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 del Point-to-Point Protocol (PPP) marca en un LAC, el LAC determina que debe remitir a esa sesión PPP encendido a un L2TP Network Server (LNS) para ese cliente. El LNS después autentica al usuario y comienza la negociación PPP. Una vez que finaliza la configuración de PPP, todas las tramas se envían mediante el LAC al cliente y al LNS.

prerrequisitos

Requisitos

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. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte las Convenciones de Consejos Técnicos de Cisco.

Glosario

- Cliente: PC o router asociado a una red de acceso remoto, que es el iniciador de una llamada.
- **L2TP**: Tunnel Protocol de la capa 2. El PPP define un mecanismo de encapsulación para transportar los paquetes multiprotocolos a través de los enlaces punto a punto de la capa 2 (L2). Típicamente, un usuario obtiene una conexión L2 a un servidor de acceso a la red (NAS) usando una técnica tal como Servicio telefónico sencillo antiguo (POTS) de marcado manual, ISDN o Asymmetric Digital Subscriber Line (ADSL). El usuario entonces ejecuta el PPP sobre esa conexión. En tal configuración, la punta de terminación L2 y el punto final de la 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 el L2TP, el usuario tiene una conexión L2 a un concentrador de acceso, y el concentrador entonces hace un túnel las tramas individuales PPP 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**: L2TP Access Concentrator. Un nodo que actúa como un lado de un punto final del túnel L2TP y es un par al LNS. El LAC se sienta entre un LNS y un cliente y adelante los paquetes a y desde cada uno. Los paquetes se envían desde el LAC hacia el LNS requieren una tunelización con el protocolo L2TP. La conexión del LAC al cliente está típicamente con el ISDN o el análogo.
- **LNS**: L2TP Network Server. 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, un túnel existe entre un par LAC-LNS. El túnel consiste en un control de conexión y cero o más sesión L2TP. El túnel lleva los datagramas PPP y los mensajes encapsulados del control entre el LAC y el LNS. El proceso es el mismo que se aplica al L2F.
- **Sesión**: El L2TP está orientado a la conexión. LNS y LAC mantienen un estado para cada llamada que se inicia o responde a través de LAC. Una sesión L2TP se crea entre el LAC y el LNS cuando una conexión PPP de punta a punta se establece entre un cliente y el LNS. Los datagramas relacionados con la conexión PPP se envían sobre el túnel entre el LAC y el LNS. Hay a relación uno a uno entre las sesiones establecidas L2TP 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 el LAC (típicamente usando un módem o un indicador luminoso LED amarillo de la placa muestra gravedad menor 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. Hace esto usando su configuración de VPDN local o entrar en contacto un servidor del Authentication, Authorization, and Accounting (AAA).
6. Porque el cliente es usuario VPDN, el LAC la consigue una cierta información (de su configuración de VPDN local o de un servidor de AAA) esa utiliza para traer para arriba un túnel L2TP o L2F con el LNS.
7. El LAC trae para arriba 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 de la GRIETA al cliente.
13. Se realiza la fase del IP Control Protocol (IPCP) y entonces la ruta está instalada: la sesión PPP está activada y se ejecuta entre el cliente y el LNS. El LAC sólo reenvía las tramas PPP. Las tramas PPP son tunneled entre el LAC y el LNS.

Protocolo de tunelización

Un túnel VPDN se puede construir usando la capa 2 que remite (L2F) o el protocolo Layer 2 Tunneling Protocol (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). Por otra parte, los soportes L2F acceden telefónicamente solamente el VPDN mientras que el L2TP soporta el dial-in y el dial-hacia fuera VPDN.

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). Un desafío y los pares AV de la GRIETA se incluyen en este mensaje.
2. El LNS responde con una Principio-Control-Conexión-contestación (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: El antedichos de los mensajes usados para abrir un túnel o una sesión llevan los pares de valores de atributos (AVP) definidos en el RFC 2661. Describen las propiedades y la información (tal como Bearercap, nombre de host, nombre del proveedor y tamaño de la ventana). Algunos pares AV son obligatorios y otros son opcionales.

Nota: Un túnel ID se utiliza para multiplexar y para demultiplexar los túneles entre el LAC y el LNS. Un ID de sesión se utiliza para identificar a una sesión específica con el túnel.

Para el L2F, la configuración para hacer un túnel a una sesión PPP es lo mismo que para el L2TP. Implica:

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. El gateway de inicio 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. El gateway de inicio responde con un L2F_Open. La respuesta de la GRIETA del desafío NAS se incluye en este mensaje. El túnel está activo.
5. El NAS envía un L2F_Open al 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: Un túnel se identifica con un CLID (ID de cliente). El Multiplex ID (MEDIADOS DE) identifica

una conexión determinada dentro del túnel.

‘Configuración de VPDN’

Para la información sobre configurar el VPDN, refiera al manual de las Redes privadas virtuales que configura, y vaya a la sección en configurar el VPN.

Información Relacionada

- Páginas de soporte de la tecnología del Marcado y acceso remotos
- Soporte Técnico y Documentación - Cisco Systems