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]).

Lorsqu'un client PPP (Point-to-Point Protocol) compose un numéro d'appel dans un LAC, le LAC détermine qu'il doit transférer cette session PPP sur un serveur réseau L2TP (LNS) pour ce client. Le LNS authentifie ensuite l'utilisateur et lance la négociation PPP. Une fois la configuration PPP terminée, toutes les trames sont envoyées au client et au LNS par l'intermédiaire du LAC.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

Conventions

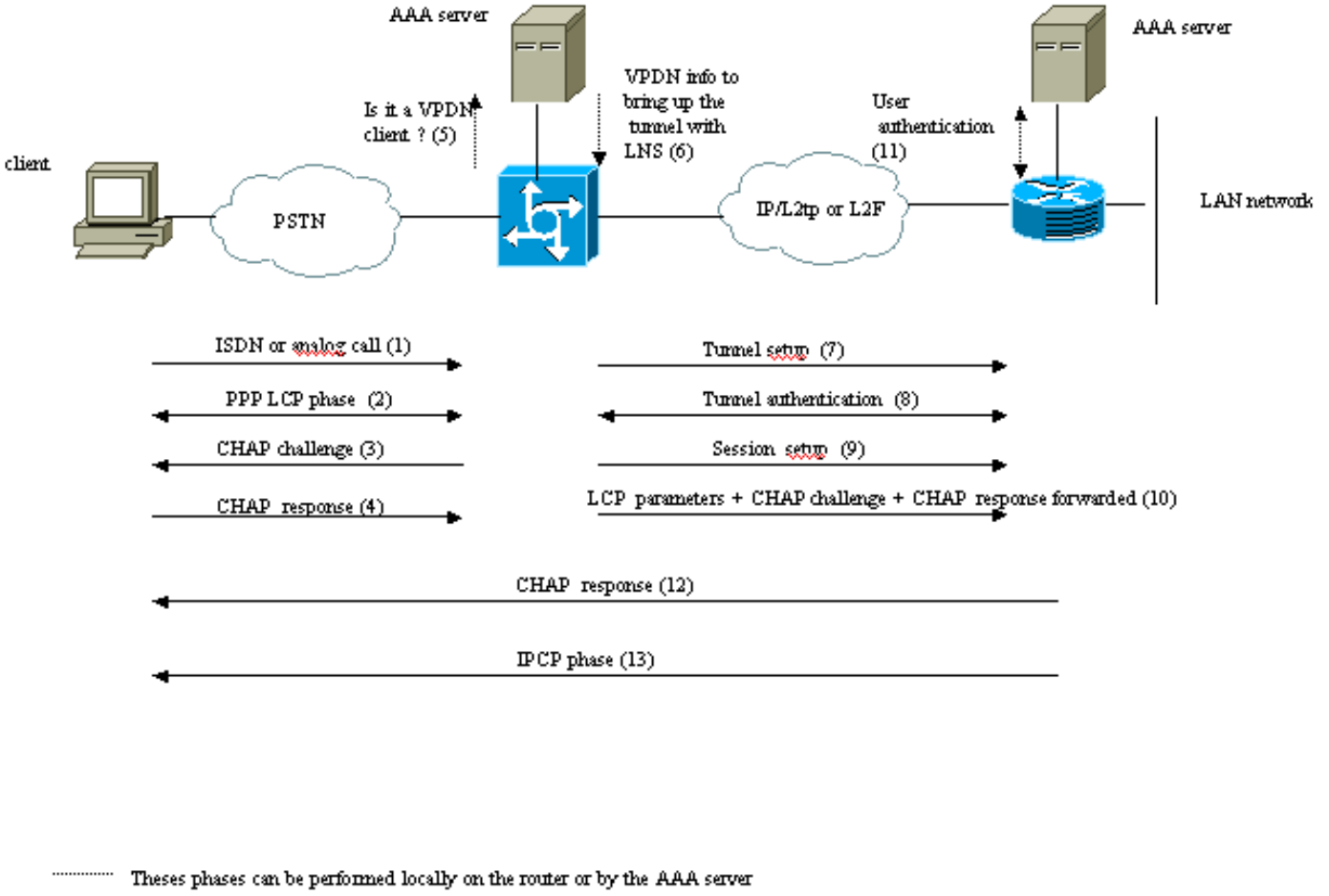
For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Glossaire

- **Client :** PC ou routeur connecté à un réseau d'accès distant, qui est l'initiateur d'un appel.
- **L2TP** : Protocole de tunnel de couche 2. Le protocole PPP définit un mécanisme d'encapsulation pour le transport de paquets multiprotocoles sur des liaisons point à point de couche 2 (L2). En règle générale, un utilisateur obtient une connexion L2 à un serveur d'accès réseau (NAS) à l'aide d'une technique telle que POTS (service téléphonique ordinaire commuté), RNIS ou ADSL (Asymmetric Digital Subscriber Line). L'utilisateur exécute ensuite PPP sur cette connexion. Dans une telle configuration, le point de terminaison L2 et le point de terminaison de session PPP résident sur le même périphérique physique (le NAS).L2TP étend le modèle PPP en permettant aux terminaux L2 et PPP de résider sur différents périphériques interconnectés par un réseau. Avec L2TP, l'utilisateur dispose d'une connexion L2 à un concentrateur d'accès, et le concentrateur effectue ensuite un tunnel de trames PPP individuelles vers le NAS. Cela permet de séparer le traitement réel des paquets PPP de la terminaison du circuit L2.
- **L2F** : Protocole de transfert de couche 2. L2F est un protocole de tunnellisation plus ancien que L2TP.
- **BAC** : Concentrateur d'accès L2TP. Noeud qui agit comme un côté d'un point de terminaison de tunnel L2TP et qui est homologue au LNS. Le LAC se situe entre un LNS et un client et transfère les paquets à destination et en provenance de chacun. Les paquets envoyés par le LAC au LNS nécessitent une transmission tunnel avec le protocole L2TP. La connexion entre le LAC et le client s'effectue généralement par le biais d'un RNIS ou d'une connexion analogique.
- **LNS** : Serveur réseau L2TP. Noeud qui agit comme un côté d'un point de terminaison de tunnel L2TP et qui est homologue du LAC. Le LNS est le point de terminaison logique d'une session PPP qui est tunnelisée à partir du client par le LAC.
- **Passerelle domestique** : Même définition que LNS dans la terminologie L2F.
- **NAS** : Même définition que BAC dans la terminologie L2F.
- **Tunnel:** Dans la terminologie L2TP, il existe un tunnel entre une paire LAC-LNS. Le tunnel se compose d'une connexion de contrôle et de zéro ou plusieurs sessions L2TP. Le tunnel transporte des datagrammes PPP encapsulés et des messages de contrôle entre le LAC et le LNS. Le processus est le même pour L2F.
- **Session** : L2TP est orienté connexion. Le LNS et le LAC conservent un état pour chaque appel initié ou répondu par un LAC. Une session L2TP est créée entre le LAC et le LNS lorsqu'une connexion PPP de bout en bout est établie entre un client et le LNS. Les datagrammes liés à la connexion PPP sont envoyés via le tunnel entre LAC et LNS. Il existe une relation un-à-un entre les sessions L2TP établies et leurs appels associés. Le processus est le même pour L2F.

Présentation 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 (généralement à l'aide d'un modem ou d'une carte RNIS).
2. Le client et le LAC démarrent la phase PPP en négociant les options LCP (méthode d'authentification PAP [Password Authentication Protocol] ou CHAP [Challenge Handshake Authentication Protocol], multiliaison PPP, compression, etc.).
3. Supposons que le protocole CHAP ait été négocié à l'étape 2. Le BAC envoie un défi CHAP au client.
4. Le BAC reçoit une réponse (par exemple username@DomainName et mot de passe).
5. En fonction du nom de domaine reçu dans la réponse CHAP ou du service d'information sur le numéro composé (DNIS) reçu dans le message de configuration RNIS, le LAC vérifie si le client est un utilisateur VPDN. Pour ce faire, il utilise sa configuration VPDN locale ou contacte un serveur AAA (Authentication, Authorization, and Accounting).
6. Comme le client est un utilisateur VPDN, le LAC obtient certaines informations (de sa configuration VPDN locale ou d'un serveur AAA) qu'il utilise pour activer un tunnel L2TP ou L2F avec le LNS.
7. Le LAC ouvre un tunnel L2TP ou L2F avec le LNS.
8. En fonction du nom reçu dans la demande du LAC, le LNS vérifie si le LAC est autorisé à ouvrir un tunnel (le LNS vérifie sa configuration VPDN locale). De plus, le LAC et le LNS s'authentifient mutuellement (ils utilisent leur base de données locale ou communiquent avec un serveur AAA). Le tunnel est alors activé entre les deux périphériques. Dans ce tunnel, plusieurs sessions VPDN peuvent être transportées.
9. Pour le client username@DomainName, une session VPDN est déclenchée du LAC au LNS. Il existe une session VPDN par client.
10. Le LAC transmet les options LCP qu'il a négociées au LNS avec le client, ainsi que le username@DomainName et le mot de passe reçus du client.

11. Le LNS clone un accès virtuel à partir d'un modèle virtuel spécifié dans la configuration VPDN. Le LNS prend les options LCP reçues du LAC et authentifie le client localement ou en contactant le serveur AAA.
12. Le LNS envoie une réponse CHAP au client.
13. La phase IP Control Protocol (IPCP) est exécutée, puis la route est installée : la session PPP est opérationnelle entre le client et le LNS. Le LAC transfère juste les trames PPP. Les trames PPP sont tunnellisées entre le LAC et le LNS.

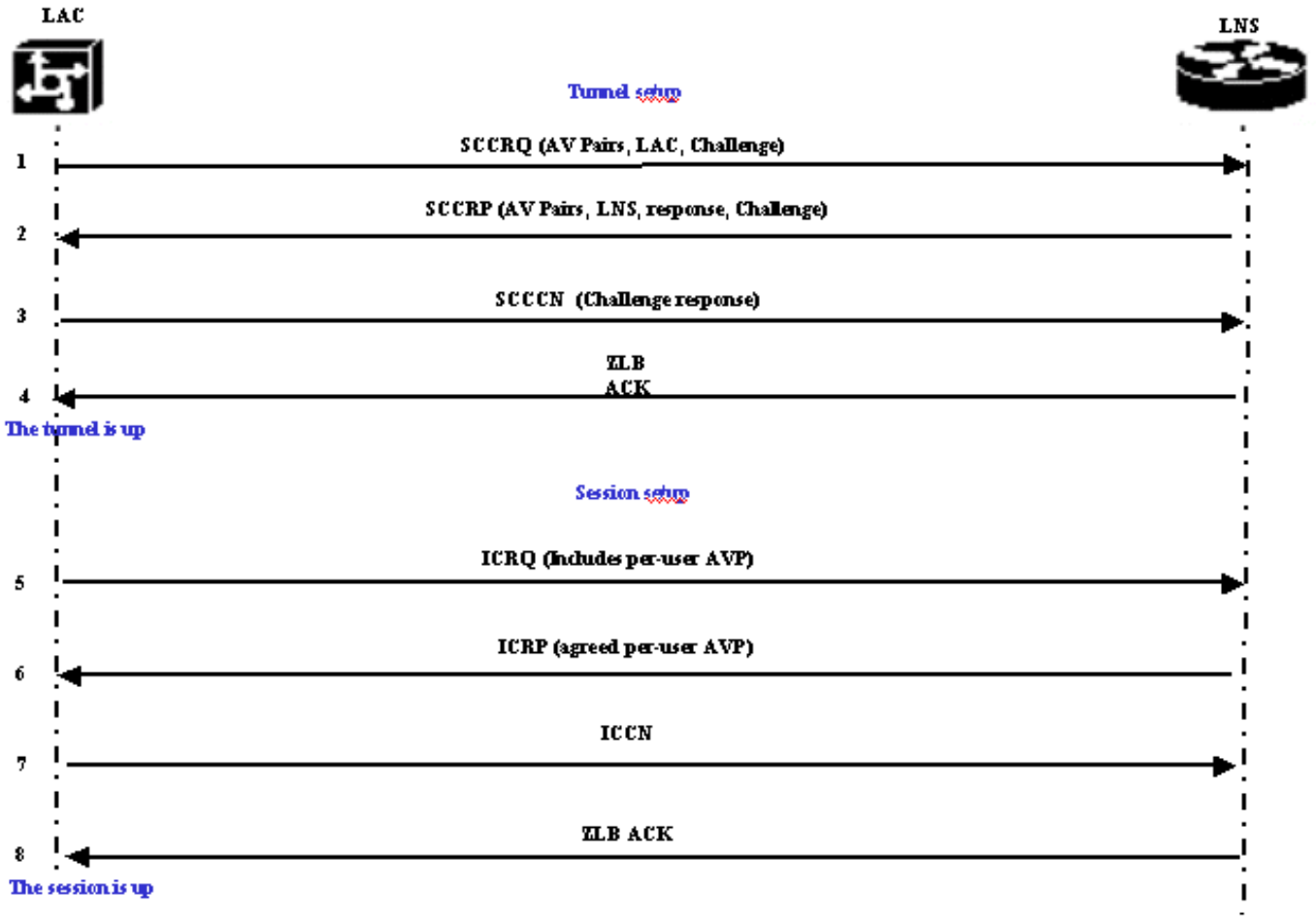
Protocoles de tunnellisation

Un tunnel VPDN peut être construit à l'aide du protocole L2F (Layer-2 Forwarding) ou L2TP (Layer-2 Tunneling Protocol).

- L2F a été introduit par Cisco dans le document RFC (Request For Comments) 2341 et est également utilisé pour transférer des sessions PPP pour Multichassis Multilink PPP.
- L2TP, introduit dans la RFC 2661, combine le meilleur du protocole L2F de Cisco et le protocole PPTP (Microsoft Point-to-Point Tunneling Protocol). De plus, L2F prend uniquement en charge le VPDN commuté entrant tandis que L2TP prend en charge le VPDN commuté entrant et sortant.

Les deux protocoles utilisent le port UDP 1701 pour construire un tunnel via un réseau IP afin de transmettre les trames de couche liaison. Pour L2TP, la configuration de la transmission tunnel d’une session PPP se compose de deux étapes :

1. Établissement d'un tunnel entre le LAC et le LNS. Cette phase se produit uniquement lorsqu'il n'y a pas de tunnel actif entre les deux périphériques.
2. Établissement d’une session entre le BAC et le SNL.



Le BAC décide qu'un tunnel doit être initié entre le BAC et le LNS.

1. Le LAC envoie une requête Start-Control-Connection (SCCRQ). Un défi CHAP et des paires AV sont inclus dans ce message.
2. Le LNS répond par un SCCRP (Start-Control-Connection-Reply). Ce message comprend un défi du CHAP, la réponse au défi de BAC et les paires AV.
3. Le LAC envoie un SCCCN (Start-Control-Connection-Connected). La réponse CHAP est incluse dans ce message.
4. Le LNS répond par un accusé de réception de corps de longueur zéro (ZLB ACK). Cet accusé de réception peut être transmis dans un autre message. Le tunnel est en service.
5. Le LAC envoie une requête d'appel entrant (ICRQ) au LNS.
6. Le LNS répond par un message ICRP (Incoming-Call-Reply).
7. Le LAC envoie un appel entrant connecté (ICCN).
8. Le LNS répond par un ACK ZLB. Cet accusé de réception peut également figurer dans un autre message.
9. La session est terminée.

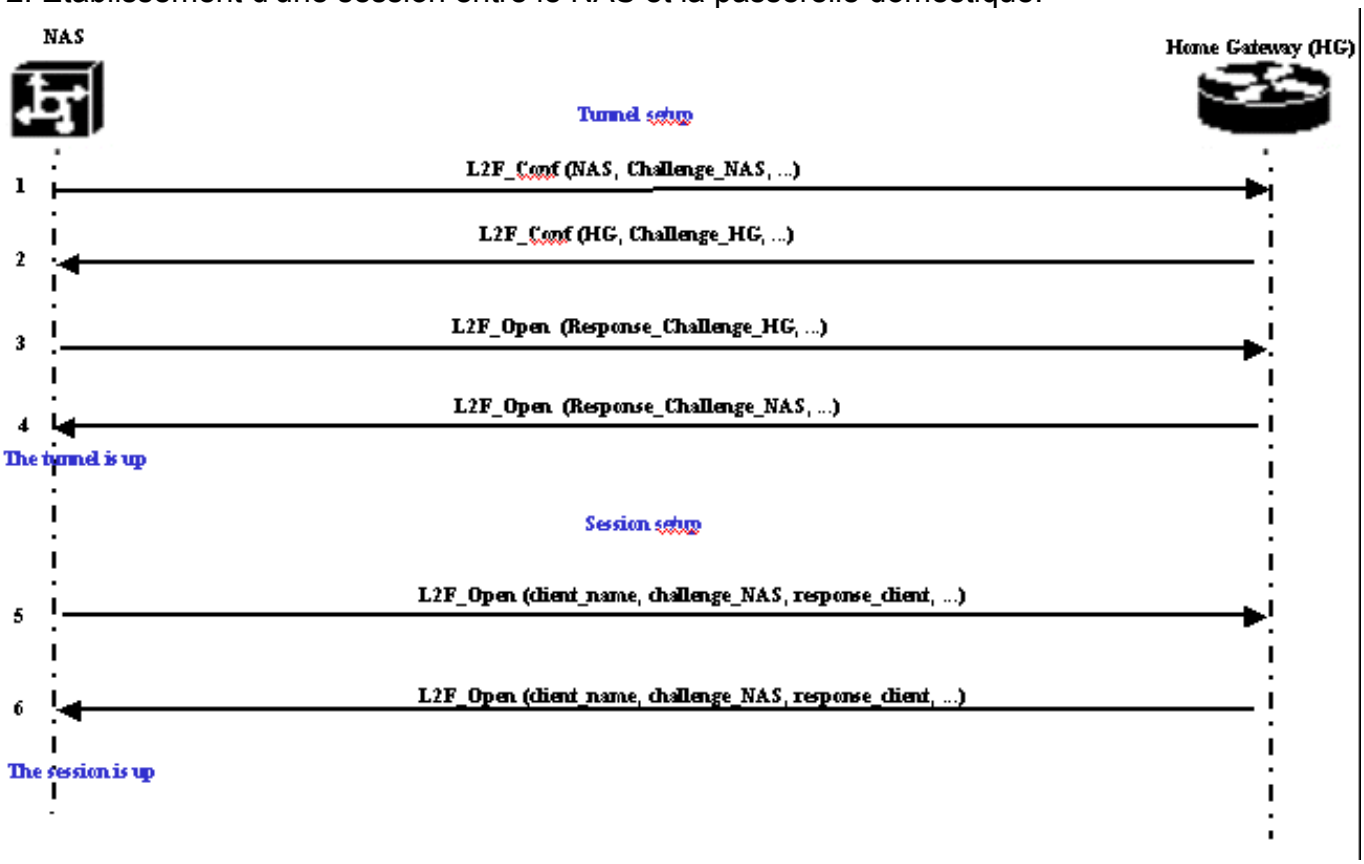
Remarque : Les messages ci-dessus utilisés pour ouvrir un tunnel ou une session portent des paires de valeurs d'attribut (AVP) définies dans la RFC 2661. Ils décrivent les propriétés et les informations (telles que Bearercap, nom d'hôte, nom du fournisseur et taille de fenêtre). Certaines paires AV sont obligatoires et d'autres facultatives.

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

Pour L2F, la configuration de la transmission tunnel d'une session PPP est identique à celle de

L2TP. Il s'agit :

1. Établissement d'un tunnel entre le NAS et la passerelle domestique. Cette phase se produit uniquement lorsqu'il n'y a pas de 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 une L2F_Conf à la passerelle domestique. Un défi CHAP est inclus dans ce message.
2. La passerelle Home Gateway répond par une L2F_Conf. Un défi CHAP est inclus dans ce message.
3. Le NAS envoie un L2F_Open. La réponse CHAP du défi de la passerelle domestique est incluse dans ce message.
4. La passerelle Home Gateway répond par un L2F_Open. La réponse CHAP du défi NAS est incluse dans ce message. Le tunnel est en service.
5. Le NAS envoie un L2F_Open à la passerelle Home Gateway. Le paquet inclut le nom d'utilisateur du client (client_name), le défi CHAP envoyé par le NAS au client (challenge_NAS) et sa réponse (response_client).
6. La passerelle domestique, en renvoyant L2F_OPEN, accepte le client. Le trafic est désormais libre de circuler dans les deux directions entre le client et la passerelle Home Gateway.

Remarque : un tunnel est identifié par un CLID (ID client). L'ID multidirectionnel (MID) identifie une connexion particulière dans le tunnel.

Configuration du VPDN

Pour plus d'informations sur la configuration du VPDN, reportez-vous au manuel Configuration des

réseaux privés virtuels, et accédez à la section Configuration du VPN.

Informations connexes

- Pages d'assistance pour les technologies de numérotation et d'accès
- Support et documentation techniques - Cisco Systems