aux utiliser sur les groupes VPDN.
- Le protocole de Tunnellisation à l'utiliser. Ceci peut être ou protocole du Tunnellisation de la couche 2 (L2T), ou posez 2 le protocole (L2F) de transmission.
- Un mot de passe pour que les Routeurs authentifient le tunnel.
- Un critère de Tunnellisation. Ceci a pu être le nom de domaine, ou le Service d'identification

du numéro composé réacheminé (RDNIS).
- Noms d'utilisateur et mots de passe pour l'utilisateur (client se connectant).
- Adresses IP et clés pour vos serveurs TACACS+.

Composants utilisés

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux Conventions relatives aux conseils techniques Cisco.

Informations générales

Pour une introduction détaillée aux réseaux de connexion privée virtuelle (VPDN) et aux groupes VPDN, voir compréhension du VPDN. Ce document examine la configuration VDPN, et ajoute le Terminal Access Controller Access Control System Plus (TACACS+).

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Remarque: Pour obtenir des informations supplémentaires sur les commandes utilisées dans ce document, utilisez l'Outil de recherche de commande (clients enregistrés seulement).

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Configurations

Ce document utilise les configurations suivantes :

- NAS/LAC
- HGW/LNS
- Fichier de config NAS/LAC TACACS+
- Fichier de config 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
```

Fichier de config 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
        }
```

Fichier de config 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 { }
        }
```

Vérifiez

Cette section présente des informations que vous pouvez utiliser pour vous assurer que votre configuration fonctionne correctement.

Certaines commandes **show** sont prises en charge par l'Output Interpreter Tool (clients

enregistrés uniquement), qui vous permet de voir une analyse de la sortie de la commande show.

- **le show vpdn tunnel** affiche **entièrement des** détails de tous les tunnels actifs.
- **utilisateur d'exposition** — affiche le nom d'utilisateur qui est connecté.
- **affichez l'interface virtuel-Access #** — te permet de vérifier le statut d'une interface virtuelle particulière sur le HGW/LNS.

Dépannez

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Dépannage des commandes

Remarque: Avant d'émettre des commandes de **débogage**, référez-vous aux informations importantes sur des commandes de debug.

- **le debug vpdn l2x-events** — affiche le dialogue entre NAS/LAC et HGW/LNS pour la création de tunnel ou de session.
- **debug ppp authentication** — te permet de vérifier si un client passe l'authentification.
- **debug ppp negotiation** — te permet de vérifier si un client passe la négociation PPP. Vous pourriez voir quelles options (comme, rappel, MLP, et ainsi de suite), et quelles protocoles (comme, IP, IPX, et ainsi de suite) sont négocié.
- **debug ppp error** — erreurs de protocole et statistiques sur les erreurs d'affichages, associées avec la négociation de connexion PPP et l'exécution.
- **debug vtemplate** — affiche le clonage des interfaces d'accès virtuelles sur le HGW/LNS. Vous pouvez voir quand l'interface est créée (copié du modèle virtuel) au début de la connexion d'accès par réseau commuté, et quand l'interface est détruite quand la connexion termitated.
- **debug aaa authentication** — te permet de vérifier si l'utilisateur ou le tunnel est authentifié par le serveur d'Authentification, autorisation et comptabilité (AAA).
- **autorisation de debug aaa** — te permet de vérifier si l'utilisateur est autorisé par le serveur d'AAA.
- **debug aaa per-user** — te permet de vérifier ce qui est appliqué à chaque utilisateur qui est authentifié. C'est différent du général met au point énuméré en haut.

Informations connexes

- Pages de support technologique - Cadran
- Support technique - Cisco Systems