Cómo funcionan las redes privadas virtuales

Contenido

Introducción

Este documento describe los aspectos básicos de VPN, como los componentes básicos de VPN, las tecnologías, los túneles y la seguridad de VPN.

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.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

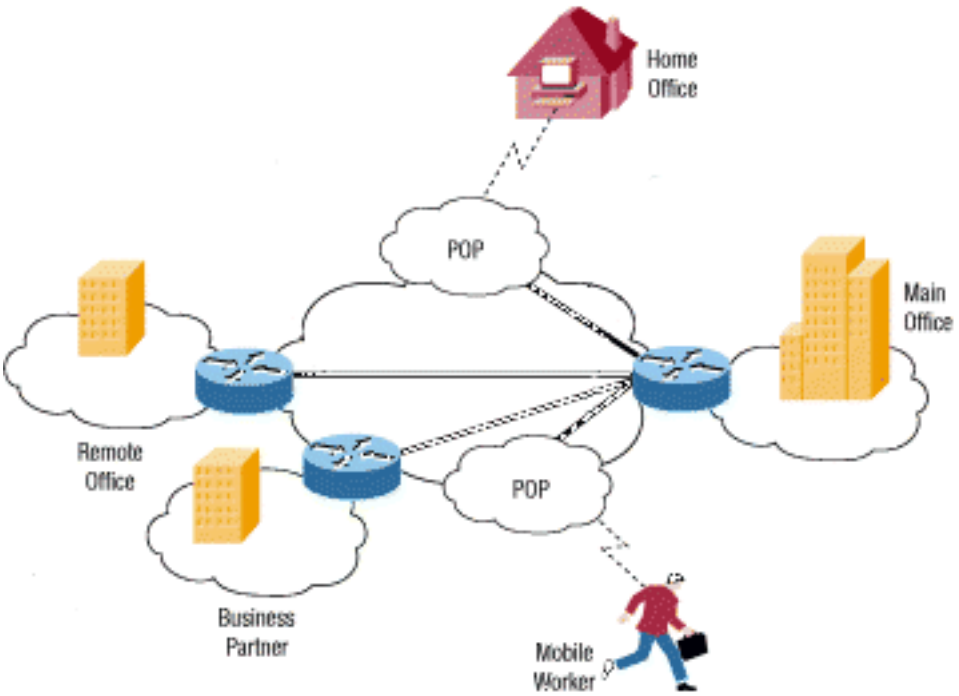
Antecedentes

El mundo ha cambiado mucho en las últimas décadas. En lugar de simplemente abordar problemas locales o regionales, muchas empresas ahora deben tener en cuenta logística y mercados globales. Muchas empresas cuentan con instalaciones diseminadas en todo el país o,

incluso, en todo el mundo. Pero hay algo que todas las empresas necesitan: una forma de mantener comunicaciones rápidas, seguras y fiables donde se encuentran sus oficinas.

Hasta hace poco, una comunicación fiable implicaba el uso de líneas arrendadas para mantener una red de área amplia (WAN). Las líneas arrendadas, desde la Red digital de servicios integrados (ISDN, que se ejecuta a 144 KB/s) hasta la fibra óptica Carrier-3 (OC3, que se ejecuta a 155 Mbps), ofrecen a una empresa una forma de ampliar su red privada más allá de su zona geográfica inmediata. Una WAN tiene ventajas claras en relación con una red pública como Internet cuando se trata de fiabilidad, rendimiento y seguridad; pero mantener una WAN, especialmente cuando se utilizan líneas arrendadas, puede volverse bastante costoso (a menudo, aumenta el costo a medida que aumenta la distancia entre las oficinas). Además, las líneas arrendadas no son una solución viable para organizaciones en las que parte de la fuerza de trabajo es muy móvil (como es el caso del personal de marketing) y puede necesitar con frecuencia conectarse a la red corporativa de forma remota y tener acceso a datos confidenciales.

A medida que ha ido aumentando la popularidad de Internet, las empresas han recurrido a esta como medio para ampliar sus propias redes. Primero, se utilizaron intranets, que son sitios diseñados para que solo los usen los empleados de la empresa. Ahora, muchas empresas crean sus propias redes privadas virtuales (VPN) para satisfacer las necesidades de los trabajadores remotos y de las oficinas lejanas.



Una VPN típica puede tener una red de área local (LAN) principal en la sede central corporativa de una empresa, otras LAN en oficinas o instalaciones remotas, y usuarios individuales que se conectan desde el campo.

Una VPN es una red privada que utiliza una red pública (por lo general, Internet) para conectar sitios o usuarios remotos entre sí. En vez de utilizar una conexión real dedicada como línea arrendada, una VPN utiliza conexiones "virtuales" enrutadas a través de Internet desde la red privada de la empresa hacia el empleado o el sitio remoto.

¿Qué constituye una VPN?

Hay dos tipos de VPN comunes.

- **Acceso remoto : también denominada Red telefónica privada virtual (VPDN), se trata de una conexión de usuario a LAN utilizada por una empresa que posee empleados que necesitan conectarse a la red privada desde distintas ubicaciones remotas.** Normalmente, una empresa que desea configurar una VPN de acceso remoto grande proporciona algún tipo de cuenta telefónica de Internet a sus usuarios mediante un proveedor de servicios de Internet (ISP). Luego, los teletrabajadores pueden marcar un número 1-800 para conectarse a Internet y usar su software de cliente VPN para acceder a la red corporativa. Un buen ejemplo de una empresa que necesita una VPN de acceso remoto sería una firma grande con cientos de miembros del personal de ventas en el campo. Las VPN de acceso remoto permiten conexiones seguras y cifradas entre la red privada de una empresa y los usuarios remotos a través de un proveedor de servicios de terceros.
- **Sitio a sitio: mediante el uso de equipos exclusivos y cifrado a gran escala, una empresa puede conectar varios sitios fijos a través de una red pública como Internet.** Cada sitio solo necesita una conexión local a la misma red pública, lo cual ahorra dinero en extensas líneas arrendadas privadas. Las VPN de sitio a sitio también se pueden clasificar en intranets o extranets. Una VPN de sitio a sitio desarrollada entre oficinas de la misma empresa se denomina VPN intranet, mientras que una VPN desarrollada para conectar la empresa con su partner o cliente se denomina VPN extranet.

Una VPN bien diseñada puede beneficiar mucho a una empresa. Por ejemplo, puede:

- Ampliar la conectividad geográfica
- Reducir costos operativos en relación a WAN tradicionales
- Reducir los tiempos de tránsito y los costos de viaje de usuarios remotos
- Mejorar la productividad
- Simplificar la topología de la red
- Proporcionar oportunidades de redes globales
- Proporcionar soporte para el teletrabajador
- Proporcionar un Retorno de la inversión (ROI) más rápido que la WAN tradicional

¿Qué funciones se necesitan en una VPN bien diseñada? Debe incorporar estos elementos:

- Security
- Confiabilidad
- Escalabilidad
- Administración de la red
- Administración de políticas

Productos analógicos: Cada LAN es una isla

Imaginemos que vive en una isla en un océano enorme. Hay miles de otras islas a su alrededor, algunas muy cercanas y otras más alejadas. La manera normal de viajar es tomar un buque de su isla a cualquier isla que desee visitar. Viajar en buque implica no tener casi nada de privacidad. Todo lo que haga lo puede ver otra persona.

Supongamos que cada isla representa una LAN privada e Internet es el océano. Viajar por buque es similar a conectarse a un servidor web u otro dispositivo a través de Internet. No tiene ningún control sobre los cables y routers que componen Internet, al igual que no tiene ningún control de

las demás personas en el buque. Esto lo deja susceptible a problemas de seguridad si intenta conectarse entre dos redes privadas a través de un recurso público.

Su isla decide crear un puente con otra isla para que haya una forma más fácil, más segura y directa para que las personas viajen entre ellas. Es costoso crear y mantener el puente, incluso si la isla con la que se conecta está muy cerca. Pero la necesidad de una ruta fiable y segura es tan grande que se crea de todas maneras. A su isla le gustaría conectarse a una segunda isla mucho más alejada, pero usted decide que es demasiado costoso.

Esta situación se asemeja a tener una línea arrendada. Los puentes (líneas arrendadas) están separados del océano (Internet), pero pueden conectarse a las Islas (LAN). Muchas otras empresas han seleccionado esta ruta debido a la necesidad de seguridad y fiabilidad en conectar sus oficinas remotas. Sin embargo, si las oficinas están muy alejadas, el costo puede ser demasiado alto, como intentar crear un puente que abarque una gran distancia.

¿Cómo se ajusta VPN a esta analogía? Podríamos ofrecer a cada habitante de nuestras islas su propio submarino pequeño con estas propiedades.

- Es rápido.
- Es fácil de llevarlo con usted, vaya donde vaya.
- Es capaz de ocultarse por completo de cualquier otro barco o submarino.
- Es fiable.
- Cuesta poco agregar submarinos adicionales a su flota una vez que se ha adquirido el primero.

Aunque estén viajando por el océano junto con el resto del tráfico, los habitantes de nuestras dos islas podrían ir y venir siempre que lo desearan con privacidad y seguridad. Así funciona básicamente una VPN. Cada miembro remoto de la red se puede comunicar de forma segura y fiable a través de Internet como medio para conectarse a la LAN privada. Una VPN puede aumentar para albergar a más usuarios y diferentes ubicaciones de manera mucho más fácil que una línea arrendada. De hecho, la escalabilidad es una ventaja importante que tienen las VPN en relación con las típicas líneas arrendadas. A diferencia de las líneas arrendadas donde el costo aumenta de manera proporcional a las distancias implicadas, las ubicaciones geográficas de cada oficina importan poco en la creación de una VPN.

Tecnologías VPN

Una VPN bien diseñada utiliza varios métodos para conservar sus datos y la conexión seguros.

- **Confidencialidad de datos : este es quizá el servicio más importante ofrecido por cualquier implementación de VPN.** Dado que los datos privados viajan a través de una red pública, la confidencialidad de estos es fundamental y puede lograrse mediante el cifrado de datos. Este es el proceso de tomar todos los datos que una computadora está enviando a otra y cifrarlos en un formato que solo la otra computadora pueda descifrar.La mayoría de las VPN utiliza uno de estos protocolos para proporcionar cifrado.**IPsec : el Protocolo de seguridad de protocolos de Internet (IPsec) proporciona funciones de seguridad mejorada como algoritmos de cifrado más potentes y autenticación integral.** IPsec tiene dos modos de cifrado: túnel y transporte. El modo de túnel cifra el encabezado y la carga de cada paquete mientras el modo de transporte solo cifra la carga. Solo los sistemas que son compatibles con IPsec pueden aprovechar este protocolo. Además, todos los dispositivos deben utilizar una clave o certificado común y deben implementar políticas de seguridad muy similares.Para los

usuarios VPN de acceso remoto, algún tipo de paquete de software de terceros proporciona la conexión y el cifrado en las PC de los usuarios. IPsec admite 56 bits (solo DES) o cifrado de 168 bits (triple DES).**PPTP/MPPE : PPTP fue creado por el foro de PPTP, un consorcio que incluye US Robotics, Microsoft, 3COM, Ascend y ECI Telematics.** PPTP admite VPN multiprotocolo, con cifrado de 40 bits y 128 bits mediante un protocolo denominado Cifrado de punto a punto de Microsoft (MPPE). Es importante tener en cuenta que PPTP no proporciona cifrado de datos por su cuenta.**L2TP/IPsec : comúnmente denominado L2TP a través de IPsec, proporciona la seguridad del protocolo de IPsec a través de los túneles de Protocolo de túneles de capa 2 (L2TP).** L2TP es producto de una asociación entre los miembros del foro de PPTP, Cisco y el Grupo de tareas de ingeniería de Internet (IETF). Se usa principalmente para VPN de acceso remoto con sistemas operativos Windows 2000, ya que Windows 2000 proporciona una IPsec nativa y un cliente L2TP. Los proveedores de servicios de Internet también pueden brindar conexiones L2TP para usuarios de acceso telefónico y, luego, cifrar el tráfico con IPsec entre su punto de acceso y el servidor de red de la oficina remota.

- **Integridad de los datos: si bien es importante que los datos se cifren a través de una red pública, es igualmente importante verificar que no se hayan modificado mientras están en tránsito.** Por ejemplo, IPsec tiene un mecanismo para asegurarse de que no se haya manipulado la parte cifrada del paquete o toda la parte de encabezado y datos del paquete. Si se ha detectado manipulación, el paquete se descarta. La integridad de los datos también puede implicar la autenticación del par remoto.
- **Autenticación de origen de datos : es muy importante verificar la identidad de la fuente de los datos que se envían.** Esto es necesario para protegerlo contra un número de ataques que utilizan la suplantación de la identidad del remitente.
- **Control antirreproducción: esta es la capacidad para detectar y rechazar paquetes reproducidos y ayuda a evitar la suplantación de identidad.**
- **Confidencialidad de tráfico/tunelizado de datos: El tunelizado es el proceso de encapsular un paquete entero dentro de otro paquete y enviarlo a través de una red.** El tunelizado de datos es útil en casos en los que se recomienda ocultar la identidad del dispositivo que originó el tráfico. Por ejemplo, un único dispositivo que utiliza IPsec encapsula el tráfico que pertenece a un número de hosts detrás de sí y agrega su propio encabezado sobre los paquetes existentes. Al cifrar el paquete y el encabezado originales (y enrutar el paquete según el encabezado de capa 3 adicional agregado en la parte superior), el dispositivo de tunelizado oculta de manera eficaz la fuente real del paquete. Solo el par de confianza es capaz de determinar la fuente real, después de que quita el encabezado adicional y descifra el encabezado original. Como se indica en RFC 2401 , "...la divulgación de las características externas de la comunicación también puede ser motivo de preocupación en algunas circunstancias. La confidencialidad de flujo de tráfico es el servicio que aborda este último problema al ocultar las direcciones de origen y destino, la longitud del mensaje o la frecuencia de la comunicación. En el contexto de IPsec, utilizar ESP en modo de túnel, especialmente en un gateway de seguridad, puede ofrecer un nivel de confidencialidad de flujo de tráfico".Todos los protocolos de cifrado que aparecen aquí también usan el tunelado como un medio para transferir los datos cifrados a través de la red pública. Es importante tener en cuenta que el tunelado, por sí solo, no proporciona seguridad de datos. El paquete original simplemente se encapsula dentro de otro protocolo y aún puede visualizarse con un dispositivo de captura de paquetes si no es cifrado. Sin embargo, aquí se menciona el motivo por el que es una parte integral de cómo funcionan las VPN.El tunelado requiere tres protocolos diferentes.**Protocolo de pasajero: los datos originales (IPX, NetBeui, IP) que se**

transportan.Protocolo de encapsulación: el protocolo (GRE, IPsec, L2F, PPTP, L2TP) que envuelve los datos originales.Protocolo de transporte: el protocolo utilizado por la red a través de la cual viaja la información. El paquete original (Protocolo de pasajero) se encapsula dentro del protocolo de encapsulación, que, luego, se coloca dentro del encabezado del protocolo de la portadora (generalmente IP) para la transmisión a través de la red pública. Tenga en cuenta que el protocolo de encapsulación muy a menudo también lleva a cabo el cifrado de los datos. Los protocolos como IPX y NetBeui, que normalmente no se transfieren a través de Internet, pueden transmitirse de forma segura.Para las VPN de sitio a sitio, el protocolo de encapsulación generalmente es IPsec o Encapsulamiento de routing genérico (GRE). GRE incluye información sobre qué tipo de paquete está encapsulando e información sobre la conexión entre el cliente y el servidor.Para VPN de acceso remoto, el tunelado generalmente se realiza mediante el Protocolo punto a punto (PPP). Como parte de la pila TCP/IP, PPP es la portadora de otros protocolos IP cuando se comunican a través de la red entre la computadora host y un sistema remoto. El tunelado PPP utilizará uno de los Reenvíos de capa 2 (L2F) de PPTP, L2TP o Cisco.

- **AAA**: la autenticación, autorización y contabilización se utiliza para un acceso más seguro en un entorno VPN de acceso remoto. Sin la autenticación del usuario, cualquiera que se encuentra en una computadora portátil o PC con software de cliente VPN bien configurado puede establecer una conexión segura a la red remota. Sin embargo, con la autenticación de usuario, también se debe introducir un nombre de usuario y contraseña válidos antes de completar la conexión. Los nombres de usuario y contraseñas se pueden almacenar en el propio dispositivo de terminación de VPN o en un servidor AAC externo, lo que puede suministrar autenticación a muchas otras bases de datos como Windows NT, Novell, LDAP, etc.Cuando una solicitud para establecer un túnel proviene de un cliente de acceso telefónico, el dispositivo VPN solicita un nombre de usuario y una contraseña. Luego, esto se puede autenticar de forma local o enviarse al servidor AAC externo, que comprueba:Quién es usted (Autenticación)Qué tiene permitido hacer (Autorización)Qué hace realmente (Cuenta)La información de Cuenta es especialmente útil para realizar el seguimiento de uso del cliente con fines de auditoría, facturación o informes de seguridad.
- **No rechazo: en determinadas transferencias de datos, especialmente las relacionadas con las transacciones financieras, el no rechazo es una función muy recomendable.** Esto resulta útil para evitar situaciones donde una de las partes niega haber participado en una transacción. De manera similar a como un banco requiere su firma antes de otorgarle un cheque, el no rechazo funciona al agregar una firma digital en el mensaje enviado, por lo que impide la posibilidad de que el remitente niegue participación en la transacción.

Existe un número de protocolos que pueden utilizarse para crear una solución de VPN. Todos estos protocolos proporcionan un subconjunto de los servicios que aparecen en este documento. La elección de un protocolo depende del conjunto de servicios que desee. Por ejemplo, una organización puede no tener problemas con que los datos se transfieran en texto no cifrado, pero puede preocuparse por mantener su integridad, mientras que otra organización puede considerar la confidencialidad de los datos absolutamente esencial. Entonces, su elección de protocolos puede ser diferente. Para obtener más información sobre los protocolos disponibles y sus fortalezas relativas, consulte ¿Qué solución de VPN es adecuada para usted?

Productos VPN:

Según el tipo de VPN (acceso remoto o de sitio a sitio), debe implementar ciertos componentes para generar la VPN. Entre ellos se encuentran:

- Cliente de software de escritorio para cada usuario remoto
- Hardware exclusivo, como un concentrador de VPN de Cisco o un Firewall Cisco Secure PIX
- Servidor de VPN exclusivo para servicios telefónicos
- Servidor de acceso a la red (NAS) usado por el proveedor de servicios para el acceso de VPN de usuario remoto
- Red privada y Centro de administración de políticas

Debido a que no hay ningún estándar ampliamente aceptado para la implementación de una VPN, muchas otras empresas han desarrollado sus propias soluciones integrales. Por ejemplo, Cisco ofrece varias soluciones de VPN que incluyen:

- **Concentrador de VPN: al incorporar las técnicas de autenticación y cifrado más avanzadas disponibles, los concentradores de VPN de Cisco se desarrollaron específicamente para crear una VPN de acceso remoto o de sitio a sitio y preferentemente se deben implementar donde se los necesita para que un único dispositivo gestione un alto número de túneles VPN.** El concentrador de VPN se desarrolló específicamente para abordar el requisito de un dispositivo VPN de acceso remoto con diseño específico. Los concentradores proporcionan alta disponibilidad, alto rendimiento y escalabilidad, e incluyen componentes, denominados módulos de Procesamiento de cifrado escalable (SEP), que permiten a los usuarios aumentar fácilmente el rendimiento y la capacidad. Los concentradores se ofrecen en modelos adecuados tanto para pequeñas empresas con 100 usuarios de acceso remoto o menos como para empresas con hasta 10 000 usuarios remotos simultáneos. 
- **Router activado por VPN/Router optimizado por VPN: todos los routers de Cisco que ejecutan software Cisco IOS® son compatibles con las VPN IPsec.** El único requisito es que el router debe ejecutar una imagen de CISCO IOS con el conjunto de funciones adecuado. La solución de VPN de Cisco IOS es totalmente compatible con los requisitos de VPN de acceso remoto, intranet y extranet. Esto significa que los routers de Cisco pueden funcionar igualmente bien al estar conectados a un host remoto, ejecutar el software de cliente de VPN o conectarse a otro dispositivo VPN como un router, Firewall PIX o Concentrador de VPN. Los routers con VPN son adecuados para las VPN con cifrado moderado y requisitos de túnel, y proporcionan servicios de VPN totalmente a través de funciones de software Cisco IOS. Entre los ejemplos de routers con VPN activado se incluyen las series Cisco 1000, Cisco 1600, Cisco 2500, Cisco 4000, Cisco 4500 y Cisco 4700.Los routers optimizados para VPN de Cisco proporcionan escalabilidad, routing, seguridad y calidad del servicio (QoS). Los routers se basan en el software Cisco IOS y se dispone de un dispositivo adecuado para cada situación, desde acceso para una pequeña oficina u oficina en el hogar (SOHO) hasta agregación de VPN de central a sitio para necesidades empresariales a gran escala. Los routers optimizados para VPN están diseñados para satisfacer los requisitos de tunelizado y cifrado de alto nivel y, a menudo, utilizan hardware adicional, como tarjetas de cifrado para lograr un alto rendimiento. Entre los ejemplos de routers con VPN activado se incluyen las series Cisco

1000, Cisco 1600, Cisco 2500, Cisco 4000, Cisco 4500 y Cisco

4700.

- **Firewall Cisco Secure PIX: el Firewall Private Internet eXchange (PIX) combina la traducción de direcciones de red dinámicas, el servidor proxy, el filtrado de paquetes y las capacidades de VPN en una sola pieza de hardware.** En lugar de utilizar el software Cisco IOS, este dispositivo cuenta con un sistema operativo altamente optimizado que sacrifica la capacidad para gestionar una variedad de protocolos por una solidez y un rendimiento extremos, centrándose en la IP. Como con los routers de Cisco, todos los modelos de Firewall PIX son compatibles con la VPN IPsec. Todo lo que se necesita es cumplir con los requisitos de

licencia para activar la función VPN.
- **Clientes VPN de Cisco: Cisco ofrece clientes VPN de hardware y software.** El Cliente VPN de Cisco (software) se incluye con el Concentrador de VPN serie 3000 de Cisco sin costo adicional. Este cliente de software puede instalarse en la máquina host y utilizarse para conectarse de forma segura al concentrador del sitio central (o cualquier otro dispositivo VPN, como router o firewall). El cliente VPN 3002 de hardware es una alternativa a implementar el software de Cliente VPN en cada máquina y proporciona conectividad VPN a un número de dispositivos.

La opción de dispositivos que se utiliza para generar la solución VPN es, en última instancia, un problema de diseño que depende de un número de factores, incluidos el rendimiento deseado y el número de usuarios. Por ejemplo, en un sitio remoto con un conjunto de usuarios detrás de una PIX 501, usted podría considerar configurar el PIX existente como terminal de la VPN IPsec, siempre que acepte el rendimiento 3DES de aproximadamente 3 Mbps del 501 y el límite de un máximo de 5 pares de VPN. Por otro lado, en un sitio central que actúa como terminal de VPN para un gran número de túneles VPN, se recomienda adoptar un router optimizado para VPN o un concentrador de VPN. La opción ahora depende del tipo (LAN a LAN o de acceso remoto) y el número de túneles VPN configurados. La amplia gama de dispositivos Cisco compatibles con VPN proporciona a los diseñadores de red una amplia flexibilidad y una solución sólida para satisfacer todas las necesidades de diseño.

Información Relacionada

- Introducción a VPDN'
- Redes privadas virtuales (VPN)

- Página de soporte técnico de Concentradores de VPN serie 3000 de Cisco
- Página de soporte del VPN 3000 Client de Cisco
- Página de Soporte del Protocolo IKE/la Negociación de IPSec
- Página de soporte técnico de Firewalls PIX serie 500
- RFC 1661: Protocolo punto a punto (PPP)
- RFC 2661: Layer Two Tunneling Protocol "L2TP"
- Cómo funciona el material: Cómo funcionan las redes privadas virtuales
- Descripción general de las VPN
- Página de VPN de Tom Dunigan
- Consorcio de Red privada virtual (VPN)
- Solicitudes de Comentarios (RFC)
- Soporte Técnico - Cisco Systems