Descripción general y prácticas recomendadas de VPN de los routers Cisco RV

Objetivo

El objetivo de este documento es ofrecer una descripción general de las prácticas recomendadas de la red privada virtual (VPN) a cualquier persona nueva en los routers de la serie Cisco RV.

Table Of Contents

Introducción

Parece que hace tanto tiempo que el único lugar donde se podía trabajar era en la oficina. Tal vez recuerden, en su día, tener que ir a la oficina el fin de semana para resolver un asunto de trabajo. No había otra forma de obtener datos de los recursos de la empresa a menos que estuviera físicamente en la oficina. Esos días han terminado. En la actualidad, puede estar fuera de casa, haciendo negocios desde casa, desde otra oficina, desde una cafetería o incluso desde otro país. La desventaja es que los hackers siempre buscan obtener sus datos confidenciales. No es seguro utilizar Internet público. ¿Qué puede hacer para obtener flexibilidad y seguridad? Configure una VPN.

Una conexión VPN permite a los usuarios acceder, enviar y recibir datos desde y hacia una red privada a través de una red pública o compartida como Internet, pero sigue garantizando una conexión segura a una infraestructura de red subyacente para proteger la red privada y sus

recursos.

Un túnel VPN establece una red privada que puede enviar datos de forma segura mediante el cifrado para codificar los datos, y la autenticación para garantizar la identidad del cliente. Las oficinas corporativas a menudo utilizan una conexión VPN, ya que es útil y necesario permitir que sus empleados tengan acceso a su red privada incluso si se encuentran fuera de la oficina.

Normalmente, las VPN de sitio a sitio conectan redes enteras entre sí. Amplían una red y permiten que los recursos informáticos de una ubicación estén disponibles en otras ubicaciones. Mediante el uso de un router compatible con VPN, una empresa puede conectar varios sitios fijos a través de una red pública como Internet.

La configuración de cliente a sitio para una VPN permite a un host remoto, o cliente, actuar como si se encontraran en la misma red local. Se puede configurar una conexión VPN entre el router y un terminal después de que el router se haya configurado para la conexión a Internet. El cliente VPN depende de la configuración del router VPN, además del requisito de que la configuración coincida para establecer una conexión. Además, algunas de las aplicaciones cliente VPN son específicas de la plataforma, y también dependen de la versión del sistema operativo (SO). La configuración debe ser exactamente la misma o no se pueden comunicar.

Una VPN se puede configurar con cualquiera de los siguientes elementos:

- Secure Socket Layer (SSL)
- Seguridad de protocolo de Internet (IPSec)
- Protocolo de túnel de punto a punto (PPTP): no es tan seguro como SSL o IPSec
- Encapsulación de routing genérico (GRE)
- Protocolo de túnel de capa 2 (L2TP)

Si nunca ha configurado una VPN antes, recibirá mucha información nueva en este artículo. No se trata de una guía paso a paso, sino más bien de una descripción general a modo de referencia. Por lo tanto, sería beneficioso leer este artículo en su totalidad antes de continuar e intentar configurar una VPN en su red. En este artículo se proporcionan vínculos para pasos específicos.

Cisco no admite productos de terceros que no sean de Cisco, como TheGreenBow, OpenVPN, Shrew Soft y EZ VPN. Se incluyen estrictamente con fines de orientación. Si necesita asistencia sobre estos temas más allá del artículo, debe ponerse en contacto con el tercero para obtener asistencia.

Ventajas de utilizar una conexión VPN

- El uso de una conexión VPN ayuda a proteger los datos y recursos confidenciales de la red.
- Proporciona comodidad y accesibilidad para los trabajadores remotos o empleados

corporativos, ya que podrán acceder fácilmente a los recursos de la oficina principal sin tener que estar físicamente presentes y, sin embargo, mantener la seguridad de la red privada y sus recursos.
- La comunicación mediante una conexión VPN proporciona un mayor nivel de seguridad en comparación con otros métodos de comunicación remota. Esto es posible gracias a un avanzado algoritmo de cifrado, que protege la red privada contra el acceso no autorizado.
- Las ubicaciones geográficas reales de los usuarios están protegidas y no expuestas a redes públicas o compartidas como Internet.
- Una VPN permite agregar nuevos usuarios o grupos de usuarios sin necesidad de componentes adicionales o una configuración complicada.

Riesgos del uso de una conexión VPN

- Puede haber riesgos de seguridad debido a una configuración incorrecta. Dado que el diseño y la implementación de una VPN pueden ser complicados, es necesario confiar la tarea de configurar la conexión a un profesional experto y experimentado para asegurarse de que la seguridad de la red privada no se vea comprometida.
- Puede ser menos fiable. Dado que una conexión VPN requiere una conexión a Internet, es importante contar con un proveedor con una reputación probada para proporcionar un excelente servicio de Internet y garantizar un tiempo de inactividad mínimo o nulo.
- Si se produce una situación en la que es necesario añadir una nueva infraestructura o un nuevo conjunto de configuraciones, pueden surgir problemas técnicos debido a la incompatibilidad, especialmente si se trata de productos o proveedores diferentes de los que ya está utilizando.
- Se pueden producir velocidades de conexión lentas. Si utiliza una conexión ISP que proporciona un servicio VPN gratuito, es probable que la conexión también sea lenta, ya que estos proveedores no dan prioridad a las velocidades de conexión. Es importante tener en cuenta que el rendimiento de VPN depende de las capacidades de hardware del router.

Para obtener más información sobre cómo funcionan las VPN, haga clic aquí.

Sugerencias para utilizar al configurar una VPN

1. Utilice una subred IP de LAN diferente en ambos extremos mientras configura la VPN entre diferentes sitios. Por ejemplo, si el sitio al que se conecta utiliza un esquema de direcciones 192.168.x.x, debería utilizar una subred 10.x.x.x o 172.16.x.x - 172.31.x.x. Otra opción sería tener diferentes máscaras de subred. Al cambiar la dirección IP del router, los dispositivos del protocolo de configuración dinámica de host (DHCP) seleccionarán automáticamente una dirección IP de la subred.
2. Utilice la IP pública estática en la interfaz WAN del router para una conectividad VPN estable.
3. Asegúrese de que el nivel de cifrado y autenticación seleccionado es el mismo que el router al que desea establecer un túnel VPN para la VPN.
4. Asegúrese de que PSK y Key Lifetime especificados sean los mismos que los del router remoto. Una PSK puede ser lo que usted quiera que sea, solo tiene que coincidir en el sitio

y con el cliente cuando se configuran como cliente en su computadora. Dependiendo del dispositivo, puede haber símbolos prohibidos que no pueda utilizar. La duración de la clave es la frecuencia con que el sistema cambia la clave. Se prefiere un certificado porque se considera más seguro.
5. Para la mayoría de las VPN, los clientes no necesitan un certificado para utilizar una VPN, es solo para la verificación a través del router. Por ejemplo, OpenVPN requiere certificados de cliente y de sitio.
6. Establezca su vida útil de SA en la Fase I más tiempo que su vida útil de SA de Fase II. Si hace que su fase I sea más corta que la fase II, tendrá que renegociar el túnel de ida y vuelta con frecuencia en lugar del túnel de datos. Un túnel de datos necesita más seguridad, por lo que es mejor tener una vida útil en la fase II más corta que la fase I.
7. Cambie todas las contraseñas por otras más complejas.

Tipos de VPN

Capa de sockets seguros (SSL)

Los routers Cisco serie RV34x admiten una VPN SSL mediante AnyConnect. El RV160 y el RV260 tienen la opción de utilizar OpenVPN, que es otra VPN SSL. El servidor VPN SSL permite a los usuarios remotos establecer un túnel VPN seguro mediante un navegador web. Esta función permite un acceso sencillo a una amplia gama de recursos web y aplicaciones habilitadas para la Web mediante la compatibilidad nativa con el explorador de protocolo de transferencia de hipertexto (HTTP) sobre protocolo de transferencia de hipertexto seguro (HTTPS) SSL.

La VPN SSL permite a los usuarios acceder de forma remota a redes restringidas, utilizando una ruta segura y autenticada mediante el cifrado del tráfico de red.

Existen dos opciones para configurar el acceso en SSL:

1. Certificado autofirmado: certificado firmado por su propio creador. Esto no se recomienda y sólo se debe utilizar en un entorno de prueba.
2. Certificado firmado por la CA: es mucho más seguro y se recomienda encarecidamente. Por una cuota, un tercero valida que la red es legítima y crea un certificado de CA que luego se adjunta al sitio. Para obtener más información sobre los certificados de CA, consulte la sección Certificados de este artículo.

Hay enlaces a artículos sobre AnyConnect en este documento. Para obtener una descripción general de AnyConnect, haga clic aquí.

Perfil IPsec

Easy VPN (EZVPN), TheGreenBow y Shrew Soft son VPN de seguridad de protocolo de Internet (IPSec). Las VPN IPSec proporcionan túneles seguros entre dos iguales o de un cliente a un sitio. Los paquetes que se consideran sensibles deben enviarse a través de estos túneles seguros. Los parámetros que incluyen el algoritmo hash, el algoritmo de cifrado, la duración de la clave y el modo deben utilizarse para proteger estos paquetes sensibles y deben definirse especificando las

características de estos túneles. Luego, cuando el peer IPSec ve un paquete tan sensible, configura el túnel seguro apropiado y envía el paquete a través de este túnel al peer remoto.

Cuando IPsec se implementa en un firewall o un router, proporciona una seguridad sólida que se puede aplicar a todo el tráfico que cruza el perímetro. El tráfico dentro de una empresa o grupo de trabajo no incurre en la sobrecarga del procesamiento relacionado con la seguridad.

Para que los dos extremos de un túnel VPN se cifren y se establezcan correctamente, ambos deben acordar los métodos de cifrado, descifrado y autenticación. El perfil IPsec es la configuración central en IPsec que define los algoritmos como el cifrado, la autenticación y el grupo Diffie-Hellman (DH) para la negociación de las fases I y II en modo automático y en modo de clave manual.

Entre los componentes importantes de IPsec se incluyen las fases 1 y 2 del intercambio de claves de Internet (IKE).

El objetivo básico de la fase uno de IKE es autenticar los pares IPSec y configurar un canal seguro entre los pares para habilitar los intercambios IKE. La fase uno de IKE realiza las siguientes funciones:

- Autentica y protege las identidades de los pares IPSec
- Negocia una directiva de asociaciones de seguridad (SA) IKE coincidente entre pares para proteger el intercambio IKE
- Realiza un intercambio Diffie-Hellman autenticado con el resultado final de tener claves secretas compartidas coincidentes
- Configura un túnel seguro para negociar los parámetros de fase dos de IKE
- Se produce en dos modos: modo principal y modo agresivo

El propósito de la fase dos de IKE es negociar las SA de IPSec para configurar el túnel IPSec. La fase dos de IKE realiza las siguientes funciones:

- Negocia los parámetros de SA IPSec protegidos por una SA IKE existente
- Establece asociaciones de seguridad IPSec
- Renegocia periódicamente las SA de IPSec para garantizar la seguridad
- Realiza opcionalmente un intercambio Diffie-Hellman adicional
- Sólo se utiliza un modo, modo rápido

Si se especifica Confidencialidad directa perfecta (PFS) en la directiva IPSec, se realiza un nuevo intercambio DH con cada modo rápido, lo que proporciona material de claves con una entropía (vida del material de claves) mayor y, por tanto, mayor resistencia a los ataques criptográficos. Cada intercambio DH requiere grandes exponenciaciones, lo que aumenta el uso de la CPU y exige un coste de rendimiento.

- Configuración del perfil de seguridad de protocolo de Internet (IPSec) en un router serie RV34x
- Configuración de perfiles IPSec (modo de creación automática de claves) en el RV160 y el RV260
- Configuración del modo de creación manual de claves del perfil IPsec en los routers RV160

y RV260

Protocolo de Tunelización punto a Punto (PPTP)

PPTP es un protocolo de red utilizado para crear túneles VPN entre redes públicas. Los servidores PPTP también se conocen como servidores de red de marcación telefónica privada virtual (VPDN). PPTP se utiliza a veces sobre otros protocolos porque es más rápido y tiene la capacidad de trabajar en dispositivos móviles. Sin embargo, es importante tener en cuenta que no es tan seguro como otros tipos de VPN. Existen varios métodos para conectar con cuentas de tipo PPTP. Haga clic en los enlaces para obtener más información:

- Configuración de un servidor de protocolo de tunelación punto a punto (PPTP) en el router serie Rv34x
- Configuración del servidor de protocolo de túnel punto a punto (PPTP) en las series de routers VPN RV320 y RV325 en Windows

Encapsulación de routing genérico

La encapsulación de enrutamiento genérico (GRE) es un protocolo de tunelación que proporciona un enfoque genérico simple para transportar paquetes de un protocolo a través de otro protocolo mediante encapsulación.

GRE encapsula una carga útil, es decir, un paquete interno que debe entregarse a una red de destino dentro de un paquete IP externo. El túnel GRE se comporta como un link punto a punto virtual que tiene dos puntos finales identificados por la dirección de origen y destino del túnel.

Los terminales de túnel envían cargas útiles a través de túneles GRE mediante el enrutamiento de paquetes encapsulados a través de redes IP intervinientes. Otros routers IP en el camino no analizan la carga útil (el paquete interno); solo analizan el paquete IP externo a medida que lo reenvían hacia el punto final del túnel GRE. Al llegar al extremo del túnel, se elimina la encapsulación GRE y la carga útil se reenvía al destino final del paquete.

La encapsulación de datagramas en una red se realiza por varias razones, como cuando un servidor de origen desea influir en la ruta que toma un paquete para alcanzar el host de destino. El servidor de origen también se conoce como servidor de encapsulación.

La encapsulación IP en IP implica la inserción de un encabezado IP externo sobre el encabezado IP existente. La dirección de origen y de destino en el encabezado IP externo apuntan a los puntos finales del túnel IP en IP. La pila de encabezados IP se utiliza para dirigir el paquete a través de una trayectoria predeterminada hacia el destino, siempre que el administrador de la red conozca las direcciones de loopback de los routers que transportan el paquete.

Este mecanismo de tunelización se puede utilizar para determinar la disponibilidad y la latencia de la mayoría de las arquitecturas de red. Cabe señalar que no es necesario incluir en los encabezados la ruta completa desde el origen hasta el destino, pero se puede elegir un segmento de la red para dirigir los paquetes.

Protocolo de tunelización de capa 2

L2TP no proporciona mecanismos de encripción para el tráfico que tuneliza. En su lugar, se basa en otros protocolos de seguridad, como IPSec, para cifrar los datos.

Se establece un túnel L2TP entre el L2TP Access Concentrator (LAC) y el L2TP Network Server (LNS). También se establece un túnel IPSec entre estos dispositivos y todo el tráfico del túnel L2TP se cifra mediante IPSec.

Algunos términos clave con L2TP:

- CHAP - Protocolo de autenticación por desafío mutuo. Protocolo de autenticación punto a punto (PPP).
- Concentrador de acceso L2TP (LAC): Un LAC puede ser un servidor de acceso a la red de Cisco conectado a la red telefónica pública conmutada (PSTN). El LAC sólo necesita implementar medios para el funcionamiento sobre L2TP. Un LAC puede conectarse al LNS usando una red de área local o una red de área extensa como Frame Relay público o privado. El LAC es el iniciador de las llamadas entrantes y el receptor de las llamadas salientes.
- Servidor de red L2TP (LNS): casi cualquier router de Cisco conectado a una red de área local o de área extensa, como Frame Relay público o privado, puede actuar como LNS. Es el lado del servidor del protocolo L2TP y debe funcionar en cualquier plataforma que termine las sesiones PPP. El LNS es el iniciador de las llamadas salientes y el receptor de las llamadas entrantes. La figura 1 muestra la rutina de llamada entre LAC y LNS.
- Red de marcado privado virtual (VPDN): tipo de VPN de acceso que utiliza PPP para prestar el servicio.

Si desea obtener más información sobre L2TP, haga clic en los siguientes enlaces:

- Configuración de los parámetros WAN L2TP en el router RV34x
- Guía de configuración de redes de área extensa: servicios de capa 2, Cisco IOS XE versión 3S

VPN compatibles con los routers VPN de la serie RV de Cisco

	RV34X	RV32X	RV160X/RV260X
IPSec (IKEv1)			
ShrewSoft	Yes	Yes	Yes
Arco Verde	Yes	Yes	Yes
Cliente integrado en Mac	Yes	Yes	No
iPhone/iPad	Yes	Yes	No
Android	Yes	Yes	Yes
L2TP/IPSec	Sí (PAP)	No	No

PPTP (Protocolo de arquitectura de túneles punto a punto)	Sí (PAP)	Sí*	Sí (PAP)
Otro			
AnyConnect	Yes	No	No
Openvpn	No	Yes	Yes
IKEv2			
Windows:	Sí*	No	Sí*
Mac	Yes	No	Yes
iPhone	Yes	No	Yes
Android	Yes	No	Yes

Tecnología VPN	Dispositivos compatibles	Clientes admitidos*	Detalles y advertencias
IPSec (IKEv1)	RV34X, RV32X, RV160X/RV260X	Nativo: Mac, iPhone, iPad, Android Otros: EasyVPN (Cisco VPN Client), ShrewSoft, Greenbow	Fácil de configurar, solucionar problemas y ofrecer asistencia. Está disponible en todos los routers, es fácil de configurar (en su mayor parte), tiene el mejor registro para resolver problemas. Además, incluye la mayoría de dispositivos. Es por esto que normalmente recomendamos ShrewSoft (libre y funciona) y Greenbow (no libre, pero funciona). Para Windows, tenemos los clientes ShrewSoft y Greenbow como opciones, ya que Windows no tiene un cliente VPN nativo IPSec puro. Para ShrewSoft y Greenbow, está un poco más involucrado, pero no es difícil. Una vez configurados por primera vez, los perfiles de cliente se pueden exportar e importar en otros clientes. En el caso de los routers RV160X/RV260X, puesto que no disponemos de la opción Easy VPN, tenemos que utilizar la opción Cliente de terceros, que no funciona con Mac, iPhone o iPad. Sin embargo, podemos configurar clientes de ShrewSoft, Greenbow y Android para que se conecten. Para clientes Mac, iPhone y iPad, recomiendo IKEv2 (ver a continuación).
AnyConnect	RV34X	Windows,	Algunos clientes solicitan una solución

		Mac, iPhone, iPad y Android	completa de Cisco y ya está. Es fácil de configurar, tiene registro, pero puede ser difícil entender los registros. Requiere licencias de cliente obligatorias en función de los costes. Se trata de una solución completa de Cisco y está actualizada. La resolución de problemas no es tan sencilla como IPSec, pero es mejor que las demás opciones de VPN.
L2TP/IPSec	RV34X	Nativo: Windows	Esto es lo que recomendaré a los clientes que necesiten utilizar el cliente VPN integrado en Windows. Dos advertencias con esto son: 1. Solo admitimos la autenticación PAP cuando utilizamos la autenticación local. Tenemos que ir a cada cliente y seleccionar el cifrado opcional o no, desactivar las opciones MS-CHAP y habilitar PAP. Esto significa que el nombre de usuario/contraseña se envía en el clear. No es gran cosa, ya que todo está cifrado con IPSec y debe configurarse en cada cliente. En Windows, esto es configurable, pero no en dispositivos Mac, iPhone, iPad o Android, por lo que realmente solo pueden ser utilizados por clientes de Windows a menos que tengan un servidor de autenticación externo como Radius o LDAP. 2. Si el router está detrás de un dispositivo NAT, la conexión fallará en las máquinas Windows. La solución alternativa es crear una clave de registro en cada cliente para permitir NAT tanto en el cliente como en el router.
IPSec (IKEv2)	RV34X, RV160X/RV260X	Nativo: Windows, Mac, iPhone, iPad, Android	El cliente nativo de Windows para IKEv2 requiere autenticación de certificado, lo que requiere una infraestructura PKI, ya que tanto el router como todos los clientes necesitan tener certificados de la misma CA (u otra CA de confianza). Para aquellos que quieren utilizar IKEv2, lo configuramos para sus dispositivos Mac, iPhone, iPad y Android y normalmente configuramos IKEv1 para sus máquinas

			Windows (ShrewSoft, Greenbow o L2TP/IPSec).
VPN abierta	RV32X, RV160X/RV260X	Open VPN es el cliente	Difícil de configurar, difícil de resolver problemas y soporte. Compatible con RV160X/RV260X y RV320. La configuración es más compleja que la de IPSec o AnyConnect, especialmente si utilizan certificados, cosa que sucede en la mayoría de los casos. La resolución de problemas es más difícil ya que no tenemos registros útiles en el router y dependemos de los registros del cliente. Además, las actualizaciones de la versión del cliente OpenVPN han cambiado sin previo aviso los certificados que aceptaron. Además, descubrimos que esto no funciona en Chromebooks y tuvimos que recurrir a una solución IPSec.

* Probamos tantas combinaciones como podemos, si hay una combinación específica de hardware/software, por favor, diríjase aquí. De lo contrario, consulte la guía de configuración relacionada por dispositivo para ver la versión probada más reciente.

Certificados

¿Ha visitado alguna vez un sitio web y se le ha advertido de que no es seguro? No le infunde la confianza de que su información privada está segura, ¡pero no lo está! Si un sitio es seguro, verá un icono de candado cerrado antes del nombre del sitio. Este es un símbolo de que el sitio se ha comprobado que es seguro. Debe asegurarse de que el icono de candado está cerrado. Lo mismo es cierto para su VPN.

Al configurar una VPN, debe obtener un certificado de una autoridad de certificación (CA). Los certificados se adquieren de sitios de terceros y se utilizan para la autenticación. Es una manera oficial de probar que su sitio es seguro. Básicamente, la CA es una fuente de confianza que verifica que usted es una empresa legítima y que se puede confiar en usted. Para una VPN solo necesita un certificado de nivel inferior a un costo mínimo. La CA lo revisa y, una vez que verifica su información, le emitirá el certificado. Este certificado se puede descargar como un archivo en su equipo. A continuación, puede acceder al router (o servidor VPN) y cargarlo allí.

La CA utiliza la infraestructura de clave pública (PKI) al emitir certificados digitales, que utiliza la clave pública o el cifrado de clave privada para garantizar la seguridad. Las CA son responsables de administrar las solicitudes de certificados y emitir certificados digitales. Algunas CA de terceros incluyen IdenTrust, Comodo, GoDaddy, GlobalSign, GeoTrust y Verisign.

Es importante que todos los gateways de una VPN utilicen el mismo algoritmo; de lo contrario, no podrán comunicarse. Para simplificar las cosas, se recomienda que todos los certificados se compren del mismo tercero de confianza. De este modo, es más fácil administrar varios certificados, ya que deben renovarse manualmente.

Nota: Los clientes normalmente no necesitan un certificado para utilizar una VPN; es solo para la verificación a través del router. Una excepción a esto es OpenVPN, que requiere un certificado de cliente.

Algunas pequeñas empresas optan por utilizar una contraseña o una clave previamente compartida en lugar de un certificado para simplificar el proceso. Esto es menos seguro, pero se puede configurar sin coste alguno.

Puede encontrar más información sobre los certificados en los siguientes enlaces:

- Certificado (Importar/Exportar/Generar CSR) en el router de las series RV160 y RV260
- Reemplace el certificado autofirmado predeterminado por un certificado SSL de terceros en el router serie RV34x

VPN de sitio a sitio en un router

Para el router local y remoto, es importante asegurarse de que la clave precompartida (PSK)/contraseña/certificado utilizados para la conexión VPN y la configuración de seguridad coincidan. Si uno o más routers utilizan Traducción de direcciones de red (NAT), que utilizan la mayoría de los routers de la serie Cisco RV, deberá aplicar exenciones de firewall para la conexión VPN en el router local y remoto.

Consulte estos artículos de sitio a sitio para obtener más información:

- Configuración de VPN de sitio a sitio en el RV34x
- Configuración de una VPN de sitio a sitio en un router RV340 o RV345
- Charla técnica de Cisco: Configuración de VPN de sitio a sitio en routers de la serie RV340 (vídeo)
- Configuración de VPN de sitio a sitio en un router RV160 y RV260 (parámetros básicos)
- VPN de sitio a sitio en los routers RV160 y RV260 (configuración avanzada y conmutación por fallo)

VPN de cliente a sitio en un router

Antes de poder configurar una VPN en el lado del cliente, un administrador debe configurarla en el router.

Haga clic para ver estos artículos de configuración del router:

- Configuración del asistente de configuración de VPN en los routers RV160 y RV260
- Configuración de Shrew Soft VPN Client con el RV160 y el RV260

- Cisco Tech Talk: Configuración de Shrew Soft VPN en RV160 y RV260 (vídeo)
- Configuración y uso de GreenBow IPsec VPN Client para conectar con routers RV160 y RV260

Crear un perfil de cliente a sitio

En una conexión VPN de cliente a sitio, los clientes de Internet pueden conectarse al servidor para acceder a la red corporativa o LAN detrás del servidor, pero mantener la seguridad de la red y sus recursos. Esta función es muy útil, ya que crea un nuevo túnel VPN que permitiría a los teletrabajadores y a los viajeros de negocios acceder a su red mediante un software cliente de VPN sin poner en peligro la privacidad y la seguridad. Los siguientes artículos son específicos de los routers de la serie RV34x:

- Configuración de la conexión de red privada virtual (VPN) de cliente a sitio en el router serie RV34x
- Configure la conectividad de la red privada virtual (VPN) AnyConnect en el router de la serie RV34x

La VPN de cliente a sitio no funcionará si el reenvío de puertos está configurado para Todo el tráfico de origen y Todo el tráfico de destino.

Grupos de usuarios

Los grupos de usuarios se crean en el router para una colección de usuarios que comparten el mismo conjunto de servicios. Estos grupos de usuarios incluyen opciones para el grupo, como una lista de permisos sobre cómo pueden acceder a la VPN. Dependiendo del dispositivo, se puede permitir PPTP, VPN IPSec de sitio a sitio y VPN IPSec de cliente a sitio. Por ejemplo, el RV260 tiene opciones que incluyen OpenVPN, pero no se admite L2TP. La serie RV340 está equipada con AnyConnect para SSL VPN, así como con Captive Portal o EZ VPN.

Esta configuración permite a los administradores controlar y filtrar de modo que sólo los usuarios autorizados puedan acceder a la red. Shrew Soft y TheGreenBow son dos de los clientes VPN más comunes disponibles para descargar. Deben configurarse en función de los parámetros de VPN del router para poder establecer correctamente un túnel VPN. El siguiente artículo se refiere específicamente a la creación de un grupo de usuarios:

- Creación de un grupo de usuarios para la configuración de VPN en el router RV34x

Al configurar grupos de usuarios para una VPN, asegúrese de dejar la cuenta de administrador predeterminada en el grupo de administradores y crear una nueva cuenta de usuario y grupo de usuarios para VPN. Si mueve su cuenta de administrador a un grupo diferente, no podrá iniciar sesión en el router. Como resultado, tendría que hacer un restablecimiento de fábrica y volver a configurar para ese router, dejando la cuenta de administrador predeterminada en el grupo de administración solo.

Cuentas de usuario

Las cuentas de usuario se crean en el router para permitir la autenticación de usuarios locales mediante la base de datos local para varios servicios como PPTP, VPN Client, inicio de sesión en la interfaz gráfica de usuario (GUI) web y red privada virtual de capa de sockets seguros (SSLVPN). Esto permite a los administradores controlar y filtrar los usuarios autorizados sólo para acceder a la red. El siguiente artículo se refiere específicamente a la creación de una cuenta de usuario:

- Creación de una cuenta de usuario para la configuración del cliente VPN en el router RV34x

Cliente a sitio en la ubicación del cliente

En una conexión VPN de cliente a sitio, los clientes de Internet pueden conectarse al servidor para acceder a la red corporativa o LAN detrás del servidor, pero conservan la seguridad de la red y sus recursos. Esta función es muy útil ya que crea un nuevo túnel VPN que permite a los teletrabajadores y viajeros de negocios acceder a su red mediante un software cliente VPN sin poner en peligro la privacidad y la seguridad. La VPN está configurada para cifrar y descifrar datos a medida que se envían y reciben.

La aplicación AnyConnect funciona con SSL VPN y se utiliza específicamente con los routers RV34x. No está disponible con otras series de routers RV. A partir de la versión 1.0.3.15, ya no es necesaria una licencia de router, pero es necesario adquirir licencias para el cliente de la VPN. Para obtener más información sobre Cisco AnyConnect Secure Mobility Client, haga clic aquí. Para obtener instrucciones sobre la instalación, seleccione uno de los siguientes artículos:

- Instalación de Cisco AnyConnect Secure Mobility Client en una computadora Mac
- Instalación de Cisco AnyConnect Secure Mobility Client en una computadora con Windows

Hay algunas aplicaciones de terceros que se pueden utilizar para VPN de cliente a sitio con todos los routers de la serie RV. Como se ha indicado anteriormente, Cisco no es compatible con estas aplicaciones; esta información se proporciona con fines orientativos.

GreenBow VPN Client es una aplicación de cliente VPN de terceros que hace posible que un dispositivo host configure una conexión segura para el túnel IPsec o SSL de cliente a sitio. Se trata de una aplicación de pago que incluye asistencia.

- Configuración y uso de GreenBow IPsec VPN Client para conectar con routers RV160 y RV260

OpenVPN es una aplicación gratuita de código abierto que se puede configurar y utilizar para una VPN SSL. Utiliza una conexión cliente-servidor para proporcionar comunicaciones seguras entre un servidor y una ubicación de cliente remoto a través de Internet.

- OpenVPN en routers RV160 y RV260

Shrew Soft es una aplicación gratuita de código abierto que se puede configurar y utilizar para una VPN IPsec también. Utiliza una conexión cliente-servidor para proporcionar comunicaciones seguras entre un servidor y una ubicación de cliente remoto a través de Internet.

- Configuración de Shrew Soft VPN Client con el RV160 y el RV260

Easy VPN se utilizaba habitualmente en los routers RV32x. A continuación se incluye información para referencia:

- Configuración de una red privada virtual (VPN) de cliente sencillo a puerta de enlace en los routers VPN RV320 y RV325
- Preguntas y respuestas sobre Cisco Easy VPN
- Easy VPN en routers basados en software Cisco IOS

Asistente de configuración

Los routers de la serie RV de Cisco más recientes incluyen un asistente de configuración de VPN que le guía a través de los pasos de configuración. El asistente de configuración de VPN le permite configurar conexiones VPN básicas de LAN a LAN y de acceso remoto, así como asignar claves previamente compartidas o certificados digitales para la autenticación. Consulte estos artículos para obtener más información:

- Configuración del asistente de configuración de VPN en el RV160 y el RV260
- Configuración de la conexión de red privada virtual (VPN) mediante el asistente de configuración del router serie RV34x

Conclusión

Este artículo le ha llevado a una mejor comprensión de las VPN, junto con consejos para que pueda seguir su camino. Ahora ya debe estar preparado para configurar su propio dispositivo. Dedique algún tiempo a ver los enlaces y decida cuál es la mejor manera de configurar una VPN en su router de la serie Cisco RV.

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).