Cómo las redes privadas virtuales funcionan

Contenido

Introducción

Este documentos abarca los fundamentales de los VPN, tales como componentes básicos de VPN, Tecnologías, Tunelización, y seguridad VPN.

Prerequisites

Requisitos

No hay requisitos específicos para este documento.

Componentes usados

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.

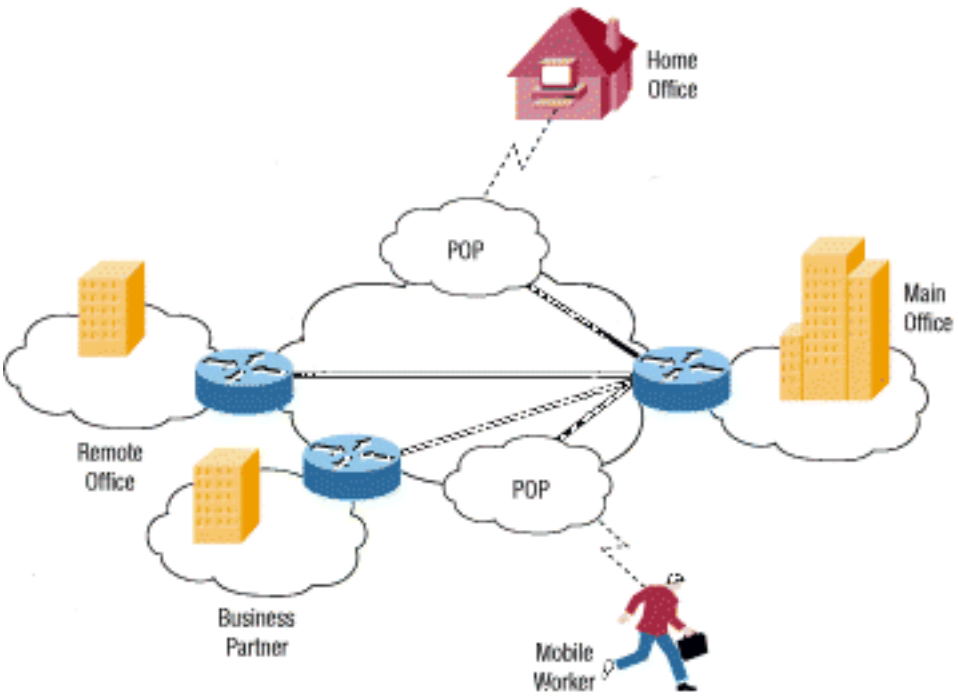
Antecedentes

El mundo ha cambiado mucho en los pares pasados de las décadas. En vez simplemente de ocuparse de las preocupaciones locales o regionales, muchos negocios ahora tienen que pensar en los mercados globales y la logística. Muchas compañías hacen que los recursos se separen

hacia fuera en todo el país, o aún en todo el mundo. Pero hay una cosa que todas las compañías necesitan: una manera de mantener rápidamente, seguro, y comunicaciones confiables dondequiera que se localicen sus oficinas.

Hasta hace poco tiempo, la comunicación confiable ha significado el uso de las líneas arrendadas de mantener un Red de área ancha (WAN). Las líneas arrendadas, extendiéndose del Integrated Services Digital Network (ISDN, que se ejecuta en 144 Kbps) (OC3, que se ejecuta en el 155 Mbps) a la fibra Óptica Carrier-3, proveen de una compañía una manera de ampliar su red privada más allá de su área geográfica inmediata. WAN tiene ventajas obvias sobre una red pública como Internet cuando se trata de la confiabilidad, del funcionamiento, y de la Seguridad; pero mantener WAN, determinado al usar las líneas arrendadas, puede llegar a ser muy costoso (él a menudo las subidas del coste como la distancia entre los aumentos de las oficinas). Además, las líneas arrendadas no son una solución viable para las organizaciones donde está muy móvil (como en el caso del equipo de comercialización) y pudo necesitar con frecuencia la parte de la fuerza de trabajo conectar con la red corporativa remotamente y tener acceso a los datos vulnerables.

Mientras que el renombre de Internet ha crecido, los negocios han dado vuelta a él como medio para extender sus propias redes. Primero vinieron los intranets, que son sitios diseñados para el uso solamente por los empleados de la compañía. Ahora, muchas compañías crean su propio Redes privadas virtuales (VPN) para acomodar las necesidades de los empleados remotos y de las oficinas lejanas.



Un VPN típico pudo tener el red de área local (LAN) principal en las oficinas principales de la compañía de una compañía, el otro LANs en las oficinas remotas o los recursos, y los usuarios individuales que conectan hacia fuera adentro del campo.

Un VPN es una red privada que utiliza una red pública (generalmente Internet) para conectar los sitios remotos o a los usuarios juntos. En vez de usar una conexión dedicada, del mundo real, tal como línea arrendada, un VPN utiliza las conexiones “virtuales” encaminadas a través de Internet de la red privada de la compañía al sitio remoto o al empleado.

¿Qué hace un VPN?

Hay dos tipos comunes de VPN.

- **Acceso Remoto** — También llamó un Virtual Private Dialup Network (VPDN), esto es una conexión de usuario a LAN usada por una compañía que tiene los empleados que necesitan conectar con la red privada de los diversos lugares remotos. Típicamente, una sociedad que desea poner un VPN de acceso remoto grande proporciona a una cierta forma de cuenta de marcado manual de Internet a sus usuarios que usan un Proveedor de servicios de Internet (ISP). Los telecommuters pueden entonces marcar un número 1-800 para alcanzar Internet y para utilizar su software cliente VPN para tener acceso a la red corporativa. Un buen ejemplo de una compañía que necesita un VPN de acceso remoto sería una empresa grande con los centenares de gente de las ventas en el campo. Los VPN de accesos remotos permiten seguro, las conexiones encriptadas entre la red privada de una compañía y a los usuarios remotos a través de un proveedor del servicio de otras compañías.
- **Sitio-a-sitio** — Con el uso del equipo dedicado y de la encripción a gran escala, una compañía puede conectar los sitios revisados múltiples sobre una red pública tal como Internet. Cada sitio necesita solamente una conexión local a la misma red pública, de tal modo guardando el dinero en las arrendar-líneas privadas largas. Los VPN de sitios a sitio se pueden categorizar más a fondo en los intranets o las extranets. Un VPN de sitio a sitio construido entre las oficinas de la misma compañía reputa un intranet VPN, mientras que un VPN construido para conectar a la compañía con su partner o cliente se refiere como extranet VPN.

Un VPN bien diseñado puede beneficiar grandemente a una compañía. Por ejemplo, puede:

- Amplíe la conectividad geográfica
- Reduzca los costos de funcionamiento contra los WAN tradicionales
- Reduzca los tiempos en tránsito y los costes que viajan para los usuarios remotos
- Mejore la productividad
- Simplifique la topología de red
- Proporcione a las oportunidades de red global
- Proporcione la ayuda del telecommuter
- Proporcione a un retorno en la inversión más rápido (ROI) que el WAN tradicional

¿Qué características se necesitan en un VPN bien diseñado? Debe incorporar estos items:

- Security
- Confiabilidad
- Capacidad de conversión a escala
- Administración de la red
- Administración de políticas

Analogía: Cada LAN es una isla

Imagínese que usted vive en una isla en un océano gigantesco. Hay millares de otras islas todo alrededor de usted, de algo muy cerca y de otros más lejos lejos. La forma normal de viajar es llevar un transbordador de su isla cualquier isla usted desea visitar. El viajar en un transbordador significa que usted no tiene casi ninguna aislamiento. Cualquier cosa que usted lo hace se puede considerar por algún otro.

Asuma que cada isla representa un LAN privado y el océano es Internet. Cuando usted viaja en

transbordador, es similar a cuando usted conecta con un servidor Web o con otro dispositivo a través de Internet. Usted no tiene ningún control sobre los alambres y el Routers que compone Internet, apenas como usted no tiene ningún control sobre la otra gente en el transbordador. Esto le deja susceptible a los problemas de seguridad si usted intenta conectar entre dos redes privadas usando un recurso público.

Su isla decide a construir un puente a otra isla de modo que haya un más fácil, una manera más segura y más directa para que la gente viaje entre los dos. Es costoso construir y mantener el puente, aunque la isla que usted está conectando con está muy cercana. Pero la necesidad de un confiable, trayecto seguro es tan grande que usted lo hace de todos modos. Su isla quisiera conectar con una segunda isla que está mucho más lejos ausente, pero usted decide que es demasiado costosa.

Esta situación es mucha como tener una línea arrendada. Los puentes (líneas arrendadas) están a parte del océano (Internet), con todo de los ellos pueden conectar las islas (LANs). Muchas compañías han elegido esta ruta debido a la necesidad de la Seguridad y la confiabilidad en la conexión de sus oficinas remotas. Sin embargo, si las oficinas están separadas muy lejano, el coste puede ser prohibitivo alto - apenas como intentar construir un puente que atraviese una gran distancia.

¿Tan cómo el VPN cabe adentro a esta analogía? Podríamos dar a cada habitante de nuestras islas su propio pequeño submarino con estas propiedades.

- Es rápido.
- Es fácil tomar con usted dondequiera que usted vaya.
- Puede ocultarle totalmente de cualesquiera otros barcos o submarino.
- Es confiable.
- Cuesta poco para agregar los submarinos adicionales a su flota una vez que se compran los primeros.

Aunque estén viajando en el océano junto con el otro tráfico, los habitantes de nuestras dos islas podrían viajar hacia adelante y hacia atrás siempre que quisieran con a la aislamiento y a la Seguridad. Ése es esencialmente cómo un VPN trabaja. Cada miembro remoto de su red puede comunicar en un seguro y una manera confiable usando Internet como el media a conectar con el LAN privado. Un VPN puede crecer para acomodar más usuarios y ubicaciones diferentes mucho más fáciles que una línea arrendada. De hecho, la capacidad de conversión a escala es una ventaja importante que los VPN tienen sobre las líneas arrendadas típicas. A diferencia de las líneas arrendadas donde el coste aumenta en proporción a las distancias implicadas, las ubicaciones geográficas de cada materia de la oficina poco en la creación de un VPN.

Tecnologías VPN

Un VPN bien diseñado utiliza varios métodos para mantener su conexión y datos seguros.

- **Confidencialidad de los datos** — Éste es quizás el servicio más importante proporcionado por cualquier implementación de VPN. Puesto que sus datos privados viajan sobre una red pública, la confidencialidad de los datos es vital y puede ser lograda cifrando los datos. Éste es el proceso de tomar todos los datos que un ordenador está enviando a otro y está codificando los en una forma que solamente el otro ordenador podrá decodificar.La mayoría de los VPN utilizan uno de estos protocolos para proporcionar al cifrado.**IPsec** — El protocolo de Seguridad del protocolo de Internet (IPsec) proporciona a las funciones de seguridad

mejorada tales como algoritmos de encripción más fuertes y más autenticación completa. IPsec tiene dos modos de encripción: túnel y transporte. El modo túnel cifra la encabezado y el payload de cada paquete mientras que el modo de transporte cifra solamente el payload. Solamente los sistemas que son IPsec-obedientes pueden aprovecharse de este protocolo. También, todos los dispositivos deben utilizar una clave común o certificarla y deben tener disposición muy similar de las políticas de seguridad.Para los usuarios del VPN de acceso remoto, una cierta forma de paquete del software de tercero proporciona a la conexión y al cifrado en la PC de los usuarios. Soportes para IPSec 56-bit (solo DES) o cifrado del 168-bit (DES triple).**PPTP/MPPE** — PPTP fue creado por el foro de PPTP, un consorcio que incluye la robótica E.E.U.U., Microsoft, 3COM, asciende, y ECI Telematics. PPTP utiliza el multi-protocol VPN, con 40-bit y el cifrado del 128-bit usando un protocolo llamado Microsoft Point-to-Point Encryption (MPPE). Es importante observar que PPTP en sí mismo no proporciona a la encripción de datos.**L2TP/IPsec** — L2TP comúnmente llamado sobre IPsec, esto proporciona a la Seguridad del Protocolo IPSec sobre el Tunelización del protocolo Layer 2 Tunneling Protocol (L2TP). L2TP es el producto de una sociedad entre los miembros del foro de PPTP, Cisco, y el Internet Engineering Task Force (IETF). Utilizado sobre todo para los VPN de accesos remotos con los sistemas operativos del Windows 2000, puesto que el Windows 2000 proporciona a un cliente de IPSec y L2TP nativo. Los proveedores de servicio de Internet pueden también proporcionar a las conexiones L2TP para dial-en los usuarios, y después cifran ese tráfico con IPsec entre su acceso-punta y el servidor de red de la oficina remota.

- **Integridad de datos** — Mientras que es importante que sus datos están cifrados sobre una red pública, están apenas como importantes verificar que no se han cambiado mientras que en el tránsito. Por ejemplo, IPsec tiene un mecanismo para asegurarse de que la porción encriptada del paquete, o la encabezado y la porción de datos enteras del paquete, no se ha tratado de forzar con. Si se detecta el tratar de forzar, se cae el paquete. La integridad de datos puede también implicar el autenticar del peer remoto.
- **Autenticación del origen de datos** — Es extremadamente importante verificar la identidad de la fuente de los datos se envían que. Esto es necesario guardar contra varios ataques que dependan de la falsificación la identidad del remitente.
- **Respuesta anti** — Ésta es la capacidad de detectar y rechazar los paquetes jugados de nuevo y las ayudas prevenga la falsificación.
- **Tunelización de datos/confidencialidad de flujo de tránsito** — El Tunelización es el proceso de encapsular un paquete entero dentro de otro paquete y de enviarlo sobre una red. La tunelización de datos es útil en caso de que sea deseable ocultar la identidad del dispositivo que origina el tráfico. Por ejemplo, un único dispositivo que utiliza IPsec encapsula el tráfico que pertenece a varios host detrás de él y agrega su propia encabezado encima de los paquetes existentes. Cifrando el paquete original y la encabezado (y encaminando el paquete basó en la encabezado adicional de la capa 3 agregada en el top), el dispositivo del Tunelización oculta con eficacia la fuente real del paquete. Solamente el par de confianza puede determinar la verdadera fuente, después de que elimine lejos la encabezado adicional y desencripte el encabezado original. Como se apunta en el RFC 2401 , "… el acceso de las características externas de comunicación también puede ser una preocupación en algunas circunstancias. La confidencialidad de flujo de tránsito es el servicio que dirige esta última preocupación encubriendo las direcciones de origen y de destino, la longitud del mensaje, o la frecuencia de comunicación. En el contexto de IPsec, usando la ESP en el modo túnel, especialmente en un gateway de seguridad, puede proporcionar a un cierto nivel de confidencialidad de flujo de tránsito."Todos los protocolos de encripción enumerados aquí

también utilizan el Tunelización como los medios de transferir los datos encriptados a través de la red pública. Es importante realizar que el hacer un túnel, en sí mismo, no proporciona a la seguridad de datos. El paquete original se encapsula simplemente dentro de otro protocolo y pudo todavía ser visible con un dispositivo de captura de paquetes si no cifrado. Se menciona aquí, sin embargo, puesto que es una parte integrante de cómo funcionan los VPN.El Tunelización requiere tres diversos protocolos.**Protocolo pasajero** — La información original (IPX, NetBeui, IP) se lleva que.**Encapsulando el protocolo** — El protocolo (GRE, IPsec, L2F, PPTP, L2TP) que se envuelve alrededor de las informaciones originales.**Protocolo de la portadora** — El protocolo usado por la red sobre la cual la información está viajando.El paquete original (protocolo pasajero) es interior encapsulado el protocolo de encapsulado, que entonces se pone dentro de la encabezado de protocolo de la portadora (generalmente IP) para la transmisión sobre la red pública. Observe que el protocolo de encapsulado también realiza muy a menudo el cifrado de los datos. Los protocolos tales como IPX y NetBeui, que no serían transferidos normalmente a través de Internet, pueden de forma segura y sin peligro ser transmitidos.Para los VPN de sitios a sitio, el protocolo de encapsulado es generalmente IPsec o Generic Routing Encapsulation (GRE). GRE incluye la información sobre qué tipo de paquete usted está encapsulando e información sobre la conexión entre el cliente y servidor.Para los VPN de accesos remotos, el hacer un túnel ocurre normalmente usando el Point-to-Point Protocol (PPP). La parte de la pila de TCP/IP, PPP es el portador para otros protocolos IP al comunicar sobre la red entre la computadora host y un sistema remoto. La tunelización PPP utilizará uno la expedición de la capa 2 PPTP, L2TP o de Cisco (L2F).

- **AAA** — La autenticación, la autorización, y las estadísticas se utiliza para más acceso seguro en un entorno del VPN de acceso remoto. Sin la autenticación de usuario, cualquier persona que se sienta en un laptop/PC con el software cliente VPN preconfigurado puede establecer una conexión segura en la red remota. Con la autenticación de usuario sin embargo, un nombre de usuario válido y una contraseña también tiene que ser ingresado antes de que se complete la conexión. Los nombres de usuario y contraseña se pueden salvar en el dispositivo sí mismo de la terminación VPN, o en un servidor AAA del externo, que puede proporcionar a la autenticación a numeroso otras bases de datos tales como Windows NT, Novell, LDAP, y así sucesivamente.Cuando una petición de establecer un túnel viene adentro de un cliente de marcado manual, el dispositivo VPN incita para un nombre de usuario y contraseña. Esto se puede entonces autenticar localmente o enviar al servidor AAA del externo, que controla:Quién usted es (autenticación)Qué a le se permite hacer (autorización)Qué usted lo hace realmente (las estadísticas)La información de la cuenta es especialmente útil para seguir el uso del cliente para los propósitos de la auditoría de seguridad, de la factura o de la información.
- **No repudiación** — En ciertas Transferencias de datos, especialmente ésos se relacionaron con las transacciones financieras, no repudiación son una característica altamente deseable. Esto es útil en la prevención de las situaciones donde un extremo niega el participar en una transacción. Como un banco requiere su firma antes de honrar su control, los trabajos de la no repudiación asociando una firma digital al mensaje enviado, así impidiendo la posibilidad del emisor que niega la participación en la transacción.

Varios protocolos existen que se pueden utilizar para construir una solución VPN. Todos estos protocolos proporcionan un cierto subconjunto de los servicios enumerados en este documento. La opción de un protocolo depende del conjunto de servicios deseado. Por ejemplo, una organización pudo ser cómoda con los datos que eran transferidos en el texto claro pero muy preocupados sobre mantener su integridad, mientras que otra organización pudo encontrar la

confidencialidad de los datos que mantenía absolutamente esencial. Su elección de protocolos pudo así ser diferente. ¿Para más información sobre los protocolos disponibles y sus fuerzas relativas, refiérase que la solución VPN correcta para usted?

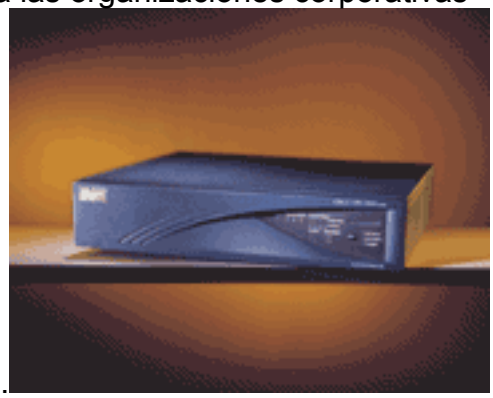
Productos VPN

De acuerdo con el tipo de VPN (Acceso Remoto o sitio-a-sitio), usted necesita establecer ciertos componentes para construir su VPN. Éstos pudieron incluir:

- Cliente de escritorio para cada usuario remoto
- Hardware dedicado tal como un Concentrador VPN de Cisco o un Firewall del Secure PIX de Cisco
- Servidor VPN dedicado para los servicios de marcado manual
- Servidor del acceso a la red (NAS) usado por el proveedor de servicio para el acceso del usuario remoto VPN
- Centro de la red privada y de la Administración de políticas

Porque no hay estándar extensamente validado para ejecutar un VPN, muchas compañías han desarrollado las soluciones mediante puesta a punto en sus los propio. Por ejemplo, Cisco ofrece varias soluciones VPN que incluyan:

- **Concentrador VPN** — Incorporando la mayoría de la encripción avanzado y de las técnicas de autenticación disponibles, los Concentradores VPN de Cisco se construyen específicamente para crear un Acceso Remoto o un VPN de sitio a sitio y se despliegan idealmente donde está el requisito para que un único dispositivo maneje un gran número de túneles VPN. El concentrador VPN fue desarrollado específicamente para dirigir el requisito para un especialmente diseñado, dispositivo del VPN de acceso remoto. Los concentradores proporcionan a la Alta disponibilidad, al rendimiento alto y a la capacidad de conversión a escala e incluyen los componentes, llamados los módulos del procesamiento de encripción Scalable (SEPT), que permiten a los usuarios aumentar fácilmente la capacidad y la producción. Los concentradores se ofrecen en los modelos convenientes para las Pequeñas empresas con 100 o menos usuarios de acceso remoto a las organizaciones corporativas grandes con hasta 10,000 usuarios remotos simultáneos.



- **Router VPN-activado Router/VPN-Optimized** — Todo el Routers de Cisco que ejecuta el software support de Cisco IOS® IPsec VPN. El único requisito es que el router debe funcionar con una imagen del Cisco IOS con el conjunto apropiado de la característica. La solución del Cisco IOS VPN utiliza completamente el Acceso Remoto, el intranet y los requisitos VPN de extranet. Esto significa que el Routers de Cisco puede trabajar igualmente bien cuando está conectado con un software cliente VPN corriente del host remoto o cuando está conectado con otro dispositivo VPN tal como un router, Firewall PIX o concentrador VPN. el Routers VPN-activado es apropiado para los VPN con los requisitos de la encripción moderada y del

Tunelización y proporciona los servicios VPN totalmente a través de las Características del Software Cisco IOS. Los ejemplos del Routers VPN-activado incluyen Cisco 1000, Cisco 1600, Cisco 2500, Cisco 4000, Cisco 4500, y las Cisco 4700 Series.Los routeres optimizados para VPN de Cisco proporcionan a la capacidad de conversión a escala, a la encaminamiento, a la Seguridad, y al Calidad de Servicio (QoS). Basan al Routers en el software del Cisco IOS, y hay un dispositivo conveniente para cada situación, del acceso del small office/home office (SOHO) con la agrupación VPN del central-sitio a las necesidades de la empresa a gran escala. Diseñan a los routeres optimizados para VPN para cumplir los altos requisitos del cifrado y del Tunelización y para hacer uso a menudo de la dotación física adicional tal como placas de encripción para alcanzar el rendimiento alto. Los ejemplos de los routeres optimizados para VPN incluyen Cisco 800, Cisco 1700, Cisco 2600, Cisco 3600,

Cisco7200, y las Cisco7500 Series.

- **Firewall del Secure PIX de Cisco** — El Firewall del private internet exchange (PIX) combina la traducción de la dirección, el servidor proxy, la filtración de paquetes, el Firewall, y las capacidades del VPN de la red dinámica en una pieza única de la dotación física. En vez de usar el software del Cisco IOS, este dispositivo tiene un sistema operativo altamente aerodinámico que negocie la capacidad de manejar una variedad de protocolos para la solidez extrema y el funcionamiento centrándose en el IP. Como con el Routers de Cisco, todos los modelos del Firewall PIX utilizan IPsec VPN. Todo se requiere que es que los requisitos para obtener la licencia de activar la característica VPN deben ser

cumplidos.

- **Clientes Cisco VPN** — Cisco ofrece a ambos clientes del hardware y software VPN. El Cliente Cisco VPN (software) viene liado con el concentrador de las 3000 Series de Cisco VPN sin costo adicional. Este cliente del software puede ser instalado en el equipo del host y ser utilizado para conectar con seguridad con el concentrador del sitio central (o a cualquier otro dispositivo VPN tal router o Firewall). El cliente de la dotación física VPN 3002 es una alternativa a desplegar el software cliente VPN en cada máquina y proporciona a la conectividad VPN a varios dispositivos.

La selección de dispositivos que usted utilizaría para construir su solución VPN es en última instancia un problema de diseño que depende de varios factores, incluyendo la producción deseada y el número de usuarios. Por ejemplo, en un sitio remoto con los pocos usuarios detrás de un PIX 501, usted podría considerar configurar el PIX existente como el punto final de VPN de IPsec, a condición de que usted valida la producción 501's 3DES áspero del 3 Mbps y el límite de

un máximo de 5 pares VPN. Por otra parte, en un sitio central la actuación como punto final de VPN para un gran número de túneles VPN, entrando para un router optimizado para VPN o un concentrador VPN sería probablemente una buena idea. La opción ahora dependería del tipo (LAN-a-LAN o Acceso Remoto) y del número de túneles VPN que son puestos. La amplia gama de dispositivos de Cisco que utilicen el VPN provee de los diseñadores de red una gran cantidad de flexibilidad y de una solución sólida para cubrir cada necesidad del diseño.

Información Relacionada

- Introducción a VPDN'
- Redes privadas virtuales (VPN)
- Página de soporte del Concentradores Cisco VPN de la serie 3000
- Página de soporte del VPN 3000 Client de Cisco
- Página de Soporte del Protocolo IKE/la Negociación de IPSec
- Página de soporte de los Firewall de la serie PIX 500
- RFC 1661: El Point-to-Point Protocol (PPP)
- RFC 2661: Layer Two Tunneling Protocol "L2TP"
- Cómo la materia trabaja: Cómo las redes privadas virtuales funcionan
- Descripción de los VPN
- Página VPN de Tom Dunigan
- Consorcio de Virtual Private Network
- Pedidos los comentarios (RFC)
- Soporte técnico - Cisco Systems