

Redes Privadas Virtuales

Lic. Gerardo Rossel

Universidad Abierta Interamericana

Facultad de Tecnología Informática

Definición

- Virtual
 - ◆ Conectividad Dinámica de la Red
- Privada
 - ◆ Seguridad de la información
- La tecnología de VPN proporciona un medio para usar el canal público de Internet como un canal apropiado para comunicar los datos privados.
- Con la tecnología de encriptación y encapsulamiento, una VPN básica, crea un túnel privado a través de Internet.

Tuneling

- El principio de funcionamiento para el proceso túnel es el siguiente: para enviar un paquete IP al host 2, el host 1 construye el paquete que contiene la dirección IP del host 2, lo inserta en un marco ethernet dirigido al enrutador multiprotocolo que enlaza la empresa X, y lo pone en el ethernet. Cuando el enrutador multiprotocolo recibe el marco, retira el paquete IP, lo inserta en el campo de carga útil del paquete de capa de red de la WAN, y dirige este último a la dirección de la WAN del enrutador multiprotocolo que enlaza con la empresa Y. Al llegar ahí, el enrutador retira el paquete IP y lo envía al host 2 en un marco ethernet.
- La tecnología de túneles *-tunneling-* es un modo de transferir datos entre 2 redes similares sobre una red intermedia.

Tuneling

- La tecnología de túneles VPN, añade otra dimensión al proceso de túneles antes nombrado: encapsulación, ya que los paquetes están encriptados de forma que los datos son ilegibles para los extraños.

Seguridad

- PPTP/L2F/L2TP
 - ◆ Enlace de datos
- IPSec
 - ◆ Red
- Socks v5
 - ◆ Session

Comparación

Protocolos	Conectividad	Soporte	Encriptado Autenticado	Implementación
PPTP/L2TP	Túnel	IP, IPX, Net Beui	Límitados	Directa Algunos Cambios
IPSec	Túnel	IP (NetBios sobre IP)	Límitados Clave Pública	Cambios pila TCP/IP
Socks v5	Directa	IP	Amplios	Algunos Cambios

Tuneling Capa 2

- PPTP: Protocolo de tuneling punto a punto
 - ◆ Impulsado por Microsoft. Viene incluido en NT4 / 2000.
 - ◆ Multiprotocolo.
 - ◆ Puede integrarse con IPSec
 - ◆ Usa RSA
- L2F: Layer 2 Forwarding
 - ◆ Desarrollado por CISCO
 - ◆ Tiene menor overhead
 - ◆ Adecuado para redes administradas
- L2TP: Layer 2 Tuneling Protocol
 - ◆ Es prácticamente la combinación de los anteriores

IPSec

- IPv6 incluye la forma de establecer en forma estandar un VPN sobre IP.
- Dicha tecnología se conoce como IPSec o Seguridad IP
- IPSec permite encriptar y autenticar paquetes bajo IP
- Se establecen tuneles para el transporte de paquetes IP encriptados a nivel capa 3
- Los tuneles se extienden entre los dispositivos de borde de redes seguras y atraviesan redes no seguras.
- Los dispositivos de borde asumen la forma de firewalls (gateways)

IPSec

■ Autenticación

- ◆ Asegura la identidad de la máquina remitente
- ◆ No proporciona autenticación de usuarios

■ Integridad

- ◆ Se detectan modificaciones a los datos

■ Privacidad

- ◆ Implica el encriptado que impide su lectura por usuarios indebidos

IPSec - Autenticación

- La cabecera de autenticación proporciona un medio para la integridad de datos
 - ◆ Cabecera siguiente (8 bits)
 - ◆ Longitud (8 bits)
 - ◆ Reservado (16 bits)
 - ◆ Índice de parámetros de seguridad (32bits)
 - ◆ Datos de autenticación (variable)
- Los datos de autenticación dependen del algoritmo que se use. Se calculan usando el paquete entero excluyendo cualquier campo que pueda tener variaciones.
- El RFC 1828 establece el uso de MD5 para autenticación.
 - ◆ Se implementa en el origen sobre el paquete IP conjuntamente con una clave secreta.

IPSec ESP

- Provee privacidad.
- Modo transporte ESP
- Modo Tunel ESP
- Cabecera
 - ◆ Comienza con un índice de parámetros de seguridad de 32 Bits.
 - ◆ El resto, si existe, contiene parámetros según el algoritmo que use
 - ◆ La primera parte de la cabecera se transmite sin encriptar.

IPSec: Modo Transporte ESP

- En el origen, el bloque de datos que consta de la parte trasera de la cabecera ESP más el segmento entero de la capa de transporte se encripta y el texto nativo se reemplaza con el texto cifrado para formar el paquete IP a transmitir.
- El paquete es encaminado al destino.
- En el destino se examina y procesa la cabecera IP mas cualquier cabecera de ampliación IP en texto nativo. Sobre la base del SPI en la cabecera ESP, el nodo destino desencripta el resto del paquete para recuperar el segmento de la cabecera de transporte.

IPSec: Modo Tunel ESP

- Se encripta el paquete IP entero.
- Se encapsula el bloque completo cabecera ESP más paquete IP encriptado, con una nueva cabecera IP con la información necesaria para el traslado

IPSec

- Todas las implementaciones compatibles con ESP deben implementar el método de encriptado: DES-CBC (Data Encryption Standard – Cipher Block Chaining)
- Encriptado antes de autenticación:
 - ◆ ESP en modo transporte
 - ◆ ESP en modo tunel
 - ◆ La autenticación se aplica al paquete IP entero entregado a la IP destino externa.
- Autenticación antes de encriptado
 - ◆ Solo ESP modo tunel

Socks 5

- Opera a nivel capa 5
- Sólo con IP
- Generalmente se implementa en un servidor proxy
- Establece un circuito virtual entre el host local y el remoto.
- Puede interoperar con protocolos inferiores IPSec, PPTP, etc.
- Controla el acceso en base a los usuarios. Ofrece funciones de registro y auditoría de usuarios así como filtrado de contenidos.

Arquitecturas VPN

- VPN de acceso remoto
 - ◆ Independiente del ISP
 - ◆ Dependiente del ISP
- VPN Intranet o Intranet extendido
- VPN Extranet