UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE UNIDAD DE EDUCACIÓN

Redes de Comunicaciones

9910

Integrantes:

Chávez Robelly Annthony Sebastian

DOCENTE:

GUSTAVO DAVID SALASAR CHACON

Investigación sobre VPNs e IPSec

Quito – Ecuador

2023

VPN

Una red privada virtual (VPN) es una red que utiliza una conexión de Internet pública para crear una conexión privada entre dos o más dispositivos. Esto permite que los dispositivos se comuniquen entre sí de forma segura, incluso si se encuentran en diferentes ubicaciones.

VPN GRE

VPN GRE (Generic Routing Encapsulation) es un protocolo de túnelización que permite encapsular paquetes de datos de un protocolo de capa de red en un paquete de otro protocolo de capa de red. Esto permite que los paquetes de datos se envíen a través de una red que no admite el protocolo de capa de red original.

GRE se utiliza a menudo para conectar redes que utilizan diferentes protocolos de capa de red, como IPv4 e IPv6. También se puede utilizar para conectar redes que se encuentran en diferentes ubicaciones, como una oficina en Londres y una oficina en Nueva York.

GRE es un protocolo simple y eficiente, y es fácil de configurar. Esto lo hace una buena opción para una variedad de aplicaciones, como el acceso remoto, la colaboración y la computación en la nube.

Aquí hay algunos ejemplos de cómo se utiliza GRE:

Para conectar dos redes que utilizan diferentes protocolos de capa de red.

Para conectar dos redes que se encuentran en diferentes ubicaciones.

Para crear una conexión de túnel privado a través de una red pública.

Para proporcionar seguridad para las comunicaciones IP.

GRE es un protocolo versátil y eficaz que se puede utilizar para una variedad de aplicaciones. Es una buena opción para las empresas que necesitan conectar redes que utilizan diferentes protocolos de capa de red o que se encuentran en diferentes ubicaciones.

Elementos de una VPN

Peers: Los peers son los dispositivos que participan en una VPN.

Protocolos: Los protocolos son los protocolos utilizados para establecer y mantener una VPN.

Túneles: Los túneles son las conexiones que se utilizan para enrutar los paquetes de datos a través de una VPN.

Tipos de VPNs

VPN de sitio a sitio: Una VPN de sitio a sitio conecta dos redes diferentes.

VPN de acceso remoto: Una VPN de acceso remoto permite a los usuarios conectarse a una red privada desde un dispositivo remoto, como un ordenador portátil o un teléfono inteligente.

Al elegir un tipo de VPN, hay varios factores a considerar. Estos incluyen:

La seguridad: El primer factor a considerar es la seguridad que ofrece la VPN. Esto incluye la cantidad de protocolos de seguridad que utiliza, la calidad de sus claves y la cantidad de datos que encripta.

La velocidad: La VPN también debe ser rápida, para que no experimentes ningún retraso al navegar por Internet o usar aplicaciones.

La facilidad de uso: La VPN debe ser fácil de usar, para que puedas configurarla y conectarte sin problemas.

El precio: Las VPN pueden variar en precio, por lo que es importante encontrar una que sea asequible para ti.

Además de estos factores, también puedes considerar otros factores, como el número de servidores que ofrece la VPN, los países en los que están ubicados esos servidores, y las características adicionales que ofrece.

Una vez que hayas considerado todos estos factores, puedes empezar a reducir tus opciones y encontrar la mejor VPN para ti.

Aquí hay algunos consejos para elegir una VPN:

Lee las reseñas de los clientes: Una de las mejores maneras de encontrar una buena VPN es leyendo las reseñas de los clientes. Esto te dará una idea de la seguridad, la velocidad y la facilidad de uso de la VPN.

Elige un proveedor de VPN con una buena reputación: Hay muchos proveedores de VPN diferentes disponibles, por lo que es importante elegir uno con una buena reputación. Esto significa que el proveedor debe tener un buen historial de seguridad y privacidad, y debe ofrecer un buen servicio al cliente.

No te fíes de las VPN gratuitas: Las VPN gratuitas pueden ser tentadoras, pero a menudo no ofrecen el mismo nivel de seguridad y privacidad que las VPN de pago. Es mejor pagar por una VPN que te ofrezca una buena seguridad y privacidad.

IPSec

IPSec (Internet Protocol Security) es un conjunto de protocolos que proporcionan seguridad para las comunicaciones IP. IPSec se utiliza para autenticar, encriptar y autenticar los paquetes de datos que se envían a través de una VPN.

Protocolos que componen IPSec

AH (Authentication Header): AH proporciona autenticación para los paquetes de datos.

ESP (Encapsulating Security Payload): ESP proporciona encriptación y autenticación para los paquetes de datos.

IKE (Internet Key Exchange): IKE es un protocolo que negocia las claves de IPSec entre los peers.

Formato de encabezado IPSec

El encabezado IPSec tiene el siguiente formato:

Version: La versión del encabezado IPSec.

IHL (Internet Header Length): La longitud del encabezado IPSec.

DSCP (Differentiated Services Code Point): El código de punto de servicio diferenciado.

ECN (Explicit Congestion Notification): La notificación explícita de congestión.

Protocolo: El protocolo de capa de transporte.

Largo: El largo del paquete de datos.

Control: Los bits de control.

Siguiente encabezado: El encabezado de la capa de transporte.

Bibliografía

https://en.wikipedia.org/wiki/Virtual_private_network

https://en.wikipedia.org/wiki/Generic_Routing_Encapsulation

https://en.wikipedia.org/wiki/IPsec

https://en.wikipedia.org/wiki/Internet_Key_Exchange

How They Work and Why You Need One" by PCMag

"The Best VPNs of 2023" by CNET

"How to Set Up a VPN" by Lifehacker