Introducción a VPDN’

Contenido

Introducción

Una red virtual de marcación privada (VPDN) permite que un servicio de marcación de red privada se extienda a servidores de acceso remoto (que se definen como concentrador de acceso [LAC]) L2TP.

Cuando un cliente de protocolo punto a punto (PPP) marca en un LAC, el LAC determina que debe reenviar esa sesión PPP a un Servidor de red L2TP (LNS) para ese cliente. El LNS luego autentica al usuario e inicia la negociación PPP. Una vez que finaliza la configuración de PPP, todas las tramas se envían mediante el LAC al cliente y al LNS.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

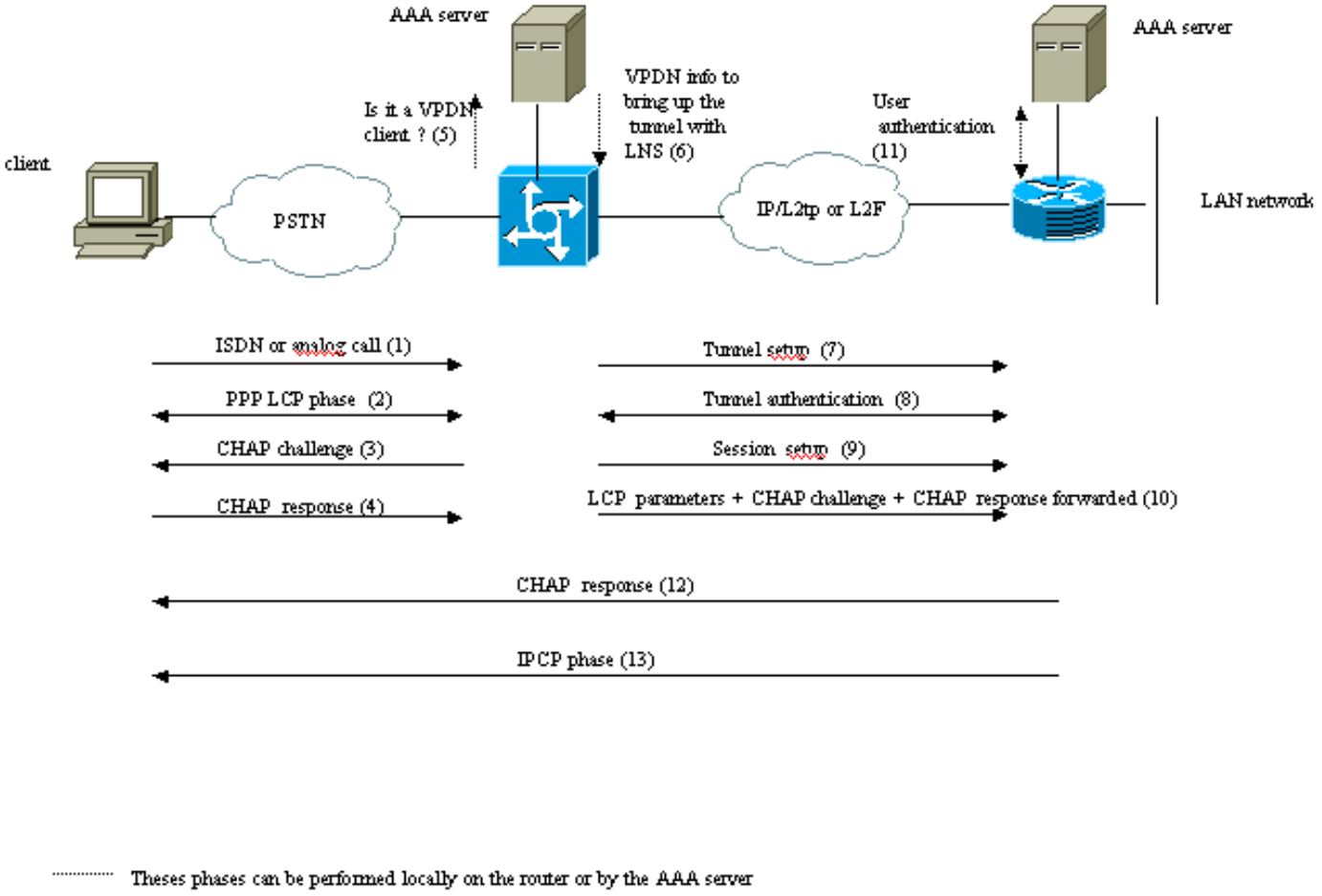
For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Glosario

- **Cliente:** PC o router conectado a una red de acceso remoto, que es el iniciador de una llamada.
- **L2TP:** Protocolo de túnel de capa 2. PPP define un mecanismo de encapsulación para transportar paquetes multiprotocolo a través de links punto a punto de capa 2 (L2). Normalmente, un usuario obtiene una conexión L2 a un servidor de acceso a la red (NAS) mediante una técnica como el servicio telefónico sencillo antiguo (POTS), ISDN o la línea de suscriptor digital asimétrica (ADSL). A continuación, el usuario ejecuta PPP en esa conexión. En tal configuración, el punto de terminación L2 y el punto final de sesión PPP residen en el mismo dispositivo físico (el NAS).L2TP amplía el modelo PPP al permitir que los puntos finales de L2 y de PPP residan en distintos dispositivos interconectados por una red. Con L2TP, el usuario tiene una conexión L2 a un concentrador de acceso y el concentrador luego tuneliza las tramas PPP individuales al NAS. Esto permite el procesamiento real de los paquetes PPP para separarse de la terminación del circuito de L2.
- **L2F:** Layer 2 Forwarding Protocol . L2F es un protocolo de tunelización más antiguo al L2TP.
- **LAC:** Concentrador de acceso L2TP. Un nodo que actúa como un lado de un extremo de túnel L2TP y es un peer para el LNS. El LAC se sitúa entre un LNS y un cliente y reenvía paquetes hacia y desde cada uno. Los paquetes se envían desde el LAC hacia el LNS requieren una tunelización con el protocolo L2TP. La conexión de LAC al cliente se realiza normalmente a través de ISDN o analógica.
- **LNS:** Servidor de red L2TP. Un nodo que funciona como un costado de un punto final de un túnel L2TP y es un par para el LAC. El LNS es el punto de terminación lógico de una sesión PPP que está siendo tunelizada desde el cliente por el LAC.
- **Gateway de inicio**: Iguales definiciones que LNS en la terminología de L2F.
- **NAS :** Iguales definiciones que LAC en la terminología de L2F.
- **Túnel:** En la terminología L2TP, existe un túnel entre un par LAC-LNS. El túnel consiste en una conexión de control y cero o más sesiones L2TP. El túnel transmite datagramas PPP encapsulados y controla los mensajes entre el LAC y el LNS. El proceso es el mismo que se aplica al L2F.
- **Sesión:** L2TP está orientado a la conexión. LNS y LAC mantienen un estado para cada llamada que se inicia o responde a través de LAC. Se crea una sesión L2TP entre LAC y LNS cuando se establece una conexión PPP extremo a extremo entre el cliente y la LNS. Los datagramas relativos a la conexión del PPP son enviados sobre el túnel entre el LAC y el LNS. Existe una relación uno a uno entre las sesiones L2TP establecidas y sus llamadas asociadas. El proceso es el mismo que se aplica al L2F.

Descripción general del proceso VPDN

En la descripción del proceso VPDN a continuación, utilizamos la terminología L2TP y LNS.



1. El cliente llama al LAC (normalmente usando un módem o una tarjeta ISDN).
2. El cliente y el LAC comienzan la fase PPP mediante la negociación de las opciones LCP (método de autenticación por Protocolo de autenticación de contraseña [PAP] o Protocolo de confirmación de aceptación de la autenticación PPP [CHAP], multilink PPP, compresión, etc.).
3. Supongamos que CHAP se negoció en el paso 2. El LAC envía un desafío CHAP al cliente.
4. El LAC obtiene una respuesta (por ejemplo, nombredeusuario@nombrededominio y contraseña).
5. Según el nombre de dominio recibido en la respuesta CHAP o el Servicio de información de número marcado (DNIS) recibido en el mensaje de configuración ISDN, el LAC verifica si el cliente es un usuario VPDN. Para ello, utiliza su configuración VPDN local o se pone en contacto con un servidor de autenticación, autorización y contabilidad (AAA).
6. Debido a que el cliente es un usuario VPDN, el LAC obtiene cierta información (de su configuración VPDN local o de un servidor AAA) que utiliza para activar un túnel L2TP o L2F con el LNS.
7. El LAC trae un túnel L2TP o L2F con el LNS.
8. Según el nombre recibido en la petición proveniente de LAC, LNS verifica si se permite que LAC abra un túnel (LNS verifica su configuración de VPDN local). Más aun, el LAC y el LNS se autentican mutuamente (usan su base de datos local o se comunican con un servidor AAA). El túnel entonces está activo entre ambos dispositivos. En este túnel, se pueden realizar varias sesiones VPDN.
9. Para el cliente username@DomainName, se accionará una sesión VPDN desde LAC hasta LNS. Hay una sesión de VPDN por cliente.
10. El LAC reenvía las opciones de LCP que negoció hacia el LNS con el cliente junto con el

nombredeusuario@nombrededominio y contraseña recibidos del cliente.
11. LNA clona un acceso virtual desde una plantilla virtual especificada en la configuración VPDN. El LNS toma las opciones de LCP recibidas desde el LAC y autentica al cliente de manera local o al contactar al servidor AAA.
12. El LNS envía una respuesta CHAP al cliente.
13. Se realiza la fase del protocolo de control IP (IPCP) y, a continuación, se instala la ruta: la sesión PPP está activada y se ejecuta entre el cliente y el LNS. El LAC sólo reenvía las tramas PPP. Las tramas PPP se tunelizan entre el LAC y el LNS.

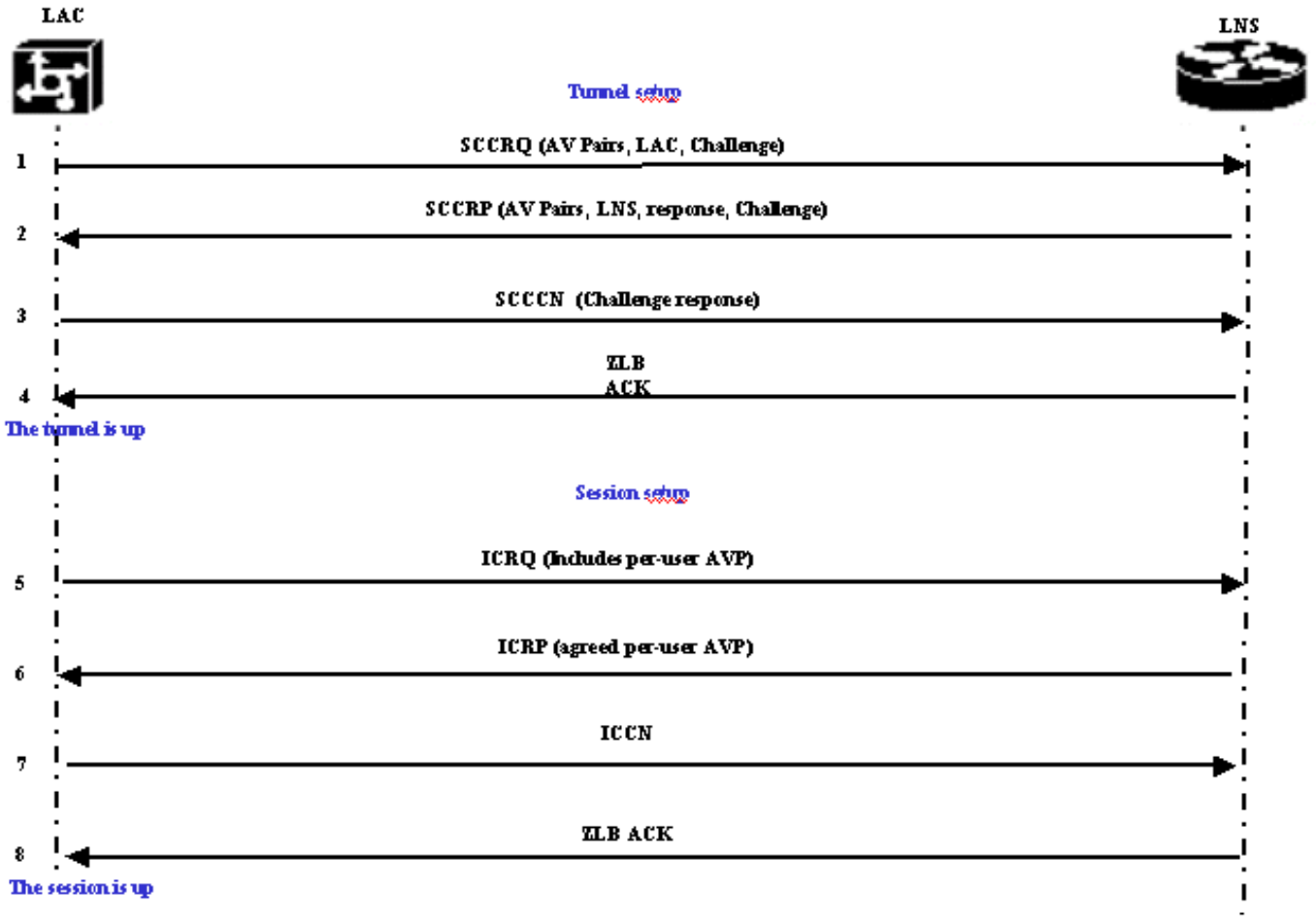
Protocolo de tunelización

Un túnel VPDN se puede crear mediante el reenvío de capa 2 (L2F) o el protocolo de tunelación de capa 2 (L2TP).

- L2F fue introducido por Cisco en la Solicitud de comentarios (RFC) 2341 y es usado para reenviar sesiones PPP para Multichasis Multilinks PPP.
- L2TP introducido en RFC 2661, combina lo mejor del protocolo de L2F y el Protocolo de tunelización punto a punto (PPTP). Además, L2F soporta solamente VPDN de marcado mientras que L2TP soporta VPDN de marcado y de marcado de salida.

Ambos protocolos utilizan el puerto UDP 1701 para construir un túnel a través de una red IP para reenviar tramas de link-capa. Para L2TP, la configuración para la tunelización de una sesión PPP está compuesta de dos pasos:

1. Establecimiento de un túnel entre el LAC y el LNS. Esta fase tiene lugar únicamente cuando no hay ningún túnel activo entre ambos dispositivos.
2. Cómo establecer una sesión entre LAC y LNS.



La LAC decide que un túnel se debe iniciar desde LAC a la LNS.

1. El LAC envía un Start-Control-Connection-Request (SCCRQ, Petición de conexión de control de inicio). En este mensaje se incluyen un desafío CHAP y pares AV.
2. El LNS responde con un Start-Control-Connection-Reply (SCCRP). En este mensaje se incluyen un desafío CHAP, la respuesta al desafío LAC y los pares AV.
3. El LAC envía una Conexión de control de inicio establecida (SCCCN). En este mensaje se incluye la respuesta CHAP.
4. El LNS responde con un reconocimiento de cuerpo de longitud cero (ZLB ACK). Es posible que ese reconocimiento se transporte en otro mensaje. El túnel está activo.
5. LAC envía una petición de llamada entrante (ICRQ) a LNS.
6. El LNS responde con un mensaje de Respuesta de llamada entrante (ICRP).
7. El LAC envía una llamada entrante conectada (ICCN).
8. El LNS responde con un ZLB ACK. Ese reconocimiento también puede ser transportado en otro mensaje.
9. La sesión está activada.

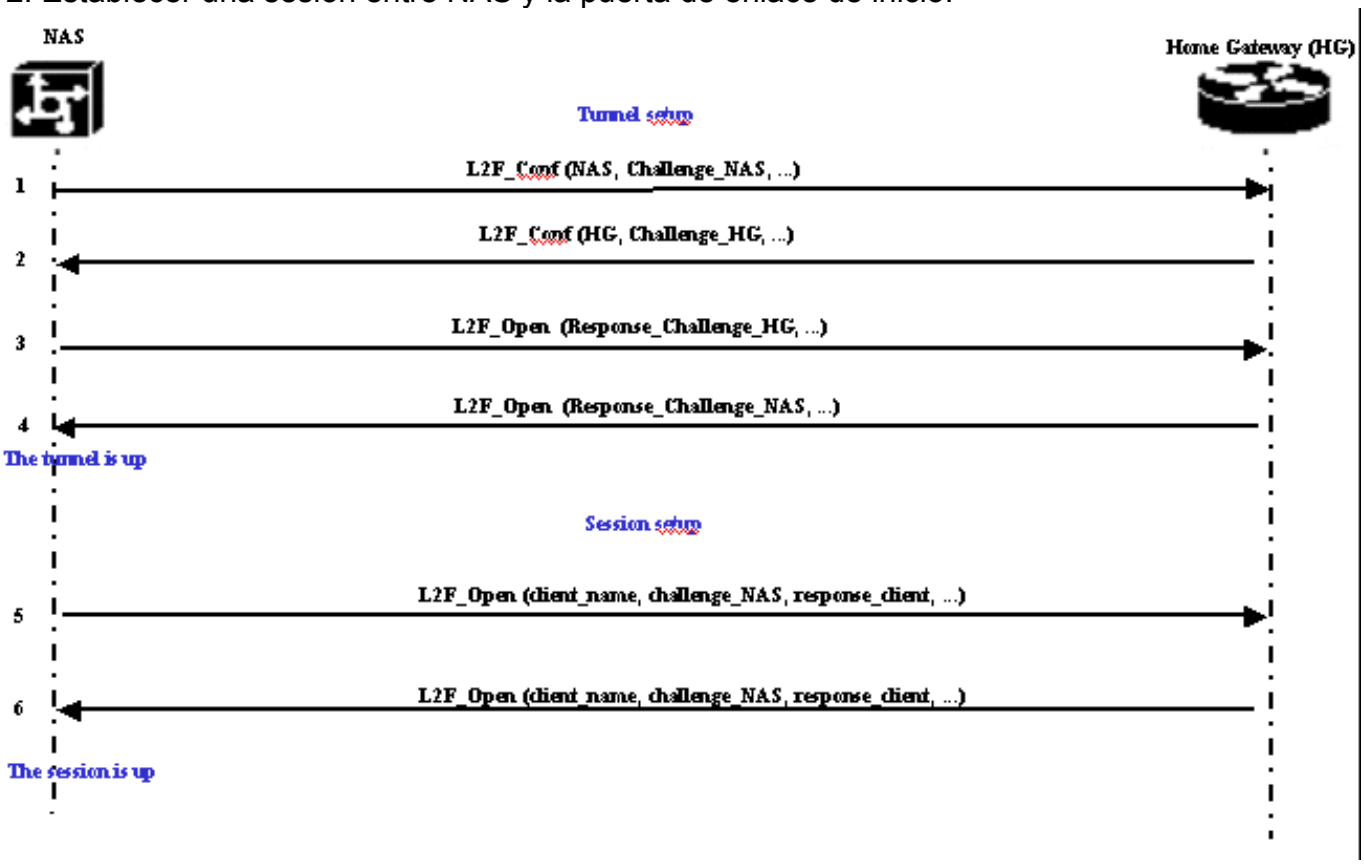
Nota: Los mensajes anteriores utilizados para abrir un túnel o una sesión llevan pares de valores de atributos (AVP) definidos en RFC 2661. Describen propiedades e información (como Bearercap, nombre de host, nombre de proveedor y tamaño de ventana). Algunos Pares AV son obligatorios y otros son opcionales.

Nota: Se utiliza una ID de túnel para multiplexar y desmultiplexar túneles entre el LAC y el LNS. Una ID de sesión se usa para identificar una determinada sesión con el túnel.

Para L2F, la configuración para tunelización de una sesión PPP es la misma que para L2TP.

Incluye:

1. Establecer un túnel entre NAS y la Gateway de inicio. Esta fase tiene lugar únicamente cuando no hay ningún túnel activo entre ambos dispositivos.
2. Establecer una sesión entre NAS y la puerta de enlace de inicio.



El NAS decide que un túnel se debe iniciar desde NAS a la Gateway de inicio.

1. El servidor NAS envía un L2F_Conf a la gateway de inicio. En este mensaje se incluye un desafío CHAP.
2. La puerta de enlace doméstica responde con un L2F_Conf. En este mensaje se incluye un desafío CHAP.
3. El NAS envía un L2F_Open. Este mensaje incluye la respuesta CHAP al desafío de la Gateway de inicio.
4. La puerta de enlace doméstica responde con un L2F_Open. La respuesta CHAP del desafío NAS se incluye en este mensaje. El túnel está activo.
5. El NAS envía un L2F_Open a la gateway de inicio. El paquete incluye el nombre de usuario del cliente (client_name), el NAS envía la impugnación CHAP al cliente (challenge_NAS) y su respuesta (response_client).
6. El Gateway de inicio, por el envío de L2F_OPEN, el cliente acepta. El tráfico ahora está libre para fluir en cualquier dirección entre el cliente y la Puerta de enlace de inicio.

Nota: Se identifica un túnel con un CLID (ID de cliente). La ID multiplex (MID) identifica una conexión determinada dentro del túnel.

'Configuración de VPDN'

Para obtener información sobre la configuración de VPDN, refiérase al manual Configuración de Redes Privadas Virtuales y vaya a la sección Configuración de VPN.

Información Relacionada

- Páginas de soporte de la tecnología de marcado y acceso
- Soporte Técnico y Documentación - Cisco Systems