Túneles VPN PPTP

Conceptos generales

Tunel PPTP

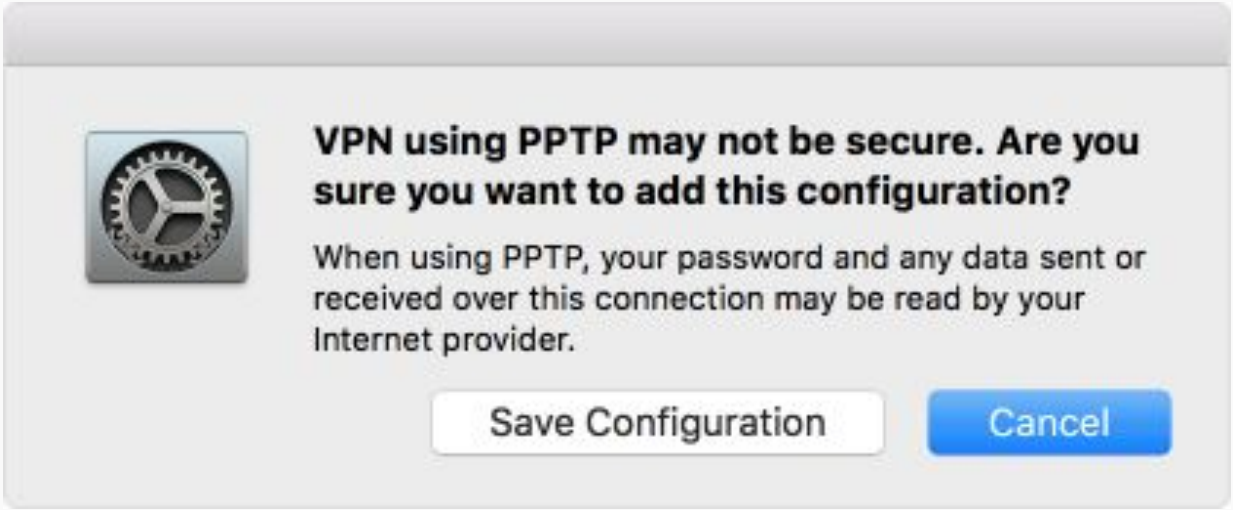
Point-To-Point Tunneling Protocol (PPTP) permitía el intercambio seguro de datos de un cliente a un servidor formando una Red Privada Virtual, empleando una red de trabajo TCP/IP. Entre los puntos fuertes de PPTP se encuentran su facilidad de configuración en entornos Windows, su capacidad para trabajar sobre demanda, y su soporte multi-protocolo que le permite funcionar sobre infraestructuras de área de trabajo existentes como Internet o conexiones de acceso telefónico PPP.

Tunel PPTP

La seguridad de PPTP ha sido completamente rota y las instalaciones con PPTP deberían ser retiradas o actualizadas a otra tecnología de VPN. La utilidad **ASLEAP** puede obtener claves de sesiones PPTP y descifrar el tráfico de la VPN. Los ataques a PPTP no pueden ser detectados por el cliente o el servidor porque el exploit es pasivo.

El fallo de **PPTP** es causado por errores de diseño en la criptografía en los protocolos handshake LEAP de Cisco y MSCHAP-v2 de Microsoft y por las limitaciones de la longitud de la clave en MPPE.

PPTP ya NO ES SEGURO



CANÓ ACADEMY

Conceptos importantes

Hay 3 conceptos importantes en la creación de túneles VPN:

Autenticación

Autorización

Contabilidad

CANÓ ACADEMY

Autenticación

La **autenticación** es el proceso por el que una entidad prueba su identidad ante otra. Normalmente la primera entidad es un cliente (usuario, ordenador, etc) y la segunda un servidor (ordenador). La Autenticación se consigue mediante la presentación de una propuesta de identidad (vg. un nombre de usuario) y la demostración de estar en posesión de las credenciales que permiten comprobarla. Ejemplos posibles de estas credenciales son las contraseñas, los testigos de un sólo uso (one-time tokens), los Certificados Digitales, ó los números de teléfono en la identificación de llamadas.

Autorización

Autorización se refiere a la concesión de privilegios específicos (incluyendo "ninguno") a una entidad o usuario basándose en su identidad (autenticada), los privilegios que solicita, y el estado actual del sistema. Las autorizaciones pueden también estar basadas en restricciones, tales como restricciones horarias, sobre la localización de la entidad solicitante, la prohibición de realizar logins múltiples simultáneos del mismo usuario, etc. Ejemplos de tipos de servicio son, pero sin estar limitado a: filtrado de direcciones IP, asignación de direcciones, asignación de rutas, asignación de parámetros de Calidad de Servicio, asignación de Ancho de banda, y Cifrado.

Contabilización

La **contabilización** se refiere al seguimiento del consumo de los recursos de red por los usuarios. Esta información puede usarse posteriormente para la administración, planificación, facturación, u otros propósitos. La contabilización en tiempo real es aquella en la que los datos generados se entregan al mismo tiempo que se produce el consumo de los recursos. La información típica que un proceso de contabilización registra es la identidad del usuario, el tipo de servicio que se le proporciona, cuando comenzó a usarlo, y cuando terminó.

PPTP

PPTP es un protocolo de capa 2, encriptado y precedido por una pequeña cabecera PPTP basada en GRE(Generic Routing Encapsulation). **Protocolo IP 47**

Los mensajes de control se intercambian por el puerto **TCP 1723** y la encriptación por los mecanismos PPP MS-CHAP-v1, MS-CHAP-v2.

PPTP utiliza MPPE(**Microsoft Point-to-Point Encryption (MPPE) para encriptación.**

PPTP

En Mikrotik es posible configurar un bridge utilizando PPTP con una interfaz ethernet que tenga una mac ya que los enlaces PPP no tienen direcciones MAC.

PPTP incluye:

Contabilización y Autenticación para cada sesión PPTP.

Encriptación: MPPE 40 bits RC4 - MPPE 128 bits RC4

Desventajas del túnel PPTP

Es un protocolo inseguro

Se puede crackear facilmente

Su encriptación de 128 bits obsoleta

Laboratorio

Vamos a trabajar con nuestro Mikrotik en la nube configurando el servidor PPTP y creando los usuarios remotos que puedan conectarse al mismo.

Configuraremos clientes en Windows y clientes en el Mikrotik que usted tiene asignado

MikroTik

DigitalOcean

CANÓ ACADEMY