Présentation de VPDN

Contenu

Introduction

Un réseau privé virtuel à accès commuté (VPDN) permet à un réseau privé en service de se répartir sur des serveurs à accès distant (définis comme concentrateur L2TP Access [LAC]).

Quand un client de Protocole point à point (PPP) introduit dans un LAC, le LAC détermine qu'il devrait expédier cette session PPP en fonction à un serveur de réseau L2TP (LNS) pour ce client. Le LNS alors authentifie l'utilisateur et commence la négociation PPP. Une fois que l'installation de PPP s'est terminée, toutes les trames sont envoyées par le LAC au client et au LNS.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

Pour plus d'informations sur les conventions de documents, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Glossaire

- **Client** : Le PC ou le routeur s'est relié à un réseau d'Accès à distance, qui est le demandeur d'un appel.
- **L2TP** : Tunnel Protocol de la couche 2. Le PPP définit un mécanisme d'encapsulation pour transporter les paquets multiprotocoles à travers les liens point par point de la couche 2 (L2). Typiquement, un utilisateur obtient une connexion L2 à un serveur d'accès à distance (NAS) utilisant une technique telle que le réseau téléphonique public commuté commuté (POTS), le RNIS ou le Ligne d'abonné numérique à débit asymétrique (ADSL). L'utilisateur exécute alors le PPP au-dessus de cette connexion. Dans une telle configuration, le point d'arrêt L2 et le point final de session PPP résident sur le même périphérique physique (le NAS).L2TP étend le modèle de PPP en permettant aux points finaux L2 et de PPP pour résider sur des différents périphériques interconnectés par un réseau. Avec L2TP, l'utilisateur a une connexion L2 à un concentrateur d'accès, et le concentrateur perce un tunnel alors différentes trames PPP au NAS. Ceci permet le traitement réel des paquets PPP à divorcer de l'arrêt du circuit L2.
- **L2F** : Protocole de transfert de couche 2. L2F est un protocole de Tunnellisation plus ancien que L2TP.
- **LAC** : Concentrateur L2TP Access. Un noeud qui agit en tant qu'un côté d'un point final de tunnel L2TP et est un pair au LNS. Le LAC se repose entre un LNS et un client et en avant les paquets à et de chacun. Les paquets envoyés du LAC au LNS exigent le Tunnellisation avec le protocole L2TP. La connexion du LAC au client est typiquement par le RNIS ou l'analogue.
- **LNS** : Serveur de réseau L2TP. Un noeud qui agit en tant qu'un côté d'un point final de tunnel L2TP et est un pair au LAC. Le LNS est le point d'arrêt logique d'une session PPP qui est percée un tunnel du client par le LAC.
- **Passerelle domestique** : La même définition que le LNS en terminologie L2F.
- **NAS** : La même définition que le LAC en terminologie L2F.
- **Tunnel** : En terminologie L2TP, un tunnel existe entre une paire LAC-LNS. Le tunnel se compose d'une connexion de contrôle et zéro sessions ou plus L2TP. Le tunnel diffuse les datagrammes de PPP et les messages encapsulés de contrôle entre le LAC et le LNS. Le processus est identique pour L2F.
- **Session** : L2TP est connecté. Le LNS et le LAC mettent à jour un état pour chaque appel qui est initié ou répondu par un LAC. Une session L2TP est créée entre le LAC et le LNS quand une connexion PPP de bout en bout est établie entre un client et le LNS. Des datagrammes liés à la connexion PPP sont envoyés au-dessus du tunnel entre le LAC et le LNS. Il y a des relations linéaires entre les sessions établies L2TP et leurs appels associés. Le processus est identique pour L2F.

Aperçu du processus VPDN

Dans la description du processus VPDN ci-dessous, nous utilisons la terminologie L2TP (LAC et LNS).

1. Le client appelle le LAC (typiquement utilisant un modem ou une carte RNIS).

2. Le client et le LAC commence la phase de PPP par négocier les options LCP (méthode d'authentification protocole d'identification de mot de passe [PAP] ou authentification Protocol à échanges confirmés [CHAP], ppp multilink, compactage, et ainsi de suite).
3. Supposons que le CHAP a été négocié dans l'étape 2. Le LAC envoie un défi de CHAP au client.
4. Le LAC obtient une réponse (par exemple username@DomainName et mot de passe).
5. Basé sur le nom de domaine reçu à la réponse de CHAP ou au service d'informations composé de nombre (DNIS) reçu dans le message de configuration RNIS, les contrôles de LAC si le client est un utilisateur VPDN. Il fait ceci à l'aide de sa configuration ou de contacter des gens du pays VPDN un serveur d'Authentification, autorisation et comptabilité (AAA).
6. Puisque le client est un utilisateur VPDN, le LAC obtient quelques informations (de sa configuration de gens du pays VPDN ou d'un serveur d'AAA) ces il l'utilise pour apporter un tunnel L2TP ou L2F avec le LNS.
7. Le LAC apporte un tunnel L2TP ou L2F avec le LNS.
8. Basé sur le nom reçu dans la demande du LAC, le LNS vérifie si le LAC est permis pour ouvrir un tunnel (le LNS vérifie sa configuration des gens du pays VPDN). D'ailleurs, le LAC et le LNS s'authentifient (ils utilisent leur base de données locale ou contactent un serveur d'AAA). Le tunnel est alors entre les deux périphériques. Dans ce tunnel, plusieurs sessions VPDN peuvent être portées.
9. Pour le client username@DomainName, une session VPDN est déclenchée du LAC au LNS. Il y a une session VPDN par client.
10. Le LAC en avant les options LCP qu'il a négociées au LNS avec le client avec username@DomainName et le mot de passe reçus du client.
11. Le LNS copie virtuel-Access d'un virtual-template spécifié dans la configuration VPDN. Le LNS prend les options LCP reçues du LAC et authentifie le client localement ou en contactant le serveur d'AAA.
12. Le LNS envoie une réponse de CHAP au client.
13. La phase du protocole de contrôle IP (IPCP) est exécutée et alors l'artère est installée : la session PPP est en service entre le client et le LNS. Le LAC juste en avant les trames PPP. Les trames PPP sont percées un tunnel entre le LAC et le LNS.

Protocoles de perçage d'un tunnel

Un tunnel VPDN peut être construit utilisant l'expédition Layer-2 (L2F) ou le Layer 2 Tunneling Protocol (L2TP).

- L2F a été introduit par Cisco dans le Request For Comments (RFC) 2341 et est également utilisé pour expédier des sessions PPP pour le PPP de Multichassis Multilink.
- L2TP, introduit dans RFC 2661, combine le meilleur du protocole L2F de Cisco et du Protocole PPTP (Point-to-Point Tunneling Protocol) de Microsoft. D'ailleurs, L2F prend en charge seulement l'accès distant VPDN tandis que L2TP prend en charge l'accès distant et la connexion VPDN.

Les deux protocoles emploient le port UDP 1701 pour construire un tunnel par un réseau IP pour expédier des trames de couche de liaison. Pour L2TP, l'installation pour percer un tunnel une session PPP se compose de deux étapes :

1. Établissement d'un tunnel entre le LAC et le LNS. Cette phase a lieu seulement quand il n'y

a aucun tunnel actif entre les deux périphériques.
2. Établissement d'une session entre le LAC et le LNS.

Le LAC décide qu'un tunnel doit être initié du LAC au LNS.

1. Le LAC envoie une Commencement-Contrôle-Connexion-demande (SCCRQ). Un défi et des paires AV de CHAP sont inclus dans ce message.
2. Le LNS répond avec une Commencement-Contrôle-Connexion-réponse (SCCRP). Un défi de CHAP, la réponse au défi du LAC et des paires AV sont inclus dans ce message.
3. Le LAC envoie Commencement-Contrôle-Connexion-connecté (SCCCN). La réponse de CHAP est incluse dans ce message.
4. Le LNS répond avec un accusé de réception de corps de Zéro-longueur (ZLB ACK). Cet accusé de réception peut être porté dedans un autre message. Le tunnel est.
5. Le LAC envoie une Entrant-Appel-demande (ICRQ) au LNS.
6. Le LNS répond avec un message de l'Entrant-Appel-réponse (l'ICRP).
7. Le LAC envoie Entrant-Appel-connecté (ICCN).
8. Le LNS répond de retour avec un ZLB ACK. Cet accusé de réception peut également être porté dedans un autre message.
9. La session est en hausse.

Remarque: Ce qui précède de messages utilisés pour ouvrir un tunnel ou une session portent des paires de valeurs d'attribut (AVPs) définies dans RFC 2661. Ils décrivent des propriétés et des informations (telles que Bearercap, adresse Internet, nom de constructeur et taille de la fenêtre). Quelques paires AV sont obligatoires et d'autres sont facultatives.

Remarque: Un ID de tunnel est utilisé pour multiplexer et démultiplexer des tunnels entre le LAC et le LNS. Un ID de session est utilisé pour identifier une session particulière avec le tunnel.

Pour L2F, l'installation pour percer un tunnel une session PPP est identique que pour L2TP. Il implique :

1. Établissement d'un tunnel entre le NAS et la passerelle domestique. Cette phase a lieu seulement quand il n'y a aucun tunnel actif entre les deux périphériques.
2. Établissement d'une session entre le NAS et la passerelle domestique.

Le NAS décide qu'un tunnel doit être initié du NAS à la passerelle domestique.

1. Le NAS envoie un L2F_Conf à la passerelle domestique. Un défi de CHAP est inclus dans ce message.
2. La passerelle domestique répond avec un L2F_Conf. Un défi de CHAP est inclus dans ce message.
3. Le NAS envoie un L2F_Open. La réponse de CHAP du défi de passerelle domestique est incluse dans ce message.
4. La passerelle domestique répond avec un L2F_Open. La réponse de CHAP du défi de NAS est incluse dans ce message. Le tunnel est.
5. Le NAS envoie un L2F_Open à la passerelle domestique. Le paquet inclut le nom d'utilisateur du client (client_name), du défi de CHAP envoyé par le NAS au client (challenge_NAS) et de sa réponse (response_client).
6. La passerelle domestique, par l'envoi soutiennent le L2F_OPEN, reçoit le client. Le trafic est maintenant libre d'entrer dans l'un ou l'autre de direction entre le client et la passerelle domestique.

Remarque: Un tunnel est identifié avec un CLID (ID de client). L'ID multiplex (MID) identifie une

connexion particulière dans le tunnel.

Configurer VPDN

Pour les informations sur configurer VPDN, référez-vous au manuel configurant de réseaux privés virtuels, et allez à la section sur configurer le VPN.

Informations connexes

- Pages de support technologique de Composition et accès
- Support et documentation techniques - Cisco Systems