Configuration de réseaux VPDN par utilisateur sans informations de domaine ou DNIS

Contenu

Introduction

Ce document fournit une configuration d'échantillon pour le par-utilisateur VPDNs sans domaine ou informations DNIS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Version de logiciel 12.1(4) ou ultérieures de Cisco IOS®.
- Logiciel Cisco IOS version 12.1(4)T ou plus tard.

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

En scénarios de Réseau privé virtuel à accès commuté (VPDN), serveur d'accès à distance (NAS) (un concentrateur d'accès L2TP, ou LAC) établit le tunnel VPDN à la passerelle domestique (LNS) basée sur les informations d'utilisateur-particularité. Ce tunnel VPDN peut être l'expédition du niveau 2 (L2F) ou le Layer 2 Tunneling Protocol (L2TP). Pour déterminer si un utilisateur devrait utiliser un tunnel VPDN, contrôle :

- Si le nom de domaine est inclus en tant qu'élément du nom d'utilisateur. Par exemple, avec le nom d'utilisateur tunnelme@cisco.com, le NAS en avant cet utilisateur au tunnel pour cisco.com.
- Le service d'informations composé de nombre (DNIS). C'est transfert d'appels basé sur le numéro appelé. Ceci signifie que le NAS peut expédier tous les appels avec un numéro appelé particulier au tunnel approprié. Par exemple, si un appel entrant a le numéro appelé 5551111, l'appel peut être expédié au tunnel VPDN, alors qu'un appel à 5552222 n'est pas expédié. Cette caractéristique exige que le réseau de l'opérateur de téléphonie fournit les informations de numéro appelé.

Pour plus d'informations sur la configuration VPDN, voir compréhension du VPDN.

Dans certaines situations, vous pouvez exiger d'un tunnel VPDN d'intiated sur une base de par-nom d'utilisateur, avec ou sans le besoin de domain-name du tout. Par exemple le **ciscouser d'**utilisateur peut être percé un tunnel à **cisco.com**, alors que d'autres utilisateurs peuvent être terminés localement sur le NAS.

Remarque: Ce nom d'utilisateur n'inclut pas l'information de domaines comme dans l'exemple précédent.

La caractéristique de Configuration propre à l'utilisateur VPDN envoie le nom d'utilisateur structuré entier au serveur d'Authentification, autorisation et comptabilité (AAA) la première fois que le routeur contacte le serveur d'AAA. Ceci permet au logiciel de Cisco IOS de personnaliser des attributs de tunnel pour les utilisateurs individuels qui utilisent un nom de domaine ou un DNIS commun.

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

Les seules commandes VPDN nécessaires sur le NAS (LAC) pour prendre en charge le par-utilisateur VPDNs sont le **vpdn enable de** commandes de configuration globale et **pour le vpdn authen-before-forward**. La commande de **vpdn authen-before-forward** demande au NAS (LAC) d'authentifier le nom d'utilisateur complet avant qu'elle prenne une décision d'expédition. Un tunnel VPDN est alors établi, basé sur les informations renvoyées par le serveur d'AAA pour cet utilisateur individuel ; si aucune informations VPDN n'est renvoyée du serveur d'AAA, l'utilisateur est terminé localement. La configuration dans cette section affiche les commandes exigées pour prendre en charge des tunnels sans information de domaines dans le nom d'utilisateur.

Remarque: Cette configuration n'est pas complète. Seulement les VPDN, l'interface et les commandes appropriés d'AAA sont inclus.

Remarque: Il est hors de portée de ce document pour discuter chaque protocole et protocole AAA possibles de tunnel. Par conséquent, cette configuration implémente un tunnel L2TP avec le serveur d'AAA RADIUS. Adaptez les principes et la configuration discutés ici pour configurer d'autres types ou protocoles AAA de tunnel.

Ce document utilise la configuration suivante :

- NAS VPDN (LAC)

NAS VPDN (LAC)

```
aaa new-model
aaa authentication ppp default group radius
!--- Use RADIUS authentication for PPP authentication.
aaa authorization network default group radius !---
Obtain authorization information from the Radius server.
!--- This command is required for the AAA server to
provide VPDN attributes. ! vpdn enable !--- VPDN is
enabled. vpdn authen-before-forward !--- Authenticate
the complete username before making a forwarding
decision. !--- The LAC sends the username to the AAA
server for VPDN attributes. ! controller E1 0 pri-group
timeslots 1-31 ! interface Serial0:15 dialer rotary-
group 1 !--- D-channel for E1 0 is a member of the
dialer rotary group 1. ! interface Dialer1 !--- Logical
interface for dialer rotary group 1. ip unnumbered
Ethernet0 encapsulation ppp dialer in-band dialer-group
1 ppp authentication chap pap callin ! radius-server
host 172.22.53.201 !--- The IP address of the RADIUS
server host. !--- This AAA server will supply the
NAS(LAC) with the VPDN attributes for the user. radius-
server key cisco !--- The RADIUS server key.
```

Configuration du serveur RADIUS

Voici quelques configurations utilisateur sur un Cisco Secure pour le serveur de RAYON d'Unix (CSU) :

1. Un utilisateur qui doit être terminé localement sur le NAS : `user1 Password = "cisco" Service-Type = Framed-User`
2. Un utilisateur pour qui une session VPDN devrait être établie :`user2 Password = "cisco"`

```
Service-Type = Framed-User,
Cisco-AVPair = "vpdn:ip-addresses=172.22.53.141",
Cisco-AVPair = "vpdn:l2tp-tunnel-password=cisco",
Cisco-AVPair = "vpdn:tunnel-type=l2tp"
```

Le NAS (LAC) utilise les attributs spécifiés avec Cisco-AVPair VPDN pour initier le tunnel VPDN à la passerelle domestique. Assurez-vous que vous configurez la passerelle domestique pour recevoir des tunnels VPDN du NAS.

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.

- **utilisateur de show caller** — paramètres d'expositions pour un utilisateur particulier, tel que l'interface utilisée et asynchrone de ligne TTY (module, emplacement ou port), le numéro de canal DS0, numéro de modem, adresse IP assignée, paramètres d'ensemble de PPP et de PPP, et ainsi de suite. Si votre version de logiciel de Cisco IOS ne prend en charge pas cette commande, utilisez l'ordre d'**utilisateur d'exposition**.
- **show vpdn** — affiche des informations au sujet de L2F actif et tunnels et identificateurs de message de protocole L2TP dans un VPDN.

Exemple de sortie de la commande show

Quand l'appel connecte l'utilisation la commande de *nom d'utilisateur d'***utilisateur de show caller** aussi bien que la commande de **show vpdn** de vérifier que l'appel est réussi. Un résultat témoin est affiché ci-dessous :

```
maui-nas-02#show caller user vpdn_authen User: vpdn_authen, line tty 12, service Async Active
time 00:09:01, Idle time 00:00:05 Timeouts: Absolute Idle Idle Session Exec Limits: - - 00:10:00
Disconnect in: - - - TTY: Line 12, running PPP on As12 DS0: (slot/unit/channel)=0/0/5 Line: Baud
rate (TX/RX) is 115200/115200, no parity, 1 stopbits, 8 databits Status: Ready, Active, No Exit
Banner, Async Interface Active HW PPP Support Active Capabilities: Hardware Flowcontrol In,
Hardware Flowcontrol Out Modem Callout, Modem RI is CD, Line is permanent async interface,
Integrated Modem Modem State: Ready User: vpdn_authen, line As12, service PPP Active time
00:08:58, Idle time 00:00:05 Timeouts: Absolute Idle Limits: - - Disconnect in: - - PPP: LCP
Open, CHAP (<- AAA) IP: Local 172.22.53.140 VPDN: NAS , MID 4, MID Unknown HGW , NAS CLID 0, HGW
CLID 0, tunnel open !--- The VPDN tunnel is open. Counts: 85 packets input, 2642 bytes, 0 no
buffer 0 input errors, 0 CRC, 0 frame, 0 overrun 71 packets output, 1577 bytes, 0 underruns 0
output errors, 0 collisions, 0 interface resets maui-nas-02#show vpdn L2TP Tunnel and Session
Information Total tunnels 1 sessions 1 LocID RemID Remote Name State Remote Address Port
Sessions 6318 3 HGW est 172.22.53.141 1701 1 LocID RemID TunID Intf Username State Last Chg
Fastswitch 4 3 6318 As12 vpdn_authen est 00:09:33 enabled !--- The tunnel for user vpdn_authen
is in established state. %No active L2F tunnels %No active PPTP tunnels %No active PPPoE tunnel
```

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 ppp authentication** — des messages du protocole d'authentification de PPP d'affichages, et inclut des échanges de paquet de protocole d'authentification CHAP (Challenge Handshake Authentication Protocol) et des échanges de Password Authentication Protocol (PAP).
- **debug aaa authentication** — affiche des informations sur l'authentification AAA/RADIUS.
- **autorisation de debug aaa** — affiche des informations sur l'autorisation AAA/RADIUS.
- **debug radius** — les informations de débogage détaillées d'affichages associées avec le RAYON. Utilisez l'Output Interpreter Tool (clients enregistrés seulement) pour décoder les messages de debug radius. Par exemple, référez-vous à la section d'**exemple de sortie de débogage**. Employez les informations du **debug radius** pour déterminer quels attributs sont négociés.
- **debug tacacs** — les informations de débogage détaillées d'affichages associées avec le TACACS+.
- **événement de debug vpdn** — erreurs et événements des affichages L2x qui sont une partie de l'établissement normal d'un tunnel ou un arrêt pour VPDNs.
- **erreur de debug vpdn** — erreurs de protocole des affichages VPDN.
- **le debug vpdn l2x-event** — des affichages a détaillé les erreurs et les événements L2x qui sont une partie de l'établissement normal d'un tunnel ou un arrêt pour VPDNs.
- **debug vpdn l2x-error** — erreurs de protocole des affichages VPDN L2x.

Exemple de sortie de débogage

Voici la **sortie de débogage** pour un appel réussi. Dans cet exemple, notez que le NAS obtient les attributs pour le tunnel VPDN du serveur de rayon.

```
maui-nas-02#show debug General OS: AAA Authentication debugging is on AAA Authorization
debugging is on PPP: PPP authentication debugging is on VPN: L2X protocol events debugging is on
L2X protocol errors debugging is on VPDN events debugging is on VPDN errors debugging is
onRadius protocol debugging is on maui-nas-02# *Jan 21 19:07:26.752: %ISDN-6-CONNECT: Interface
Serial0:5 is now connected to N/A N/A !--- Incoming call. *Jan 21 19:07:55.352: %LINK-3-UPDOWN:
Interface Async12, changed state to up *Jan 21 19:07:55.352: As12 PPP: Treating connection as a
dedicated line *Jan 21 19:07:55.352: As12 AAA/AUTHOR/FSM: (0): LCP succeeds trivially *Jan 21
19:07:55.604: As12 CHAP: O CHALLENGE id 1 len 32 from "maui-nas-02" *Jan 21 19:07:55.732: As12
CHAP: I RESPONSE id 1 len 32 from "vpdn_authen" !--- Incoming CHAP response from user
vpdn_authen. *Jan 21 19:07:55.732: AAA: parse name=Async12 idb type=10 tty=12 *Jan 21
19:07:55.732: AAA: name=Async12 flags=0x11 type=4 shelf=0 slot=0 adapter=0 port=12 channel=0
*Jan 21 19:07:55.732: AAA: parse name=Serial0:5 idb type=12 tty=-1 *Jan 21 19:07:55.732: AAA:
name=Serial0:5 flags=0x51 type=1 shelf=0 slot=0 adapter=0 port=0 channel=5 *Jan 21 19:07:55.732:
AAA/ACCT/DS0: channel=5, ds1=0, t3=0, slot=0, ds0=5 *Jan 21 19:07:55.732: AAA/MEMORY:
create_user (0x628C79EC) user='vpdn_authen' ruser='' port='Async12' rem_addr='async/81560'
authen_type=CHAP service=PPP priv=1 *Jan 21 19:07:55.732: AAA/AUTHEN/START (4048817807):
port='Async12' list='' action=LOGIN service=PPP *Jan 21 19:07:55.732: AAA/AUTHEN/START
(4048817807): using "default" list *Jan 21 19:07:55.732: AAA/AUTHEN/START (4048817807):
Method=radius (radius) *Jan 21 19:07:55.736: RADIUS: ustruct sharecount=1 *Jan 21 19:07:55.736:
RADIUS: Initial Transmit Async12 id 6 172.22.53.201:1645, Access-Request, len 89 *Jan 21
19:07:55.736: Attribute 4 6 AC16358C *Jan 21 19:07:55.736: Attribute 5 6 0000000C *Jan 21
19:07:55.736: Attribute 61 6 00000000 *Jan 21 19:07:55.736: Attribute 1 13 7670646E *Jan 21
19:07:55.736: Attribute 30 7 38313536 *Jan 21 19:07:55.736: Attribute 3 19 014CF9D6 *Jan 21
19:07:55.736: Attribute 6 6 00000002 *Jan 21 19:07:55.736: Attribute 7 6 00000001 *Jan 21
```

19:07:55.740: RADIUS: Received from id 6 172.22.53.201:1645, Access-Accept, len 136 *Jan 21 19:07:55.740: Attribute 6 6 00000002 *Jan 21 19:07:55.740: Attribute 26 40 0000000901227670 *Jan 21 19:07:55.740: Attribute 26 40 0000000901227670 *Jan 21 19:07:55.740: Attribute 26 30 0000000901187670

Les paires de valeurs d'attribut (AVPs) nécessaires pour le tunnel VPDN sont abaissées du serveur de RAYON. Cependant, le **debug radius** produit un résultat codé indiquant l'AVPs et leurs valeurs. Vous pouvez coller le résultat présenté dans la police **grasse** ci-dessus dans l'Output Interpreter Tool (clients enregistrés seulement). La sortie suivante en gras est la sortie décodée obtenue de l'outil :

Access-Request 172.22.53.201:1645 id 6 Attribute Type 4: NAS-IP-Address is 172.22.53.140 Attribute Type 5: NAS-Port is 12 Attribute Type 61: NAS-Port-Type is Asynchronous Attribute Type 1: User-Name is vpdn Attribute Type 30: Called-Station-ID(DNIS) is 8156 Attribute Type 3: CHAP-Password is (encoded) Attribute Type 6: Service-Type is Framed Attribute Type 7: Framed-Protocol is PPP Access-Accept 172.22.53.201:1645 id 6 Attribute Type 6: Service-Type is Framed Attribute Type 26: Vendor is Cisco Attribute Type 26: Vendor is Cisco Attribute Type 26: Vendor is Cisco
*Jan 21 19:07:55.740: AAA/AUTHEN (4048817807): status = PASS ... ... *Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:ip-addresses=172.22.53.141" *Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:l2tp-tunnel-password=cisco" *Jan 21 19:07:55.744: RADIUS: cisco AVPair "vpdn:tunnel-type=l2tp" *Jan 21 19:07:55.744: AAA/AUTHOR (733932081): Post authorization status = PASS_REPL *Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV service=ppp *Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV ip-addresses=172.22.53.141 *Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV l2tp-tunnel-password=cisco *Jan 21 19:07:55.744: AAA/AUTHOR/VPDN: Processing AV tunnel-type=l2tp *!--- Tunnel information. !--- The VPDN Tunnel will now be established and the call will be authenticated. !--- Since the debug information is similar to that for a normal VPDN call, !--- the VPDN tunnel establishment debug output is omitted.*

Informations connexes

- Présentation de VPDN
- Configurer des réseaux de connexion privée virtuelle
- Le Comment-Faire configurent l'authentification de Protocol de tunnel de la couche 2 avec le RAYON
- Le Comment-Faire configurent l'authentification de Protocol de tunnel de la couche 2 avec TACACS+
- Accès aux pages d'assistance technologique
- Support technique - Cisco Systems