Redes Privadas Virtuales

Dr. Luis Gerardo de la Fraga

Departamento de Computación
Cinvestav
Correo-e: fraga@cs.cinvestav.mx

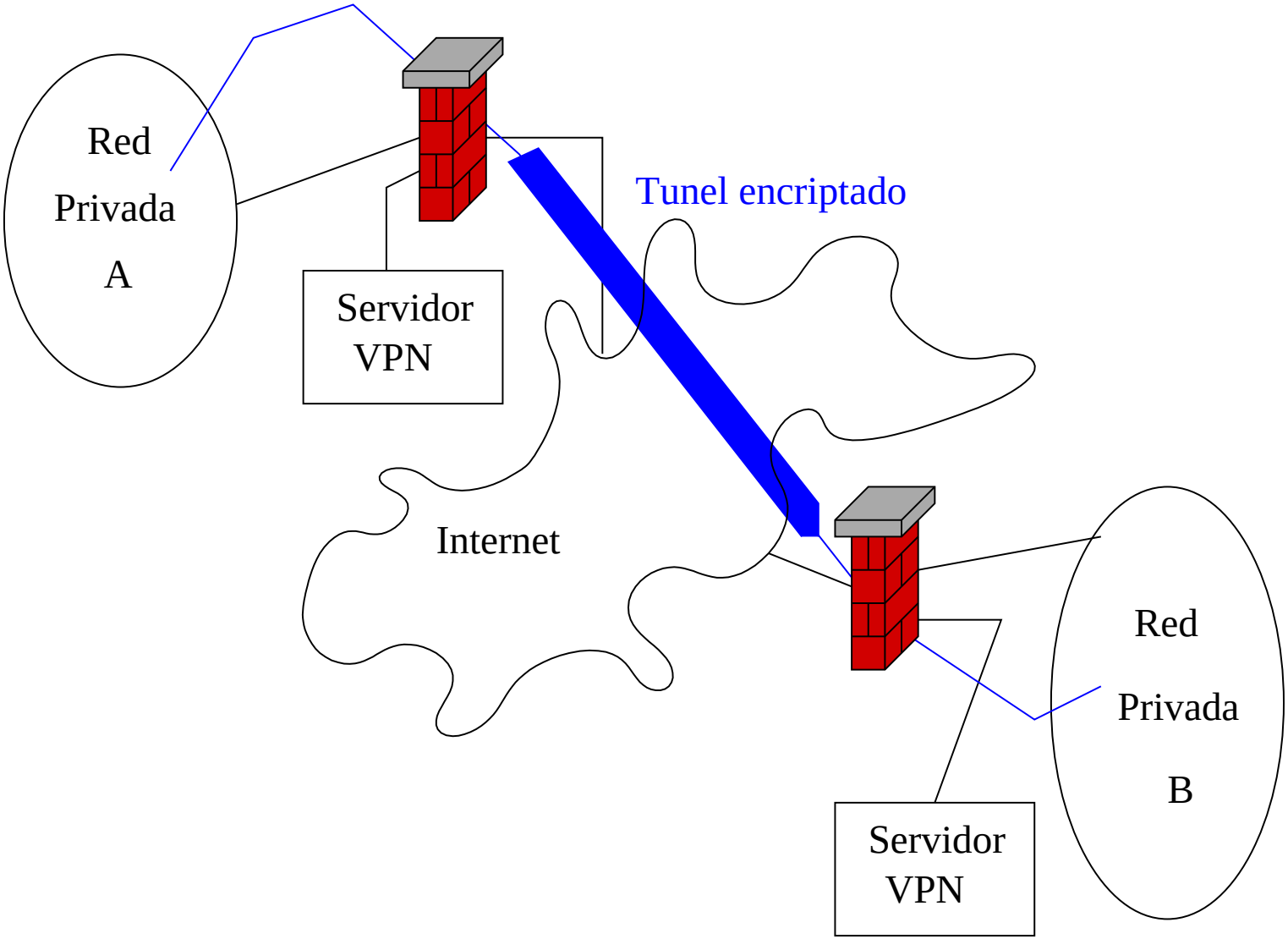
1 de junio de 2011

Redes Privadas Virtuales

VPNs se usan para conectar dos redes privadas a través de una red pública. O conectar clientes a una red segura a través de la red pública (Internet)
Por definición, una red pública es aquella sobre la que no se tiene control, no es confiable y no es segura.

Una red privada virtual puede ser la solución a los problemas de seguridad para conectar clientes en puntos de acceso inalámbricos que no son confiables
Se puede usar para conectarse a una red empresarial desde casa.
Organizaciones dispersas lo usan para encriptar sus ligas en la WAN de uso público.

RPV (Red Privada Virtual)



VPN es la solución ideal para conectar usuarios inalámbricos (desde puntos calientes o aún desde la red inalámbrica en el hogar) a los servidores de una empresa.
Previene de ataques como:

- DNS spoofing — Sustitución de DNS
- Web-session hijacking — Secuestro de sessiones WEB

Seguridad

Exiten tres categorias sobre seguridad que deben alcanzarse en este contexto:

1. Autenticación: ¿Los puntos terminales de las VPN son quienes verdaderamente dicen que son?
2. Integridad en datos: la conexión debe ser usada solo por los clientes y la red segura. No debe ser posible que un atacante inyecte tráfico extraño en el tráfico legítimo
3. Privacidad: No debe ser posible que un atacante pueda leer los datos contenidos en el tráfico sobre la VPN

Tipos de VPN

Existen dos posibles aplicaciones para una VPN

1. Sitio a sitio
2. Acceso remoto

VPN sitio a sitio

En una conexión VPN sitio a sitio los puntos terminales son generalmente ruteadores. Las dos redes se conectan por un tunel encriptado actuando como puertas para sus redes respectivas. Todos los ruteadores actualres soportan protocolos VPN, tal como IPsec

Para cada acceso remoto los túneles son creados dinámicamente: creándolos y destruyéndolos como se necesiten. Realizar túneles dinámicos puede ser costoso, computacionalmente hablando. Por ello es requerido un servidor que maneje las conexiones VPN, un concentrador VPN con alguna tarjeta especializada que realice las operaciones criptográficas.

Protocolos para realizar túneles

1. IPsec
2. Point-to-Point Tunneling Protocol (PPTP) de Microsoft
3. SSL-VPN, este encapsula el tráfico de las aplicaciones dentro del tráfico estándar HTTPS
4. OpenVPN, es una solución de software libre para realizar VPNs

IPsec

IPsec es un estándar abierto que adiciona encabezados seguros para IPv4 (en realidad es una adaptación de los mecanismos de seguridad de IPv6 en IPv4). Permite autenticar y checar la integridad en flujos IPv4 (sin crear en sí mismo un tunel). Se llaman modo de Autenticación de Encabezadas (HA) y modo de Carga Segura Encapsulada (Encapsulating Security Payload).

PPTP

Microsoft's Point-to-Point Tunneling Protocol (PPTP) es otro procolo para VPNs. Puede usarse para proteger protocolos diferentes al IP, como Microsoft NETBIOS.

Hay una opción de configurar un servidor PPTP en Linux.

No se recomiendo debido a que este protocolo tiene fallos de seguridad en su mismo diseño.

OpenVPN (1/2)

OpenVPN usa su propio demonio y software para cliente. Puede tunelear protocolos de bajo nivel, no solo IP, tal como lo hace PPTP. Y como IPsec usa realizaciones de algoritmos y protocolos criptográficos abiertos, muy bien implementados, probados y confiables.

OpenVPN (2/2)

- OpenVPN es mucho más fácil de entender, instalar y mantener que IPsec, que puede ser muy complicado y confuso.
- IPsec debe trabajar al nivel del núcleo de Linux
- OpenVPN esta compuesto de solo un programa de usuario, `openvpn`, que puede usarse para realizar tanto el servidor como el cliente.
- El sitio oficial de OpenVPN es www.openvpn.net

Referencias:

- Paranoid Penguin - Linux VPNs with OpenVPN M. Baer, Linux Journal, Feb 2010.
- Paranoid Penguin - Linux VPNs with OpenVPN, Part II M. Baer, Linux Journal, Mar 2010, pp. 24-28.
- Paranoid Penguin - Linux VPNs with OpenVPN, Part III M. Baer, Linux Journal, Apr 2010, pp. 28-31.
- Paranoid Penguin - Linux VPNs with OpenVPN, Part IV M. Baer, Linux Journal, May 2010, pp. 26-30.