¿Qué solución VPN es la adecuada para usted?

Contenido

Introducción

Las redes privadas virtuales (VPN) se están tornando notablemente populares a un costo menor y de un modo más flexible para desplegar una red a través de un área ancha. Con los avances en la tecnología viene una variedad de opciones en aumento para implementar soluciones VPN. Esta nota técnica explica algunas de estas opciones y describe dónde podrían utilizarse mejor.

Antes de comenzar

Convenciones

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

prerrequisitos

No hay requisitos previos específicos para este documento.

Componentes Utilizados

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

Nota: Cisco también brinda soporte de encripción en plataformas que no son del IOS, incluyendo el Secure PIX Firewall de Cisco, el concentrador VPN 3000 de Cisco y el concentrador VPN 5000 de Cisco.

NAT

Internet ha experimentado el crecimiento explosivo en poco tiempo, lejos más que los diseñadores originales habrían podido prever. El número limitado de direcciones disponibles en IP versión 4.0 es una evidencia de este crecimiento, y el resultado es que el espacio de la dirección está cada vez menos disponible. La traducción de direcciones de red (NAT) es una solución a este problema.

Al usar NAT, un router se configura con límites internos/externos de tal manera que el externo (generalmente Internet) vea una o algunas direcciones registradas, mientras que el interno podría tener cualquier número de hosts con un esquema de direccionamiento privado. Para preservar la integridad del esquema de la traducción de dirección, NAT debe ser configurado en cada router de frontera entre la red (privada) interna y la red (pública) externa. Una de las ventajas de NAT desde el punto de vista de la seguridad es que los sistemas en la red privada no pueden recibir una conexión IP entrante de la red externa a menos que la gateway NAT esté configurada específicamente para permitir la conexión. Por otra parte, el NAT es totalmente transparente a los dispositivos de origen y de destino. La operación recomendada NAT implica el RFC 1918 , que delinea los esquemas de direccionamiento de la red privada apropiado. El estándar para el NAT se describe en el RFC1631 .

La figura siguiente muestra el definición del límite del router de NAT con una agrupación de direcciones de red de traducción interna.

El NAT se utiliza generalmente para conservar el routable de los IP Addresses en Internet, que son costosos y limitada en gran número. El NAT también proporciona la Seguridad ocultando la red interna de Internet.

Para la información sobre el trabajo del NAT, vea cómo el NAT trabaja.

Tunelización de la encapsulación GRE

Los túneles del Generic Routing Encapsulation (GRE) proporcionan una ruta específica a través de WAN compartido y encapsulan el tráfico con los nuevos encabezados de paquete para asegurar la salida a los destinos específicos. La red es privada porque el tráfico puede ingresar un túnel solamente en un punto final y puede irse solamente en el otro punto final. Los túneles no proporcionan la confidencialidad verdadera (como el cifrado hace) pero pueden llevar el tráfico encriptado. Los túneles son puntos finales lógicos configurados en las interfaces físicas a través de las cuales se lleva el tráfico.

Como se ilustra en el diagrama, la tunelización GRE se puede también utilizar para encapsular el tráfico no IP en el IP y para enviarlo sobre Internet o la red del IP. El Internet Packet Exchange (IPX) y los protocolos Appletalk son ejemplos del tráfico no IP. Para la información sobre configurar el GRE, vea “configurar una interfaz de túnel GRE” en configurar el GRE.

El GRE es la solución de VPN correcta para usted si usted tiene una red multiprotocolo como el IPX o el APPLETALK y tiene que enviar el tráfico sobre Internet o una red del IP. También, la encapsulación GRE se utiliza generalmente conjuntamente con los otros medios de asegurar el

tráfico, tal como IPSec.

Para más detalle técnicos en el GRE, refiera al RFC 1701 y al RFC 2784 .

Cifrado IPSec

La encripción de datos enviada a través de una red compartida es la tecnología VPN lo más a menudo posible asociada con los VPN. Cisco soporta los métodos de encripción de datos de la seguridad IP (IPSec). El IPSec es un marco de los estándares abiertos que proporciona la confidencialidad de los datos, la integridad de los datos, y la autenticación de datos entre los peeres participantes en la capa de red.

La encripción de IPSec es un estándar de la Fuerza de tareas de ingeniería en Internet (IETF) (IETF) que soporta los algoritmos de encripción de la clave simétrica del 168-bit del Data Encryption Standard (DES) 56-bit y del DES triple (3DES) en el software del cliente IPSec. La configuración de GRE es opcional con el IPSec. IPSec también admite autoridades de certificado y la negociación de Intercambio de clave de Internet (IKE). El encripción IPSec puede desplegarse en entornos autónomos entre clientes, routers y firewalls, o puede usarse junto con la tunelización L2TP en VPN de acceso. El IPSec se soporta adentro en las diversas plataformas de sistema operativo.

La encripción de IPSec es la solución de VPN correcta para usted si usted quiere la confidencialidad de los datos verdadera para sus redes. El IPSec es también un estándar abierto, así que la Interoperabilidad entre diversos dispositivos es fácil de implementar.

PPTP y MPPE

El Point-to-Point Tunneling Protocol (PPTP) fue desarrollado por el Microsoft; se describe en el RFC2637 . El PPTP se despliega extensamente en software de cliente de Windows 9x/ME, del Windows NT, y del Windows 2000, y de Windows XP para habilitar los VPN voluntarios.

El Cifrado punto a punto de Microsoft (MPPE) es un borrador IETF informativo que utiliza encripción de 40 ó 128 bits basado en RC4. El MPPE es solución de software del cliente PPTP de Microsoft de la parte de y es útil en arquitecturas de VPN de acceso voluntario-MODE. El PPTP/MPPE se soporta en la mayoría de las Plataformas de Cisco.

El soporte PPTP se agregó a la versión 12.0.5.XE5 de software del IOS de Cisco en las plataformas Cisco 7100 y 7200. Se incorporó compatibilidad para más plataformas en Cisco IOS 12.1.5.T. Cisco Secure PIX Firewall y el Concentrador VPN 3000 también incluyen soporte para las conexiones de cliente PPTP.

Puesto que el PPTP soporta las redes del no IP, es útil donde los usuarios remotos tienen que marcar adentro a la red corporativa para acceder las redes corporativas heterogéneas.

Para la información sobre configurar el PPTP, vea configurar el PPTP.

VPDN y L2TP

VPDN

El Virtual Private Dialup Network (VPDN) es un estándar de Cisco que permite que un servicio de marcado manual para red privada se expanda hacia servidores de acceso remoto. En el contexto de VPDN, el servidor de acceso (por ejemplo, un AS5300) al que se llama, generalmente se lo denomina Servidor de acceso a la red (NAS). El destino del usuario de dial in se refiere como el gateway de inicio (HGW).

El escenario básico es que un cliente de Point-to-Point Protocol (PPP) marca hacia un NAS local. El NAS determina que la sesión PPP debe ser remitida a un router del gateway de inicio para ese cliente. La HGW luego autentica al usuario y comienza la negociación PPP. Una vez finalizada la configuración de PPP, todas las tramas son enviadas a través de los NAS hacia el cliente y las gateways de inicio. Este método integra varios protocolos y conceptos.

Para la información sobre configurar el VPDN, vea *configurar una red de dial up de soldado virtual* en las características de Configurar directivo de seguridad.

L2TP

El Protocolo de tunelización de Capa 2 (L2TP) es un estándar IETF que incorpora los mejores atributos de PPTP y L2F. Los túneles L2TP se utilizan principalmente en modo obligatorio (es decir, NAS de marcado hacia HGW) para acceder a los VPN tanto para el tráfico IP como no IP. Windows 2000 y Windows XP agregaron compatibilidad nativa con este protocolo como medio de conexión de cliente VPN.

El L2TP se utiliza para hacer un túnel el PPP sobre una red pública, tal como Internet, usando el IP. Puesto que el túnel ocurre en la capa 2, los protocolos de la capa superiores son ignorantes del túnel. Como el GRE, el L2TP puede también encapsular cualquier protocolo de la capa 3. El puerto 1701 UDP es utilizado para enviar el tráfico L2TP por el iniciador del túnel.

Nota: En 1996 Cisco creó un protocolo de la expedición de la capa 2 (L2F) para permitir que las conexiones VPDN ocurran. L2F todavía es compatible con otras funciones pero ha sido reemplazado por L2TP. El protocolo de tunelización punto a punto (PPTP) también se creó en 1996 basado en un borrador de Internet de IETF. PPTP proporcionó una función similar al protocolo de túnel similar a GRE para conexiones PPP.

Para más información sobre el L2TP, vea el Tunnel Protocol de la capa 2.

PPPoE

El PPP over Ethernet (PPPoE) es un RFC informativo que se despliega sobre todo en los entornos del Digital Subscriber Line (DSL). PPPoE aprovecha las infraestructuras Ethernet para permitir a los usuarios iniciar sesiones PPP múltiples dentro de la misma LAN. Esta tecnología permite la selección del servicio de capa 3, una aplicación emergente que permite a los usuarios conectarse simultáneamente a varios destinos a través de una sola conexión de acceso remoto. El PPPoE con el protocolo password authentication (PAP) o el Challenge Handshake Authentication Protocol (CHAP) es de uso frecuente informar al sitio central qué routeres remotos están conectados con él.

El PPPoE se utiliza sobre todo en las instalaciones de DSL del proveedor de servicio y las topologías de los Bridged Ethernet.

Para más información sobre configurar el PPPoE, vea configurar el PPPoE sobre los Ethernetes y

el VLA N del IEEE 802.1Q.

MPLS VPN

El Multiprotocol Label Switching (MPLS) es una nueva norma IETF basada en Cisco Tag Switching que permite el aprovisionamiento automatizado, un desarrollo rápido y características de escalabilidad que los proveedores necesitan para suministrar acceso a la intranet y servicios de extranet VPN económicos. Cisco está trabajando de cerca con los proveedores de servicio para asegurar una transición fluida a los servicios habilitados para MPLS VPN. MPLS funciona sobre un paradigma basado en etiquetas y etiqueta paquetes a medida que ingresan a la red del proveedor, a fin de acelerar el reenvío a través de un núcleo IP sin conexión. El MPLS utiliza los Route Distinguisher para identificar la pertenencia a VPN y para contener el tráfico dentro de una comunidad VPN.

El MPLS también agrega las ventajas de un acercamiento orientado a la conexión al paradigma del Routing IP, a través del establecimiento de trayectorias conmutadas de etiquetas, que se crean sobre la base del flujo de tráfico de la información de topología bastante entonces. El MPLS VPN se despliega extensamente en el entorno del proveedor de servicios.

Para la información sobre configurar el MPLS VPN, vea configurar un MPLS VPN básico.

Información Relacionada

- Página de soporte de IPSec
- Cómo las Redes privadas virtuales funcionan
- Página de Soporte de NAT
- Página de soporte GRE
- Página de soporte VPDN
- Página de soporte de PPTP
- Página del Soporte de PPPoE
- Soporte Técnico - Cisco Systems