Virtual Private Networks

¿Cómo puede conectar dos redes en ubicaciones geográficamente separadas sin instalar una conexión privada entre ellos? ¿Cómo puede proporcionar servicios remotos para permitir a los usuarios acceder a los servicios corporativos que necesitan permanecer protegidos de las miradas indiscretas del público en Internet?

La respuesta a ambas preguntas es utilizar una red privada virtual (VPN). Las Vpns proporcionar vínculos de red virtual basados en el cifrado y el aislamiento del tráfico en el nivel de paquete sobre el uso de servicios de Internet como transporte. Los dos usos más comunes de VPN son vincular las sucursales o los sitios remotos (llamada tunelización de LAN a LAN, o L2L) y para proporcionar acceso remoto a los entornos de oficina (llamado acceso remoto [RA] VPN).

Los túneles L2L se utilizan extensamente para las comunicaciones privadas entre las redes corporativas y otras redes de confianza, que podrían ser oficinas remotas u otras empresas controladas por las redes, o de terceros (por ejemplo, para la externalización o los datos de empresa a empresa [B2B] llamados también intercambio). El túnel L2L se puede pensar como el enfoque de VPN de "fuerza industrial", se utiliza típicamente de la misma manera que un circuito punto a punto o un link de red privad. Las VPN son un enfoque predeterminado para las comunicaciones seguras entre dos partes, porque las condiciones y el tráfico permitidos en el VPN se pueden controlar estrictamente de cualquiera extremo del túnel. Los VPN L2L requieren típicamente un dispositivo en ambos lados de la conexión que puede admitir las mismas características y capacidades, ya que todas las configuraciones deben ser idénticas en ambos puntos finales de una VPN para que se cree un túnel. Si bien no hay forma de proporcionar calidad de servicio (QoS) con VPN basadas en Internet, ya que el enrutamiento del tráfico todavía está a discreción de la ruta de la capa 3, son rápidas, convenientes y seguras.

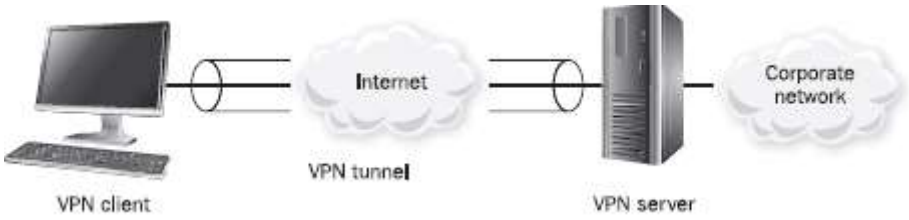
Los servicios de RA VPN permiten a los usuarios trabajar desde una ubicación remota como si estuvieran físicamente en una oficina. Por razones de conveniencia y costo, los servicios de RA VPN son cada vez más prolíficos como el teletrabajo y el acceso al sistema de terceros son cada vez más importantes para una variedad de negocios.

Cómo funciona una VPN

El objetivo de una VPN es proporcionar un canal de comunicación seguro a través de una red, la mayoría de las vpn son comúnmente un túnel privado a través de Internet. Para ello, el tráfico se encapsula con un encabezado que proporciona información de enrutamiento que ayuda al tráfico a llegar al destino.

El tráfico también se cifra, que proporciona la integridad, la confidencialidad, y la autenticidad.

Una VPN se conoce como un *Túnel* porque el cliente no conoce o se preocupa por el ruta real entre los dos extremos. Hay muchos tipos de túneles no cifrados disponible hoy en día, como los túneles de encapsulación de enrutamiento genérico (GRE), que hacen que dos lugares en una red aparecen más cerca. Mientras que una VPN topográficamente hace la mismo cosa, el componente privado de VPN se refiere al cifrado. Por ejemplo, supongamos que una sucursal está vinculada a la red corporativa por una VPN.



Protocolos VPN

Varias compañías de computación empezaron a desarrollar tecnologías VPN a mediados de la década de 1990, y sus protocolos eran específicos del proveedor. Hacia finales de la década de 1990, las VPN convergieron hacia el estándar IPSec. Hoy en día, la mayoría de los proveedores de VPN utilizan IPSec como protocolo básico en sus productos.

RFC 6040. Especifica cómo deben funcionar las VPN entre plataformas, logrando así la interoperabilidad de los proveedores. La norma no prohíbe funcionalidad más avanzada de ser añadido por cualquier proveedor en particular, pero se establece estándares mínimos por los cuales los dispositivos compatibles serán capaces de comunicarse para formar VPNs.

Es necesario que la configuración de ambos lados de una VPN coincida exactamente. Los protocolos VPN más comunes en uso hoy en día son IPSec, PPTP, L2TP a través de IPSec y SSL VPN.

IPSec

IPSec fue lanzado en 1998, después de años de diseño y debate entre los especialistas en seguridad y fabricantes de productos. Representa una especie de compromiso entre diferentes Intereses. IPSec se diseñó para proporcionar confidencialidad mediante cifrado, autenticación de puntos de conexión y la administración de claves segura. Proporciona diferentes maneras de hacer estas cosas, en gran parte debido a los debates de diseño que precedieron a su lanzamiento. Los parámetros de IPSec que se han utilizados por los puntos finales se negocian en la Asociación de seguridad (SA). Con dos incorporados protocolos de seguridad y dos "modos" de operación, cuatro combinaciones diferentes de protocolos, y es mejor asegurarse de que coincidan en ambos extremos o su VPN no funcionará.

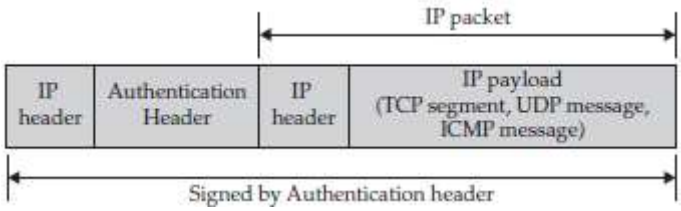
Hay dos tipos de configuraciones al usar IPSec VPN: modo de transporte y modo de túnel.

El modo de transporte solo cifra los datos de carga. Aunque el modo de transporte podría ser considerado "más rápido" dependiendo de qué protocolos de criptografía está utilizando (porque hay menos descifrado necesario con el modo de transporte), la mayoría de hardware hoy en día procesa en silicio y es lo suficientemente rápido como para no diferenciar entre el modo de túnel y modo de transporte, excepto en entornos muy exigentes/de alta carga o extremadamente sencible de latencia. Por esa razón, el modo de transporte no es muy común con equipos de alta velocidad de hoy en día.

El modo del túnel IPSec se utiliza a menudo para las conexiones del Gateway-a-Gateway L2L tales como vínculos de socios comerciales y conexiones de sucursales. Esto se debe a su flexibilidad, optimización y compatibilidad de proveedores, y también porque los parámetros de la conexión no cambian a menudo, a diferencia de otros tipos de conexiones de cliente. A menudo la conexión y los parámetros para construir el túnel entre los dispositivos se deben crear manualmente, y Aunque esto funciona bien al vincular los sitios, sería poco práctico apoyar

este para los clientes cuyos detalles de conexión (como la dirección IP del punto final) cambian con frecuencia.

Proveedores que han elegido esta solución de protocolo de tunelización han trabajado en torno a la necesidad de una configuración configuración en una variedad de maneras, pero para cualquier tipo de túnel no estático, las implementaciones son específicos de la plataforma tecnológica y no son interoperables entre proveedores.



Los clientes de VPN también usan el modo de túnel IPSec, pero normalmente requieren el cliente para cargar el software de conexión, como un cliente VPN o un paquete de instalación local que crea un adaptador de red virtual, que se puede precargar con la configuración del lado cliente, requisitos como opciones de autenticación y pertenencia a grupos.

PPTP

Hay un número de otros protocolos que se han desarrollado a lo largo de los años y sigue siendo parte de muchos productos hoy en día. El más común de estos protocolos es el de Microsoft protocolo de tunelización de punto a punto (PPTP). PPTP todavía se utiliza bastante en la industria porque es fácil de implementar, flexible y compatible con la mayoría de los sistemas operativos actuales. PPTP fue inicialmente desplegado en 1998 como parte de Windows NT 4,0 y fue inmediatamente abalanzada por la prensa debido a su horrible modelo de seguridad inicial.

Esto se ha corregido en gran medida en Windows 2000 y 2003, pero la reputación de PPTP probablemente estará siempre empinada por los errores iniciales.

Al menos a través de Windows 2008 R2, Microsoft todavía tiene capacidades PPTP, y algunas personas recomiendan usarlo como una manera "rápida y sucia" para obtener acceso remoto a una red, pero en general es menos seguro que otros métodos y sólo debe utilizarse, con precaución, para permitir acceso a redes que no lleven datos de misión crítica o confidenciales.

L2TP over IPSec

L2TP a través de IPSec es el resultado de combinar las mejores partes de PPTP de Microsoft y Layer Protocolo de reenvío de dos (L2F) de Cisco. L2TP a través de IPSec utiliza IPSec modo de transporte y tiene la ventaja de ser un túnel basado en PPP, que permite que dos cosas: los protocolos que no sean TCP/IP pueden ser fácilmente soportados en el túnel, y los sistemas operativos pueden crear un objeto de conexión conocido que se puede utilizar para abordar el túnel (esto es particularmente importante en los sistemas operativos de Microsoft). Estas opciones son significativo si el diseño del sistema operativo permite el uso de varios protocolos.

Aunque L2TP a través de IPSec proporciona más flexibilidad tanto al cliente como al servidor, crea sobrecarga en el entorno del túnel que podría argumentarse que es innecesario, especialmente si el entorno sólo utiliza TCP/IP. Sin embargo, muchas organizaciones que

implementan VPNs consideran el soporte nativo de Windows de L2TP a través de IPSec es una ventaja significativa. Normalmente, L2TP sobre IPSec se utiliza para la conectividad de cliente a servidor porque los parámetros de conexión pueden controlar dinámicamente los clientes que cambian. Si su entorno de red requiere el uso de protocolos que no sean TCP/IP, L2TP también se puede utilizar para conexiones Gateway-Gateway.

Puesto que el IPSec y el L2TP se definen dentro del estándar IETF, hay más proveedores que soportan esta solución, aunque todavía hay muchos más soportando por el modo del túnel IPSec.

SSL VPNs

Las implementaciones modernas de VPN SSL pueden igualar (o exceder) exactamente la funcionalidad de una VPN basada en cliente de software para el acceso remoto. Cuando se trata de acceso remoto de usuario, muchos productos aprovechan los enlaces protegidos con SSL a las aplicaciones corporativas a través de algún tipo de portales de acceso autenticado, que se denominan comúnmente "enlaces publicados." Este enfoque tiene tres grandes ventajas:

• Casi todos los clientes tienen el software necesario cargado por defecto: el navegador de Internet. No se necesita software adicional.

• La mayoría de los firewalls admiten SSL y no es necesario abrir protocolos ni puertos adicionales para admiten este tipo de conexión.

• En muchos casos, los usuarios remotos simplemente necesitan realizar tareas predecibles, como comprobar su correo electrónico o ejecutar una aplicación específica, y muchos de ellos son ya basada en Web.

Muchas organizaciones han vuelto a las VPN SSL para el acceso remoto porque el cliente base IPSec tienen una amplia sobrecarga informática (requieren la carga administrativa de crear, distribuir y mantener un archivo de conexión local para el PC), se pueden volver costosas, y muchos vendedores tienen problemas con sus extensiones propietarias.

Remote Access VPN Security

Al permitir que los sitios y los clientes remotos se conecten a la red corporativa a través de redes, la seguridad de los dispositivos en el otro extremo del túnel VPN es importante, porque pueden acceder a la red interna.

Los siguientes problemas de seguridad deben tenerse en cuenta al diseñar una RA VPN.

• A menos que la organización proporcione todos los sistemas remotos y mandatos que solo estos pueden ser utilizado, es imposible predecir el historial o los ajustes en los clientes. Para administrar y mantener la seguridad de la red de una organización, todas las entidades conectadas en la red necesitan ser administrados, soportados, y aseguradas según las políticas, los estándares y los procedimientos de la organización. Los sistemas que no son propiedad y gestionada por la organización no permiten la gestión de parches, antivirus, cortafuegos y otras medidas de seguridad. Incluso si un tercero en particular es diligente en mantener limpios sus sistemas, la falta de gestión empresarial hace que estos sistemas sean un riesgo en la red. Es

posible que los sistemas remotos de terceros no sean capaz de "llamar a wsus" para las actualizaciones y correcciones de seguridad, los sistemas de terceros no pueden recibir actualizaciones y cambios para ajustarse a los nuevos estándares proporcionados por la organización, y el malware pueden introducirse en la red por sistemas externos.

Authentication Process

Muchos procesos de autenticación para clientes remotos se basan en un nombre de usuario y una contraseña, incluso aquellos que están utilizando el intercambio de certificados como el mecanismo para asegurar la conexión.

Los nombres de usuario y las contraseñas se siguen utilizando hoy en día porque son fáciles de implementar y usar, y este tipo de autenticación ha existido durante tanto tiempo que está muy bien apoyado en casi todas las implementaciones de los sistemas operativos cliente.

En la industria de ti, los métodos de acceso remoto de empresa se mueven hacia el proceso de 2 factores de autenticación. Los criterios para estas soluciones son los que el usuario debe tener, conocer o ser algo único.

Para entornos basados en Windows, este normalmente implica una tarjeta inteligente basada en certificados. Otras soluciones van desde la base de tokens sistemas de contraseña de una sola vez (OTP) a escáneres biométricos.

Para los clientes de VPN que utilizan la compatibilidad nativa con L2TP a través de IPSec en Microsoft Windows (independientemente del servidor back-end), el comportamiento predeterminado es requerir un certificado para iniciar la Asociación de seguridad entre el cliente y el servidor. Esto suele ser un IPSec specifico certificado (normalmente para usuarios que no son de dominio) o un certificado de máquina (normalmente para equipos que son miembros del dominio). Los sistemas Windows también admiten el uso de un secreto compartido (también llamada clave preshared) para construir la Asociación de seguridad.

El objetivo final de la autenticación en un entorno VPN es doble:

• **Identificando la Máquina** El certificado de la máquina (o el secreto compartido, a una menor extensión) identifica el sistema como un sistema válido para establecer la seguridad IPSec Asociación. (Este paso no ocurre con PPTP y algunas otras soluciones VPN.)

• **Identificando el Usuario** El usuario demuestra quiénes se basan en el nombre de usuario, certificado, o algún otro mecanismo, pero la función básica es determinar Si el usuario tiene permiso para establecer una conexión.

La mayoría de los proveedores de acceso remoto tienen métodos para autenticar al usuario y, a continuación, comprobar la configuración de cliente antes de dar acceso completo. Esto se denomina validación de la postura (PV).

Configuración de cliente

En casi todos los ataques, los puntos finales del túnel son las víctimas. Si bien es posible atacar el tráfico en ruta cuando pasa a través de un túnel VPN, pero esto nos llevaría mucho tiempo, requerirá un alto nivel de sofisticación y requiere la captura de tráfico en ubicaciones de red específicas. Más los ataques no molestan o interfieren con el tráfico, pero se dirigen en lugar a los puntos finales del túnel. Es mucho más fructífero lanzar ataques simples en servidores o clientes en un esfuerzo por comprometer tanto el tráfico como la propia red corporativa. Por lo tanto, la condición del túnel extremos es fundamental en cualquier plan de acceso remoto.

La estrategia de seguridad sólo se refería a si un usuario tenía los derechos para conectarse al servicio de acceso remoto, pero en estos días, es común requerir ciertas configuraciones de los sistemas cliente. Este es un movimiento necesario debido al número de seguridad, parches y actualizaciones de software que deben implementarse en el sistema cliente para endurecerlos contra los ataques de punto final.

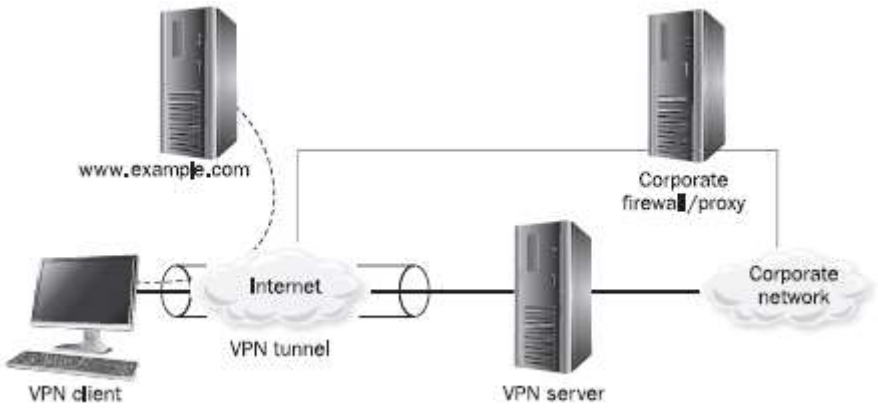
Al implementar soluciones de acceso remoto, muchas organizaciones toman el curso lógico de tratar de comprar una solución VPN para todo tipo de clientes. Si la organización ha limitado los tipos de clientes, esto es relativamente fácil, pero puede ser un desafío para las organizaciones que tienen un amplio base de clientes. Aunque idealmente se puede encontrar una solución unificada para todos los clientes, es a menudo el caso de que sólo algunos clientes pueden ser compatibles, o algunos son compatibles mejor que Otros. El arquitecto de acceso remoto tendrá que evaluar estos problemas y cómo afectan a la organización, y luego decidir sobre el mejor curso de acción.

En los primeros días, las VPN normalmente estaban destinadas a permitir que los sistemas Windows se conecten entre sí, pero hoy en día la proliferación de diferentes sistemas operativos de usuario final y dispositivos (incluyendo dispositivos móviles) ha complicado la imagen. Normalmente, una organización querriere tres cosas de un cliente remoto antes de permitir una conexión:

- Los parches de seguridad y los Service Packs deben estar a un nivel específico.
- Un firewall de software basado en host debe estar instalado.
- El software antivirus con las definiciones de virus actuales debe estar presente.

Entorno de red de cliente

Otra preocupación para el factor en un diseño de acceso remoto es cómo el cliente se configura para manejar la conexión de red para el túnel virtual. Cuando el cliente se puede conectar a más de una red remota a la vez, esto se conoce comúnmente como *túnel dividido*.



El ruteo del túnel dividido causa la preocupación por dos razones. La primera razón es que cuando un enrutamiento del cliente sabe cómo hablar directamente a la red corporativa e Internet, tráfico no autorizado se puede enrutar a través del cliente a la red corporativa. El segundo razón es que si un troyano se instaló en el cliente, un atacante podría tomar el control de los clientes y, a continuación, acceder a la red corporativa. Esta táctica es comúnmente explotada por los atacantes, por lo que el caso de túnel dividido debe evaluarse seriamente antes de permitir su uso.

Cualquier cliente con una configuración del túnel dividido se debe tener una buena configuración de seguridad y políticas estrictas que garanticen todas las redes y equipos que están en contacto o pudieran estar en contacto con este.

Hay realmente sólo algunas ventajas de un entorno de túnel dividido:

• Cuando la tabla de ruteo permite una conexión directa a un destino en lugar de tener el flujo de conexión a través de los firewalls corporativos y servidores proxy, en los clientes remotos potencialmente pueden tener más capacidades. Por ejemplo, la organización, las reglas de Firewall podrían no permitir el tráfico del servidor terminal desde el exterior, pero desde el tráfico de cliente no se filtraría por el firewall, podría conectarse a la destino con tráfico de servicio de terminal directamente.

• Las conexiones directas pueden proporcionar un aumento de velocidad para los sitios web de Internet. La velocidad dependerá realmente del diseño de la red y del conducto al Servicios VPN.

Muchos diseñadores utilizan servidores de almacenamiento en caché para ayudar con este problema, y en muchos casos no sólo pueden aumentar la velocidad para que coincida con la conexión directa, pero puede aprovechar los grandes vínculos de Internet de una organización para mejorar el Rendimiento.

• Algunos programas de VPN deshabilitan la capacidad de imprimir o acceder a los recursos locales en cualquier subredes, por lo que si tiene una LAN de oficina pequeña detrás de un dispositivo de conexión compartida, podría no ser capaz de transferir archivos o imprimir

cuando el túnel está conectado. Éste crea problemas para los usuarios que desean imprimir en una impresora local.

• Por último, es posible que los usuarios domésticos que utilizan sus propios sistemas no quieran que la organización tengan pista de a donde van. Esto es comprensible, pero en su lugar deben desconectar de los recursos corporativos cuando quieren trabajar en material personal.

Como arquitecto de acceso remoto, tendrá que establecer lo que considera un cliente bien protegido. Por ejemplo, consideremos un cliente típico de Windows y comencemos a compilar sobre los criterios para el proceso de inicio de sesión. Supongamos que la Directiva de acceso remoto dicta el siguiente requisitos de autenticación:

• Debe establecer la Asociación de seguridad IPSec con un certificado válido de una raíz de confianza

• Debe proporcionar inicio de sesión de tarjeta inteligente basada en certificado a través de la autenticación extensible Protocolo (EAP)

Una vez hecho esto, el cliente se coloca en una red de cuarentena virtual, y podemos forzar al cliente continuar con las siguientes comprobaciones:

• Debe estar ejecutando Windows 7 o superior

• Debe tener instalado un Service Pack definido (normalmente el más reciente)

• Debe tener todos los parches de seguridad críticos instalados (o al menos hasta una fecha determinada, o parches específicos en función de las necesidades y requisitos de la organización)

• Debe estar ejecutando el escáner de virus corporativo estándar con el último archivo de firma

• Debe estar ejecutando el software de Firewall corporativo (gestionado centralmente)

Si el cliente está ejecutando los tres primeros elementos, pero no está ejecutando el escáner de virus corporativo y cortafuegos, podemos dar al cliente un mensaje explicando los resultados del escaneo, iniciar una applet para supervisar el entorno de enrutamiento y, a continuación, sacar al cliente de la cuarentena.

Una vez que el cliente cargue los dos últimos elementos (que también podrían automatizarse para no requieren la intervención manual del usuario), entonces podrían comenzar a utilizar el ruteo más flexible. Los únicos elementos de configuración de cliente que estamos exigir con el fin de tomar el sistema fuera de cuarentena son la versión del sistema operativo, los Service Packs y los parches.

Hay varias maneras en que el cliente puede ser puesto en cuarentena desde el resto de la empresa:

• **Terminar la conexión** Algunos proveedores han elegido simplemente para enviar al cliente un mensaje que explica el problema con el cliente y simplemente suelta la conexión. Esto es prevenir posibles infecciones.

• **Establezca un límite de tiempo en la conexión** En esta situación, se envía al usuario un mensaje que explica el problema y, a continuación, se le da una cierta cantidad de tiempo para solucionar el problema antes de que se desconecte la sesión. Esto introduce un problema potencial cuando son grandes parches y conexiones lentas, y tiende a ser más difícil de soportar.

• Cree listas de control de acceso (ACL) en la sesión para "sandbox" que el cliente en este caso de que el cliente recibirá un mensaje explicando el problema y, a continuación, el sesión de conexión tendrá filtros aplicados que pueden restringir el tráfico a ciertos puertos o destinos internos. Esto es ideal, ya que le da al cliente la oportunidad para solucionar el problema utilizando recursos internos sin plantear un gran riesgo para el resto de la Corporación. Esto puede ser bastante complejo de configurar y mantener, por lo que el equipo de acceso remoto debe ser muy claro sobre los requisitos mínimos del cliente, tanto inicialmente como cambios y mejoras son necesarios.

Site-to-Site VPN Security

La popularidad de Internet y la disponibilidad de VPNs han conducido a organizaciones reemplazar las líneas arrendadas o las conexiones permanentes cableadas entre sitios y socios.

Esto es porque las conexiones VPN tienden a ser una fracción del costo de las líneas arrendadas o de conexiones MPLS. Mientras que el rendimiento de la VPN es en gran parte un factor del ancho de banda, latencia, la gran mayoría de los casos de uso para los VPN no requieren un nivel de rendimiento que requiera una red privada real (incluso el streaming de medios de comunicación, como lo demuestra la consumerización de la transmisión de vídeo bajo demanda a través de la Internet).

Varios de los problemas descritos en este capítulo se relacionan con el uso de clientes de acceso remoto como los puntos finales no son problemas para L2L VPN. Esto se debe principalmente a que una organización normalmente posee y controla ambos extremos del túnel para conexiones de sitio a sitio, aunque las implementaciones de negocio a negocio (B2B) son generalizadas y comunes. Además, la mayoría de las sucursales las oficinas están conectadas con enrutadores o dispositivos en lugar de clientes que operan sistemas, pero tenga en cuenta que hoy en día muchos dispositivos de red están ejecutando algún sabor de un sistema operativo de productos básicos (normalmente una variante de UNIX) bajo el capó, que requiere parches y actualizaciones como cualquier otro sistema. Puesto que los usuarios no inician sesión al routers y navegan Internet, instalar aplicaciones desconocidas o hacer doble clic en archivos adjuntos de correo electrónico, de sitio a sitio conexiones tienden a ser más seguras.

Las conexiones B2B mencionadas anteriormente son enlaces de sitio a sitio donde la Corporación posee solo un lado de la conexión. Esto se encuentra típicamente en situaciones donde el redes de la organización están vinculadas con las de los socios comerciales. No hay ningún quarantinetype solución que comprobará este tipo de conexión todavía, por lo que depende del acceso remoto arquitecto para definir los requisitos mínimos para el punto final del túnel del Partner, o para traer la conexión a través de un lugar en la red donde está aislado y hay visibilidad en lo que está teniendo lugar. Es importante monitorear el tráfico del link y, si es posible, restringirlo solo a los destinos internos necesarios.