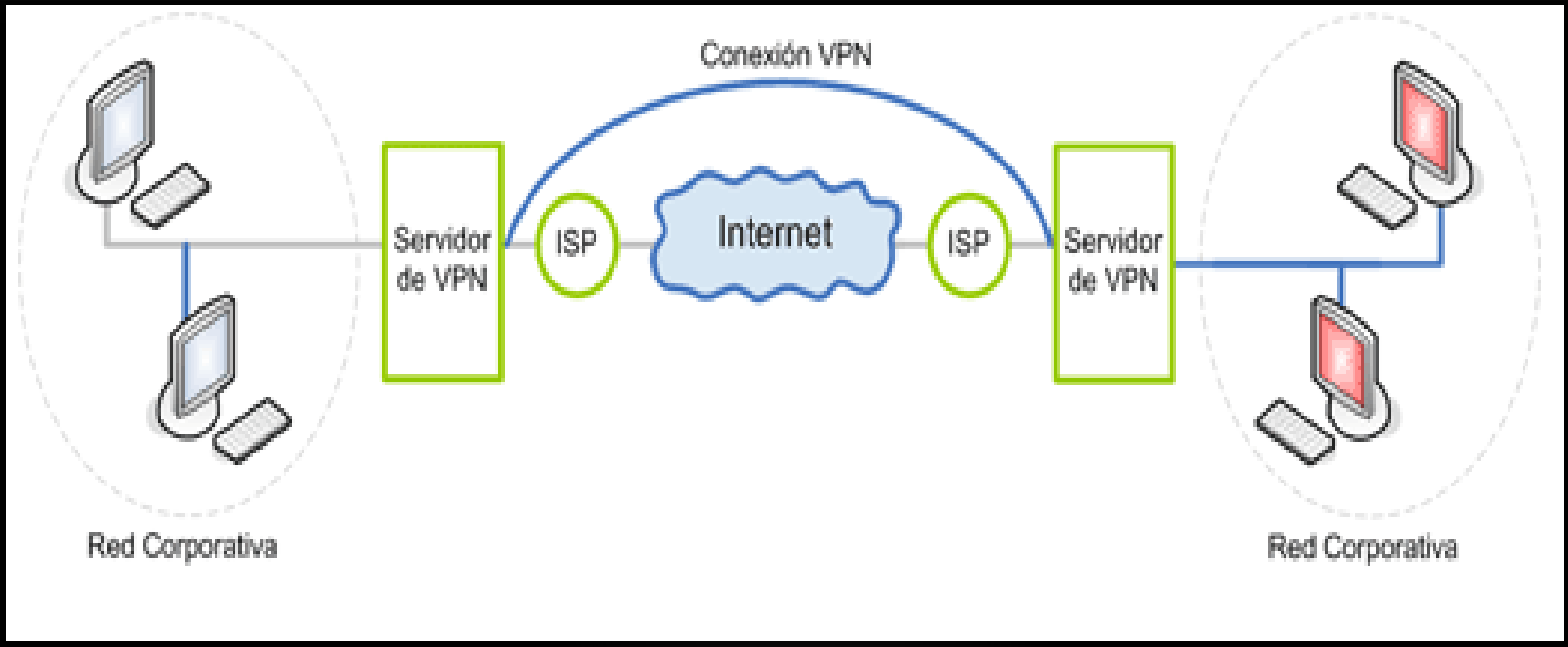
REDES PRIVADAS VIRTUALES (VPN)

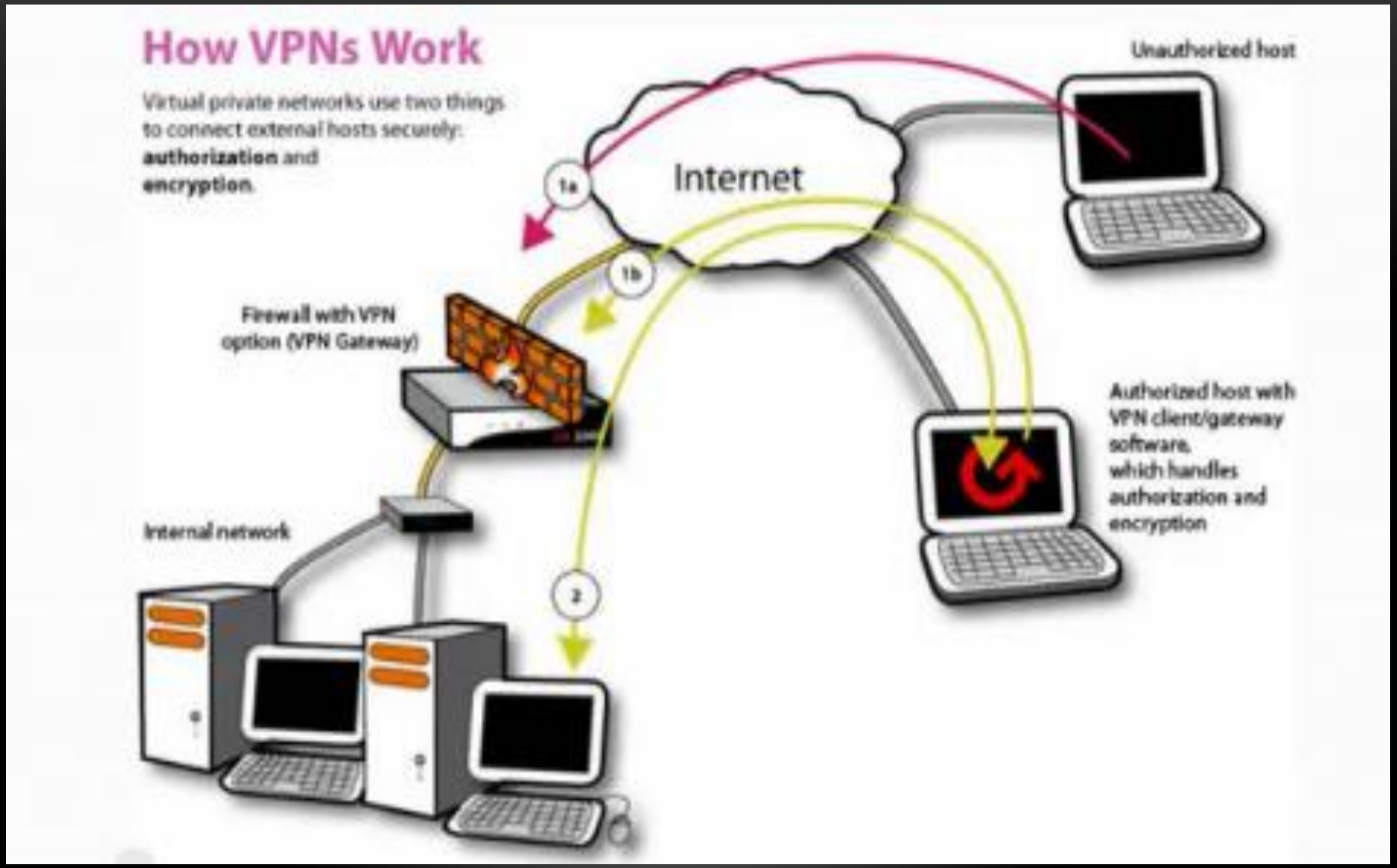
Las VPNs pueden proporcionar acceso remoto a los usuarios de la empresa a través de Internet, y al mismo tiempo conservar la privacidad de la información.

En vez de tener que utilizar una línea alquilada o hacer llamadas de larga distancia a un servidor de acceso a red corporativo o externo (NAS), el usuario debe llamar a un número telefónico local NAS de ISP, posteriormente, el software de la VPN crea una red privada virtual entre el usuario que marca y el servidor corporativo de VPN a través de Internet.

En este caso, tanto el router o el servidor de VPN de la sucursal como el de la central corporativa utilizan ISPs para conectarse a la red pública.

El software de la VPN utiliza las conexiones creadas para la creación de una conexión VPN entre la sucursal y la central. El servidor de la central es quien confirma la conexión pedida por la sucursal y se crea la conexión lógica entre ambos servidores

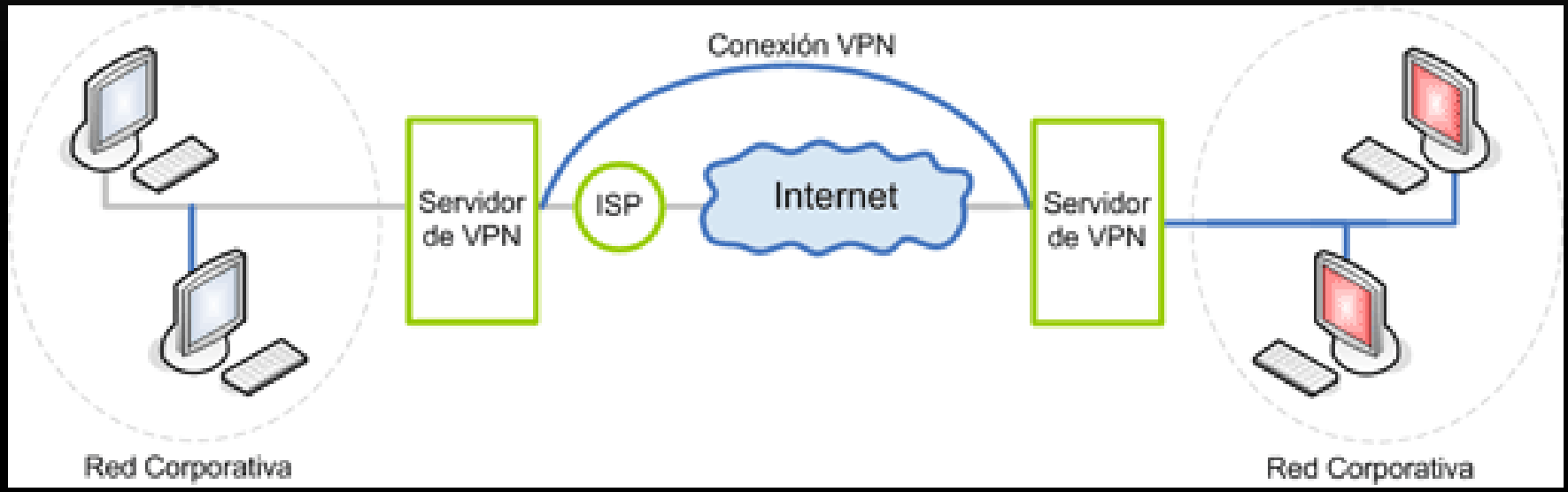

Conexión VPN
Servidor de VPN
ISP
Internet
ISP
Servidor de VPN
Red Corporativa
Red Corporativa


How VPNs Work
Virtual private networks use two things to connect external hosts securely: **authorization** and **encryption**.
Unauthorized host
Internet
1a
1b
Firewall with VPN option (VPN Gateway)
Authorized host with VPN client/gateway software, which handles authorization and encryption
Internal network
2

En este caso, el router en la sucursal puede llamar al ISP local o por algún tipo de conexión con Internet.

El software de la VPN instalado en el cliente utiliza la conexión al ISP local para la petición de la creación de la conexión VPN al servidor de la central. Al ser autorizada la conexión se crea lógicamente un túnel entre el servidor de la sucursal y el servidor de la central .

En este caso en particular el servidor de la central esta esperando que lleguen las peticiones de conexión.


Conexión VPN
Servidor de VPN
ISP
Internet
Servidor de VPN
Red Corporativa
Red Corporativa

Características básicas de la seguridad

Para hacerlo posible de manera segura es necesario proporcionar los medios para garantizar la autentificación, integridad de toda la comunicación:

Autentificación y autorización: ¿Quién está del otro lado? Usuario/equipo y qué nivel de acceso debe tener.

Integridad: de que los datos enviados no han sido alterados. Para ello se utiliza funciones de Hash. Los algoritmos de hash más comunes son los Message Digest (MD2 y MD5) y el Secure Hash Algorithm (SHA).

Confidencialidad: Dado que sólo puede ser interpretada por los destinatarios de la misma. Se hace uso de algoritmos de cifrado como Data Encryption Standard (DES), Triple DES (3DES) y Advanced Encryption Standard (AES).

No repudio: es decir, un mensaje tiene que ir firmado, y quien lo firma no puede negar que envió el mensaje.

TIPOS DE VPN

Básicamente existen tres arquitecturas de conexión VPN:

VPN de acceso remoto

Es quizás el modelo más usado actualmente, y consiste en usuarios o proveedores que se conectan con la empresa desde sitios remotos (oficinas comerciales, domicilios, hoteles, aviones preparados, etcétera) utilizando Internet como vínculo de acceso. Una vez autenticados tienen un nivel de acceso muy similar al que tienen en la red local de la empresa. Muchas empresas han reemplazado con esta tecnología su infraestructura dial-up (módems y líneas telefónicas).

VPN punto a punto

Este esquema se utiliza para conectar oficinas remotas con la sede central de la organización.

El servidor VPN, que posee un vínculo permanente a Internet, acepta las conexiones vía Internet provenientes de los sitios y establece el túnel VPN.

Los servidores de las sucursales se conectan a Internet utilizando los servicios de su proveedor local de Internet, típicamente mediante conexiones de banda ancha. Esto permite eliminar los costosos vínculos punto a punto tradicionales (realizados comúnmente mediante conexiones de cable físicas entre los nodos), sobre todo en las comunicaciones internacionales.

Es más común el siguiente punto, también llamado tecnología de túnel o tunneling.

La técnica de tunneling consiste en encapsular un protocolo de red sobre otro (protocolo de red encapsulador) creando un túnel dentro de una red de computadoras

Los dos tipos de redes virtuales privadas cifradas:

•VPN IPsec de sitio a sitio: Esta alternativa a Frame Relay o redes WAN de línea arrendada permite a las empresas extender los recursos de la red a las sucursales, oficinas en el hogar y sitios de los partners comerciales.

•VPN de acceso remoto: Esto extiende prácticamente todas las aplicaciones de datos, voz o video a los escritorios remotos, emulando los escritorios de la oficina central. Las redes VPN de acceso remoto pueden desplegarse usando redes VPN SSL, IPsec o ambas, dependiendo de los requisitos de implementación.

Tipos de conexión

Conexión de acceso remoto

Una conexión de acceso remoto es realizada por un cliente o un usuario de una computadora que se conecta a una red privada, los paquetes enviados a través de la conexión VPN son originados al cliente de acceso remoto, y éste se autentifica al servidor de acceso remoto, y el servidor se autentifica ante el cliente.

Conexión VPN router a router

Una conexión VPN router a router es realizada por un router, y este a su vez se conecta a una red privada.

En este tipo de conexión, los paquetes enviados desde cualquier router no se originan en los routers.

El router que realiza la llamada se autentifica ante el router que responde y este a su vez se autentica ante el router que realiza la llamada y también sirve para la intranet.

Conexión VPN firewall a firewall

Una conexión VPN firewall a firewall es realizada por uno de ellos, y éste a su vez se conecta a una red privada.

En este tipo de conexión, los paquetes son enviados desde cualquier usuario en Internet.

El firewall que realiza la llamada se autentifica ante el que responde y éste a su vez se autentifica ante el llamante

Red privada virtual

Conexión segura de oficinas, usuarios y partners

Las redes privadas virtuales (VPN) ayudan a las organizaciones a ampliar la conectividad y mejorar la velocidad en forma segura y rentable.

FIRMA DIGITAL

Una firma digital es un mecanismo criptográfico que permite al receptor de un mensaje firmado digitalmente determinar la entidad originadora de dicho mensaje (autenticación de origen y no repudio), y confirmar que el mensaje no ha sido alterado desde que fue firmado por el originador (integridad)

La firma digital se aplica en aquellas áreas donde es importante poder verificar la autenticidad y la integridad de ciertos datos, por ejemplo documentos electrónicos o software, ya que proporciona una herramienta para detectar la falsificación y la manipulación del contenido