Sistemas seguros de acceso y transmisión de datos.

IFCT0109 – Seguridad informática

MF0488_3 (60 horas)

Comunicaciones seguras

- Introducción
- Definición, finalidad y funcionalidad de redes privadas virtuales
- Protocolo IPSec
- Protocolos SSL y SSH
- Sistemas SSL VPN
- úneles cifrados
- Ventajas e inconvenientes de las distintas alternativas para la implantación de la tecnología de VPN
- Resumen

Introducción

La introducción al uso de los algoritmos criptográficos en la creación de comunicaciones seguras es un tema de gran relevancia en el ámbito de la tecnología de la información. Este proceso comienza con el entendimiento de los algoritmos criptográficos y su mecanismo de operación, lo cual sienta las bases para su aplicación práctica, particularmente en la seguridad de las comunicaciones.

El establecimiento de comunicaciones seguras entre dos entidades mediante un canal de comunicación que no es seguro por sí mismo introduce el concepto de la red privada virtual (VPN). Este concepto clave se explora en detalle, resaltando sus objetivos y funcionalidades principales, para proporcionar una comprensión clara de su importancia y cómo facilita conexiones seguras a través de internet.

Las VPNs, sin embargo, no están limitadas a un único protocolo para su implementación; existen múltiples protocolos disponibles, cada uno con sus propias características y aplicaciones específicas. Entre estos, los protocolos IPsec, SSL y SSH son de particular interés, ya que cada uno ofrece diferentes métodos para el establecimiento de túneles cifrados, esenciales para la seguridad de las comunicaciones.

Con una variedad de protocolos disponibles, es crucial comprender las ventajas y desventajas asociadas con cada opción. Este conocimiento es vital para tomar decisiones informadas al seleccionar el protocolo más adecuado para crear una VPN, considerando tanto las necesidades específicas de seguridad como el contexto en el que se implementará la VPN.

Definición, finalidad y funcionalidad de las redes privadas virtuales

Las Redes Privadas Virtuales, comúnmente conocidas por sus siglas en inglés, VPN (Virtual Private Network), representan una tecnología crucial en el ámbito de las comunicaciones digitales. Estas redes permiten la creación de un canal seguro de comunicación sobre la infraestructura de una red pública existente, como es el caso de internet. Su principal atributo es la capacidad de conectar dispositivos dispersos geográficamente como si estuvieran presentes en una misma red local, facilitando así un intercambio de información seguro y privado.

Ventajas de las VPN:

- Conexión Segura: Asegura la privacidad y la seguridad de los datos transmitidos entre los dispositivos conectados, a pesar de utilizar una red pública.
- Acceso Remoto: Permite a los empleados acceder a los recursos de la empresa de manera segura desde cualquier lugar del mundo, lo que es especialmente útil en el contexto del teletrabajo.

Ejemplo Ilustrativo:

Consideremos la familia A, compuesta por tres miembros: padre, madre y Pepito, su hijo. Si un amigo de Pepito viene a visitar y se le otorga acceso a la red familiar, este visitante podrá interactuar dentro de la red como si fuera un miembro más de la familia, a pesar de no serlo oficialmente.

Esta situación se asemeja a cómo operan las VPN en el entorno digital: permiten que dispositivos externos se comuniquen como si estuvieran físicamente conectados a una red privada, garantizando la seguridad y la privacidad de esa comunicación. Esencialmente, una VPN convierte a un "amigo" (un dispositivo externo) en un "miembro de la familia" (parte de la red privada), sin importar su ubicación geográfica.

Para entender plenamente el mecanismo detrás de las VPN, es crucial familiarizarse con los principios fundamentales de las redes de ordenadores, incluyendo cómo se transmiten los datos y se mantienen seguros a lo largo de su recorrido por internet.

Definición, finalidad y funcionalidad de las redes privadas virtuales

Conceptos previos. El modelo OSI

Para establecer comunicaciones seguras mediante redes privadas virtuales (VPN), es fundamental comprender la estructura y funcionamiento de las redes a través del Modelo de Interconexión de Sistemas Abiertos (OSI). Este modelo se organiza en siete capas, cada una responsable de distintas facetas de la comunicación a través de una red. Este enfoque estratificado asegura que los datos se transmitan de manera eficiente y segura desde el emisor hasta el receptor, independientemente de la naturaleza de las redes involucradas.

Las capas del modelo OSI son las siguientes:

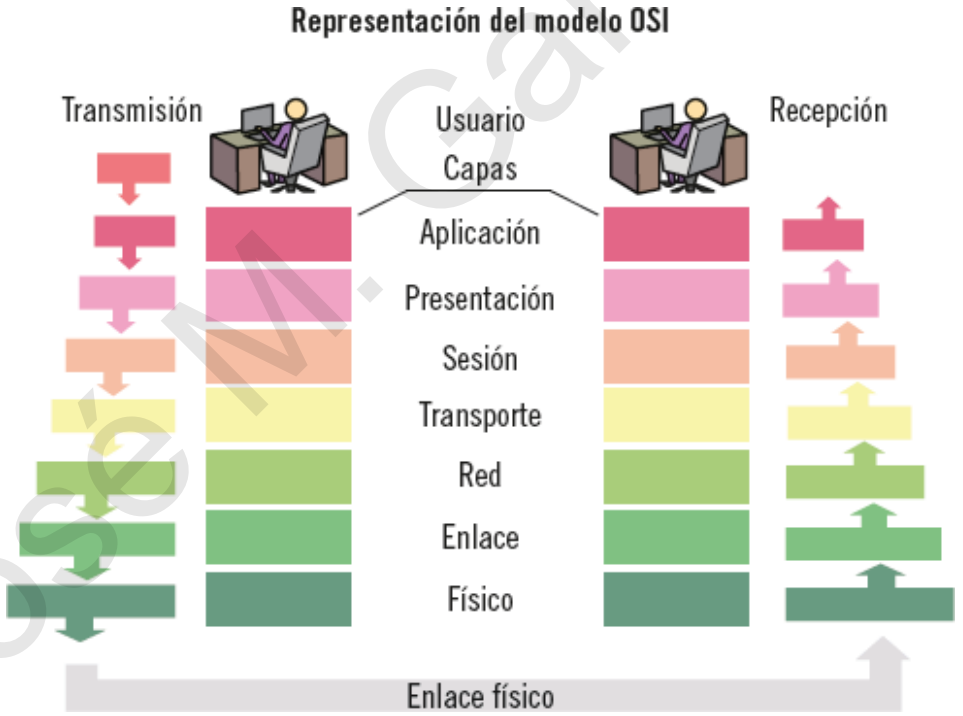
- Nivel Físico (Capa 1): Se ocupa de la transmisión física de los datos a través del medio de comunicación.
- Nivel de Enlace (Capa 2): Define cómo los dispositivos en una red local se identifican y comunican entre sí, usando direcciones MAC.
- Nivel de Red (Capa 3): Facilita la comunicación entre dispositivos en diferentes redes mediante direcciones IP.
- Nivel de Transporte (Capa 4): Permite el uso simultáneo del canal de comunicación por múltiples aplicaciones, introduciendo el concepto de puerto.
- Nivel de Sesión (Capa 5) y Presentación (Capa 6): Gestionan las sesiones de comunicación entre aplicaciones y la correcta interpretación de los datos transmitidos, respectivamente.
- Nivel de Aplicación (Capa 7): Define los protocolos específicos que utilizan las aplicaciones para intercambiar datos.

Definición, finalidad y funcionalidad de las redes privadas virtuales

Conceptos previos. El modelo OSI

En el contexto de las VPN, el envío de datos se efectúa encapsulando la información a través de estas capas, desde la aplicación emisora hasta el nivel físico, añadiendo en cada paso información relevante como puertos, direcciones IP y MAC. Al llegar al destinatario, este proceso se invierte, desencapsulando y ascendiendo por las capas hasta llegar a la aplicación receptora.

La técnica de encapsulamiento permite que los datos se transmitan seguramente a través de redes distintas, funcionando como si estuvieran directamente conectadas. Este mecanismo es fundamental para las VPN, ya que permite la creación de "túneles" seguros a través de los cuales la información puede viajar protegida de accesos no autorizados.



Definición, finalidad y funcionalidad de las redes privadas virtuales

Descripción de las VPN

Las Redes Privadas Virtuales (VPN) facilitan la interconexión de dispositivos distantes, creando un entorno seguro como si estuvieran en la misma red local. Esto es crucial para acceder a recursos específicos, como servidores de datos, bajo una política de seguridad estricta que asegura el acceso exclusivo a miembros autorizados de la red. Al usar VPN, los dispositivos adoptan una configuración que los identifica como parte de la red deseada, a pesar de su ubicación física, otorgando una ilusión de proximidad.

El valor central de las VPN radica en la confidencialidad de los datos transmitidos. Esto se traduce en la formación de una red privada sobre infraestructura pública, generalmente Internet, resguardando la información de accesos no autorizados. La percepción de trabajar dentro de una red local, aun estando físicamente dispersos, subraya la naturaleza "virtual" y "privada" de estas redes.

Las VPN no solo garantizan la confidencialidad, sino que también ofrecen autenticación de origen e integridad de datos, esenciales para prevenir accesos indebidos y alteraciones en la información durante su transmisión. Estas redes pueden aplicarse para conexiones ordenador-a-red, permitiendo a empleados acceder a la red corporativa desde sus casas, o para enlaces sitio-a-sitio, uniendo edificios de una misma empresa bajo una red unificada.

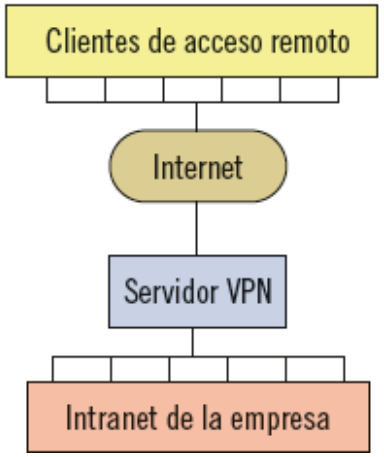
Definición, finalidad y funcionalidad de las redes privadas virtuales

Descripción de las VPN

Para implementar VPN, se utilizan diversos protocolos de tunelado como:

- IPSec (Internet Protocol Security)
- SSL (Secure Socket Layer)
- SSH (Secure Shell)
- PPTP (Point-to-Point Tunnelling Protocol)
- L2TP (Layer 2 Tunnelling Protocol)
- DTLS (Datagram Transport Layer Security)

Diagrama de una red privada virtual (VPN)



De estos, SSL e IPSec son las opciones predominantes por su eficacia y seguridad en el establecimiento de VPNs. Estos protocolos aseguran que las conexiones virtuales privadas mantengan la integridad, autenticidad y confidencialidad de los datos comunicados a través de una infraestructura pública.

Definición, finalidad y funcionalidad de las redes privadas virtuales

Ventajas y desventajas de las VPN

Las Redes Privadas Virtuales (VPN) han revolucionado la manera en que las empresas y los individuos se conectan y protegen sus datos en Internet. Presentan una serie de ventajas significativas que abarcan desde el coste hasta la seguridad, pero no están exentas de ciertas limitaciones y desafíos.

Ventajas de las VPN

- Bajo Coste de Despliegue: Las VPN eliminan la necesidad de redes dedicadas costosas, permitiendo que diferentes sedes de una empresa se comuniquen a través de Internet de manera segura y económica.
- Transparencia de Comunicación: Para los usuarios, el uso de una VPN es casi imperceptible. Ofrece la misma experiencia de uso que si estuvieran conectados directamente a la red local de su oficina, independientemente de su ubicación geográfica.
- Seguridad en los Sistemas: Las VPN proporcionan una capa adicional de seguridad, protegiendo la información sensible mediante cifrado y otros métodos de seguridad.
- Simplicidad Administrativa: Facilitan la gestión de accesos y recursos, ya que todos los dispositivos se tratan como si estuvieran en la misma red local.

Protocolo IPSEC

Introducción

IPSec (Internet Protocol Security) es un conjunto de protocolos ampliamente utilizado para la creación de redes privadas virtuales (VPN). Mediante la analogía del envío de correos entre urbanizaciones, IPSec juega un papel crucial en la encapsulación de datos, es decir, en el proceso de envolver un "sobre" de datos dentro de otro, garantizando la confidencialidad y autenticación de los datos transmitidos. Este mecanismo asegura que la información sea legítima y que su contenido permanezca privado e inalterado durante su transmisión.

Una distinción significativa de IPSec es su operación en el nivel de red, específicamente en el nivel 3 del modelo OSI, a diferencia de otros protocolos como SSL, que operan en la capa de transporte (nivel 4). Esta característica permite que cualquier servicio o aplicación situada en capas superiores del modelo OSI se beneficie de las capacidades de seguridad que IPSec ofrece.

Los protocolos primordiales que componen IPSec son el Internet Key Exchange (IKE) y el Encapsulating Security Payload (ESP). Tradicionalmente, se menciona a Authenticated Header (AH) como un tercer protocolo; sin embargo, basándose en las investigaciones de William Stallings, se destaca que AH ha caído en desuso. Esto se debe a que ESP ahora cubre las necesidades de autenticación de mensajes, objetivos inicialmente asignados a AH. Por lo tanto, aunque AH aún se conserva por compatibilidad, su uso no se recomienda en desarrollos recientes.

En la implementación de IPSec, IKE establece las reglas para la encapsulación de datos, definiendo aspectos como el tamaño y la preparación de los "sobres" de datos. Por otro lado, ESP lleva a cabo el proceso de encapsulación conforme a lo acordado por IKE, asegurando la confidencialidad e integridad de la información transmitida.

Protocolo IPSEC

Internet Key Exchange (IKE)

Internet Key Exchange (IKE) es un protocolo esencial para establecer asociaciones de seguridad entre dos partes comunicantes. Su función primordial es definir los parámetros de seguridad que permiten a ambas entidades comunicarse de manera segura, incluyendo la selección del algoritmo criptográfico, su modo de operación, y la clave de cifrado para los datos intercambiados.

La asociación de seguridad creada mediante IKE facilita un esquema de funcionamiento acordado, aprovechable en el protocolo Encapsulating Security Payload (ESP). Este protocolo, al igual que IKE, es parte integral de la suite de protocolos IPsec, proporcionando servicios esenciales de seguridad en la red.

IKE opera mediante intercambios de mensajes estructurados en dos fases principales:

- IKE_SA_INIT: Este intercambio inicial permite negociar parámetros fundamentales para la asociación de seguridad, intercambiar valores aleatorios y utilizar el algoritmo Diffie-Hellman para generar una clave compartida. Dicha clave sirve como base para derivar dos claves adicionales: una para el cifrado y otra para la autenticación de los mensajes, mediante el uso de funciones hash.

  La simplicidad de este intercambio radica en que el emisor propone opciones de algoritmos criptográficos, y el receptor selecciona uno adecuado o indica un error si ninguno lo es.

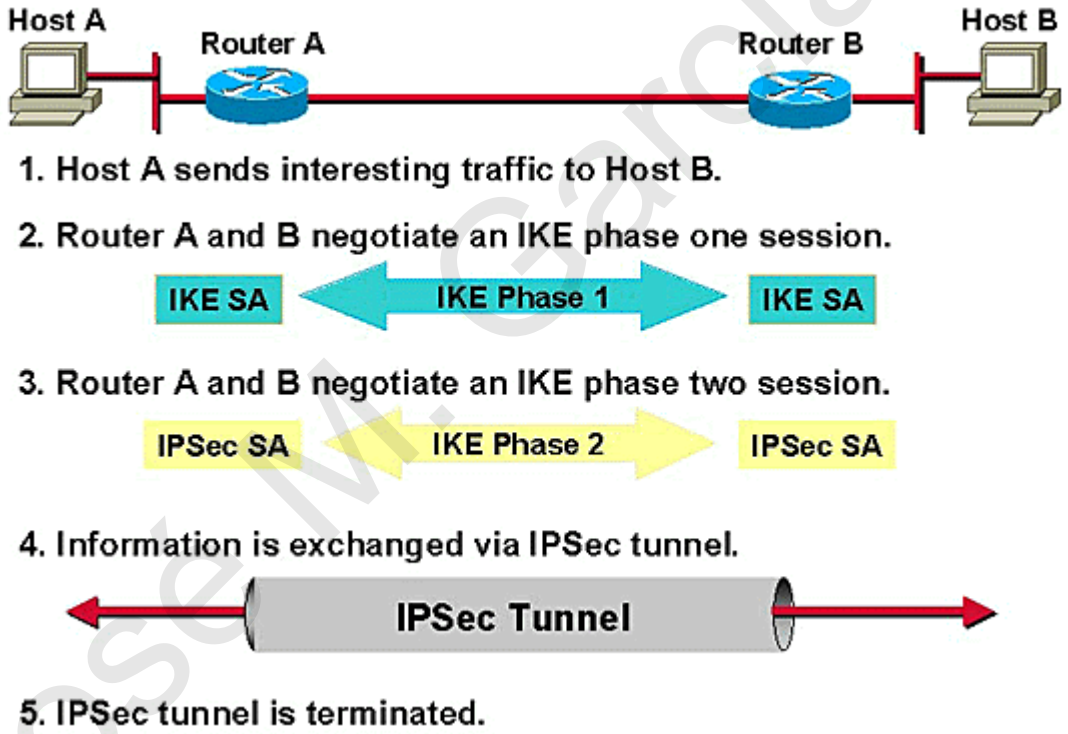
- IKE_AUTH: Durante esta fase, las partes se autentican mutuamente y se establece la asociación de seguridad que se utilizará con ESP.

  Nota: La asociación de seguridad establecida en este punto es inicial, pero no exclusiva. Los comunicantes tienen la capacidad de negociar nuevas asociaciones mediante el intercambio CREATE_CHILD_SA, una necesidad derivada del uso limitado en el tiempo de las claves, para mantener la durabilidad y la seguridad de la comunicación.

Protocolo IPSEC

Internet Key Exchange (IKE)

Los mensajes intercambiados durante la fase de autenticación se cifran con la clave negociada anteriormente para proteger la identidad de los participantes y evitar su exposición a terceros no autorizados. La autenticación puede realizarse a través de certificados de clave pública, añadiendo una capa adicional de seguridad al proceso de verificación de identidades.



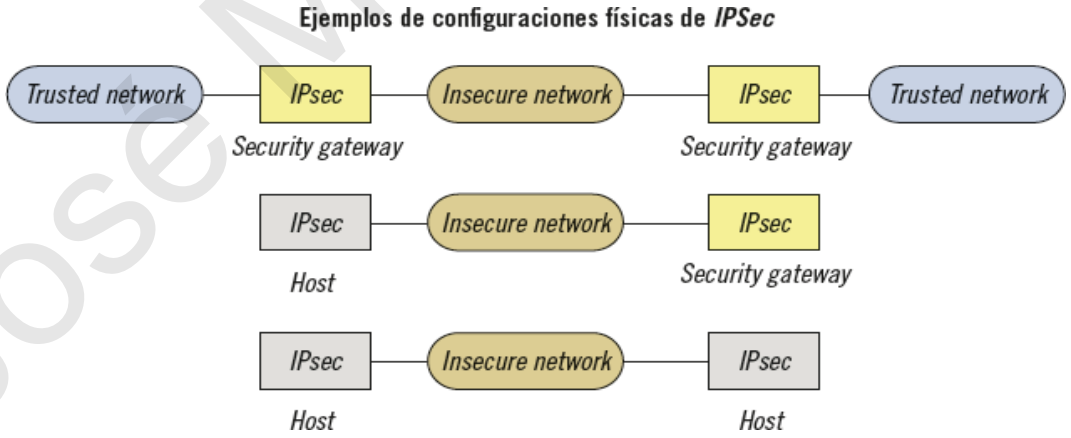
Protocolo IPSEC

Escenarios de uso

IPSec, un protocolo fundamental para la seguridad en redes privadas virtuales (VPN), se utiliza en diversos escenarios, dependiendo de la configuración física de los participantes y el tipo de protección deseada. Su flexibilidad permite adaptarse tanto a necesidades individuales como corporativas, garantizando la seguridad de la información transmitida.

Según la configuración física. La implementación de IPSec puede variar según el rol que juegan los dispositivos en la red:

- Equipos finales conectados a equipos intermedios: En este escenario, dispositivos como ordenadores portátiles de empleados utilizan equipos intermedios (routers, gateways) dedicados a establecer conexiones seguras mediante IPSec.
- Un extremo final y un intermediario: Aquí, solo uno de los dispositivos es un equipo final directamente implicado en la comunicación, mientras que el otro extremo actúa como un intermediario.
- Ambos extremos son equipos finales: En este caso, ambos dispositivos implementan IPSec directamente, sin necesidad de intermediarios, proporcionando una conexión segura de extremo a extremo.



Protocolo IPSEC

Escenarios de uso

Según el tipo de protección. IPSec ofrece dos modos principales de protección, adecuados para diferentes necesidades de seguridad:

- Modo Transporte: Protege únicamente la carga útil de los paquetes, dejando intacta la cabecera original. Es ideal para comunicaciones seguras entre equipos finales donde la ocultación de las direcciones IP no es necesaria.
- Modo Túnel: Encapsula el paquete original completo, incluida su cabecera, dentro de un nuevo paquete IPSec. Este modo es preferido cuando al menos uno de los participantes es un intermediario, ya que permite proteger integralmente la información transmitida, incluidas las direcciones IP.

Estos modos de uso reflejan la versatilidad de IPSec para adaptarse a una amplia gama de escenarios de red, desde el acceso remoto seguro por empleados hasta la conexión segura entre diferentes sedes de una organización.

Protocolo IPSEC

Encapsulating Security Payload (ESP)

El protocolo Encapsulating Security Payload (ESP) juega un papel crucial en el aseguramiento de la confidencialidad, autenticación e integridad de la información transmitida a través de una red. Operando como parte esencial del conjunto de protocolos IPSec, ESP encapsula la información original en un nuevo paquete, al cual se aplican diversos mecanismos de seguridad derivados de la asociación de seguridad establecida por Internet Key Exchange (IKE).

Este nuevo paquete contiene elementos clave para la seguridad y el manejo adecuado de los datos:

- Identificador de la Asociación de Seguridad: Esencial para que los participantes entiendan cómo procesar el paquete.
- Número de Secuencia: Facilita al receptor el reordenamiento de los paquetes, considerando que en Internet, los datos pueden llegar en un orden diferente al enviado. Si este número alcanza su valor máximo, indica la necesidad de renegociar la asociación de seguridad.
- Vector de Inicialización: Necesario para algunos algoritmos de cifrado, asegurando que cada mensaje sea único.
- Carga Útil: El contenido original, que puede incluir relleno para prevenir ataques de análisis de tráfico o para cumplir con requisitos específicos de tamaño del paquete.
- Control de Integridad: Verifica que el contenido del paquete no haya sido alterado durante la transmisión, empleándose únicamente si se acordó en la asociación de seguridad.

ESP, por lo tanto, no solo protege la información contra el acceso no autorizado sino que también mantiene la integridad y la autenticidad de los datos transmitidos, adaptándose a las necesidades de seguridad de la comunicación en redes complejas y diversificadas.

Protocolos SSL y SSH

Los protocolos Secure Sockets Layer (SSL) y Secure Shell (SSH) son esenciales para la seguridad en la red, facilitando la creación de túneles confidenciales para el envío seguro de datos y la verificación de su integridad. Sin embargo, presentan diferencias significativas en su aplicación y método de autenticación. Mientras SSL emplea certificados para la autenticación, favoreciendo su uso en aplicaciones con datos sensibles como las bancarias, SSH utiliza comúnmente usuario y contraseña, siendo ideal para la administración remota de sistemas.

Secure Sockets Layer (SSL)

Desarrollado inicialmente por Netscape, SSL ha evolucionado significativamente desde sus inicios problemáticos hasta la versión SSL 3.0 en 1996, que después se convertiría en TLS (Transport Security Layer). Actuando sobre el nivel de transporte (nivel 4 del modelo OSI), SSL proporciona un marco de seguridad para servicios a nivel de aplicación (nivel 5 del modelo OSI), manifestándose comúnmente en navegadores como "https" para sitios web que manejan información delicada, como es el caso de la banca online.

SSL se distingue por su capacidad de compresión, que es opcional, el uso de certificados X.509 v3, y la provisión de varios servicios de seguridad, como la autenticación del servidor y opcionalmente del cliente, la integridad, la confidencialidad, y el no repudio por parte del cliente. El proceso de SSL involucra un intercambio inicial de claves públicas certificadas, seguido de la creación y envío de una clave secreta por parte del cliente al servidor, permitiendo así el inicio seguro de la transmisión de datos.

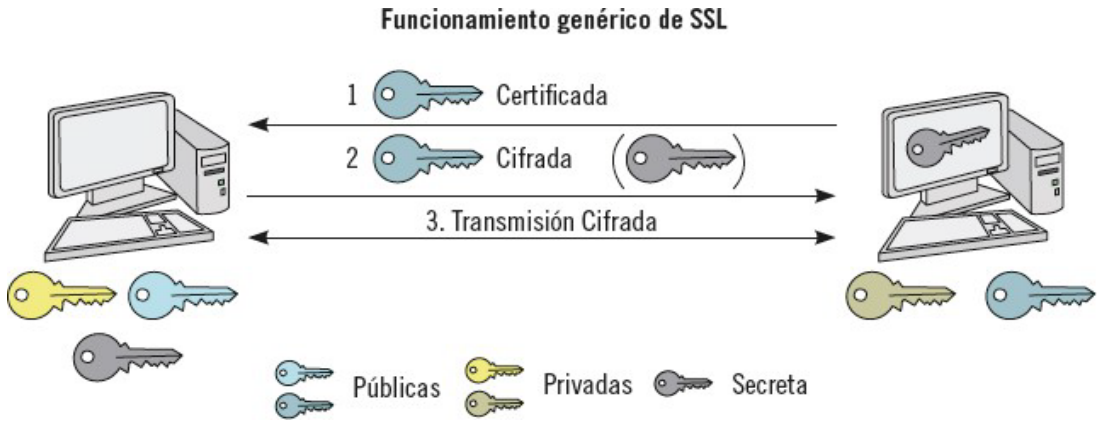
Protocolos SSL y SSH

Secure Sockets Layer (SSL)

Los subprotocolos de SSL incluyen:

- Protocolo de Salutación (Handshake Protocol): Establece la comunicación segura entre cliente y servidor. Los interlocutores negocian qué versión de protocolo usar, seleccionan los algoritmos criptográficos, autentican unos a otros y establecen las claves criptográficas que se usarán.
- Protocolo de Registro (Record Protocol): Sirve para el cifrado de la información que se transmitirá y garantiza la confidencialidad e integridad de los datos. Este protocolo envuelve los datos de aplicación en una estructura segura antes de su transmisión.
- Protocolo de Cambio de Especificación de Cifrado (Change Cipher Spec Protocol): Señala los cambios en la negociación de seguridad y se utiliza para cambiar las claves y algoritmos que se están utilizando en la conexión segura.
- Protocolo de Alerta (Alert Protocol): Notifica a las partes sobre cualquier error o problemas relacionados con la seguridad, incluidos los mensajes de advertencia y los errores fatales que pueden terminar la sesión.La infraestructura de SSL/TLS es fundamental para asegurar comunicaciones en la web, protegiendo contra la interceptación y manipulación de datos sensibles.

La infraestructura de SSL/TLS es fundamental para asegurar comunicaciones en la web, protegiendo contra la interceptación y manipulación de datos sensibles.



Protocolos SSL y SSH

SSL Extended Validation (EV-SSL) (Variante de SSL)

La variante SSL Extended Validation (EV-SSL) surge como un esfuerzo por incrementar la confianza en las transacciones electrónicas, garantizando que el servidor con el que se conecta un usuario es auténtico y fiable. A pesar de que EV-SSL opera igual que SSL en términos de las fases y el funcionamiento básico, establece estándares más altos para la emisión de certificados:

- Auditorías a las Autoridades de Certificación (CA): Estas deben superar auditorías regulares que validen la minuciosidad en la emisión de certificados.
- Solicitud del Certificado: Los certificados EV-SSL se otorgan únicamente cuando son solicitados por el responsable del dominio o por aquellos con control exclusivo sobre él.
- Implementación de OCSP: Las CA deben utilizar el protocolo Online Certificate Status Protocol (OCSP), lo que permite a los navegadores verificar en tiempo real la validez del certificado.
- Políticas de Certificación Distinguidas: Los certificados EV-SSL se emiten con políticas específicas que los navegadores pueden identificar, diferenciándolos de otros tipos de certificados.

Los usuarios pueden reconocer fácilmente los sitios web con EV-SSL por los indicadores visuales en la barra de direcciones del navegador, tales como el candado verde, el nombre de la compañía destacado o la barra de direcciones coloreada, que son señales distintivas de un alto nivel de autenticación.

Protocolos SSL y SSH

Secure Shell (SSH)

Secure Shell (SSH) es un protocolo de red criptográfico que ofrece una manera segura de acceder a un ordenador remoto y ejecutar comandos, transferir archivos o realizar otras tareas de red sobre una conexión no segura. Diseñado inicialmente como una alternativa segura a protocolos no cifrados como TELNET, SSH ha evolucionado para incluir una variedad de funciones más allá del acceso remoto.

Con la versión SSH2, se introdujeron mejoras significativas en términos de seguridad y rendimiento, y esta versión es la que se ha convertido en la estándar para las comunicaciones seguras en la mayoría de las aplicaciones cliente-servidor y sistemas operativos. SSH es especialmente conocido por su uso en el inicio de sesión remoto y la creación de túneles de red seguros.

Los tres protocolos principales que componen SSH son:

Protocolo de la Capa de Transporte: Asegura una conexión segura mediante el intercambio de claves y el cifrado de los datos de sesión.

Protocolo de Autenticación de Usuario: Verifica la identidad del usuario que intenta conectarse al sistema remoto, a menudo utilizando un par de claves pública y privada.

Protocolo de Conexión: Permite múltiples conexiones seguras y simultáneas dentro de la sesión de transporte cifrada establecida.

SSH es una herramienta esencial en el ámbito de la administración de sistemas, proporcionando un mecanismo confiable y seguro para las tareas de administración remota y la transferencia de datos.

Protocolos SSL y SSH

Secure Shell (SSH)

Protocolo de la capa de transporte

El Protocolo de la Capa de Transporte es fundamental para la seguridad en las comunicaciones en la red, actuando en el nivel 4 del Modelo OSI. Este protocolo se encarga de la autenticación de las entidades, asegurando la autenticidad de los mensajes y protegiendo la confidencialidad e integridad de los datos.

Dentro de este marco, la autenticación del servidor se realiza mediante claves criptográficas, un par de claves públicas y privadas que el servidor posee para validar su identidad ante el cliente.

El término "host" hace referencia a cualquier equipo informático implicado en la comunicación, ya sea cliente o servidor.

La autenticación del servidor puede realizarse de dos maneras:

- Base de Datos Local del Cliente: El cliente mantiene una base de datos local que vincula el nombre de cada host con su clave pública correspondiente. Este método prescinde de la necesidad de un tercero de confianza pero puede ser complejo de mantener.
- Certificación por una Autoridad: Las claves públicas están certificadas por una autoridad competente, lo que permite al cliente verificar la validez de las claves con la certeza de que proceden de una fuente fiable. Esto simplifica la gestión de las claves, ya que el cliente solo necesita almacenar de forma segura la clave de la autoridad raíz.

Después de la autenticación, los hosts proceden al intercambio de paquetes. Esta conexión se establece fuera del propio protocolo y durante el intercambio de datos se aplican métodos de compresión, cifrado y control de integridad, como el uso de códigos MAC. Los algoritmos utilizados para estas funciones son previamente negociados entre las partes.

Protocolos SSL y SSH

Secure Shell (SSH)

Protocolo de la capa de transporte

En cuanto al cifrado, se utiliza criptografía simétrica, y el intercambio de claves se efectúa por medio de variantes del método de Diffie-Hellman, con el servidor autenticándose frente al cliente mediante la firma de su componente en el intercambio de claves.

El proceso concluye con una solicitud de servicio por parte del cliente, que puede ser para iniciar el Protocolo de Autenticación de Usuarios o el Protocolo de Conexión.

Protocolos SSL y SSH

Secure Shell (SSH)

Protocolo de autenticación de usuarios

El Protocolo de Autenticación de Usuarios desempeña un papel crucial en la validación de identidades entre usuarios y servidores. Este protocolo opera sobre otros protocolos que ya garantizan la confidencialidad y la integridad de la comunicación, formando así una base segura para la autenticación.

Existen diferentes métodos para autenticar a los usuarios, cada uno con su propio enfoque en cuanto a seguridad y facilidad de uso:

- Método de Clave Pública: El cliente proporciona al servidor su clave pública firmada, que el servidor debe verificar. Este método se basa en el uso de pares de claves criptográficas asimétricas, permitiendo una autenticación robusta sin el intercambio de secretos como las contraseñas.
- Método de Contraseña: Es el método más tradicional donde el cliente simplemente envía una contraseña que el servidor compara con la que tiene almacenada. Aunque es de fácil implementación y uso, plantea desafíos de seguridad si no se maneja con cuidado.
- Método Hostbased: En este método, el cliente envía una firma creada con la clave de su host. Si el servidor confía en el host, y este último certifica que el usuario se ha autenticado correctamente, el servidor aceptará la autenticación. Este método aprovecha la autenticación previa que ha tenido lugar en el host del cliente.

Cada uno de estos métodos de autenticación responde a diferentes requisitos y escenarios de seguridad, y la elección entre ellos dependerá de factores como la infraestructura existente, el nivel de seguridad deseado y la facilidad de uso.

Protocolos SSL y SSH

Secure Shell (SSH)

Protocolo de conexión

El Protocolo de Conexión se ejecuta sobre el Protocolo de la Capa de Transporte y es esencial en la gestión de múltiples y concurrentes usos de una conexión SSH. Facilita la creación de canales para diferentes propósitos como sesiones de comandos o gráficos (X11).

Los canales SSH transitan por tres etapas:

- Apertura del Canal: Se define el tipo de canal y se acuerdan parámetros como el tamaño de la ventana de transmisión y el tamaño máximo del paquete, lo que garantiza una transmisión de datos eficiente.
- Transmisión de Datos: Durante esta fase se utiliza activamente el canal para la comunicación de datos entre el cliente y el servidor.
- Cierre del Canal: Culmina la interacción por ese canal y puede ser iniciado por cualquiera de las partes involucradas en la comunicación.

Una funcionalidad notable de SSH es la redirección de puertos, que permite la comunicación a través de puertos designados, reenviándolos para evitar restricciones como las impuestas por cortafuegos. Esta característica es invaluable para el acceso remoto seguro a redes empresariales protegidas.

Sistemas SSL VPN

Introducción

Los sistemas SSL VPN posibilitan la creación de una red privada virtual utilizando simplemente un navegador web, eliminando la necesidad de software adicional en el dispositivo del usuario. Esto simplifica notablemente el proceso para los usuarios finales y facilita la conexión remota segura a sistemas corporativos.

Una SSL VPN puede considerarse un conjunto de dispositivos que cifran el tráfico de datos mediante SSL a través del navegador. Esto no solo brinda las ventajas típicas de una VPN en términos de acceso y seguridad, sino que también permite a los administradores aplicar controles de acceso muy específicos a aplicaciones y servicios.

Sin embargo, las SSL VPN también conllevan riesgos:

- Riesgo de Malware: Dado que se usa comúnmente un navegador web, existe la posibilidad de que el dispositivo del usuario esté comprometido por malware, lo que podría extenderse a la red corporativa durante la conexión VPN. Para mitigar este riesgo, se puede forzar la comprobación de la integridad del cliente, denegando conexiones que no cumplan con ciertas políticas de seguridad.
- Riesgos de Privacidad: Las conexiones a través de navegadores dejan rastros digitales como cookies e historiales de URL. Cuando se usan dispositivos públicos, estos datos pueden quedar expuestos a terceros no autorizados. Para evitarlo, el extremo de la conexión VPN SSL puede implementar medidas para borrar los datos al final de cada sesión.
- Vulnerabilidad a Ataques de Descubrimiento de Contraseñas: Al no requerir software de cliente, el acceso a una VPN SSL está disponible para cualquier usuario con acceso a Internet, lo que aumenta el riesgo de ataques para descubrir contraseñas. La implementación de la autenticación de dos factores puede mejorar considerablemente la seguridad en este aspecto.

Sistemas SSL VPN

Tipos de SSL VPN

Los sistemas VPN SSL se dividen en dos categorías principales, cada una soportada por la mayoría de los sistemas operativos, y ofrecen una experiencia de usuario transparente.

VPN SSL Portal

Este tipo permite a los usuarios acceder a una web que actúa como entrada a servicios de red diversos y seguros. La página de entrada requiere autenticación, y luego presenta al usuario aplicaciones y servicios de una red interna o de internet.

Reescritura de URL

Un aspecto clave de las SSL VPN portal es la reescritura de URL, que adapta las direcciones de los servicios para que parezcan provenir del mismo servidor. Sin embargo, si la reescritura de URL no se gestiona correctamente, puede dirigir a los usuarios a sitios maliciosos o permitir el acceso a áreas restringidas si el sistema de reescritura se ve comprometido. Además, lenguajes como JavaScript, Flash o Java, comúnmente utilizados para la reescritura, pueden introducir vulnerabilidades.

Por ejemplo, si un usuario quiere acceder a un servicio interno de la empresa cuya URL original es http://servicio.interno.com, la SSL VPN podría reescribir esta dirección como https://portalvpn.empresa.com/servicio. Esto se hace generalmente por razones de seguridad y simplicidad, permitiendo a los usuarios navegar a través de servicios internos sin tener que manejar múltiples direcciones o enfrentarse a posibles bloqueos por firewall.

Almacenamiento en Caché de Autenticación

Algunas SSL VPN guardan en caché la información de autenticación del usuario para reducir la frecuencia de inicio de sesión, lo cual es conveniente pero puede aumentar el riesgo de ataques de suplantación de identidad si la información se ve comprometida.

Sistemas SSL VPN

Tipos de SSL VPN

VPN SSL Túnel

La VPN SSL de túnel funciona creando un "túnel" cifrado entre el dispositivo del usuario y el servidor VPN, a través del cual puede pasar el tráfico de red. Este túnel se establece generalmente después de que el usuario se autentica con éxito en un portal web seguro proporcionado por el servicio de VPN SSL. Una vez establecido el túnel, el tráfico entre el dispositivo del usuario y la red a la que se accede se cifra, protegiendo así la transferencia de datos de interceptaciones, espionaje o manipulaciones.

Desafíos y Limitaciones

- Gestión de Puertos. En las redes informáticas, los puertos permiten distinguir diferentes tipos de tráfico y servicios, lo que facilita la dirección de los datos al programa adecuado en un dispositivo. El Modelo OSI, un marco de referencia para entender cómo funcionan las redes, establece claras distinciones y usos para estos puertos. Sin embargo, las SSL VPN túnel carecen de estándares definidos para la asignación de puertos en los túneles. Esto significa que los usuarios o administradores de sistemas deben conocer de antemano qué puertos específicos son necesarios para establecer una conexión segura. La falta de estándares puede complicar la configuración y el uso de las VPN, especialmente en entornos con políticas de seguridad de red estrictas que solo permiten tráfico en puertos conocidos.
- Compatibilidad de Navegadores. Las SSL VPN túnel a menudo requieren que el navegador soporte ciertas tecnologías, como Java, JavaScript, ActiveX, aplicaciones Flash, o determinados plugins, para funcionar correctamente. Sin embargo, no todos los navegadores tienen el mismo nivel de soporte para estas tecnologías, y algunos pueden ser incompatibles con las funciones específicas que la VPN necesita para operar. Esto puede obligar a los usuarios a utilizar un navegador específico, limitando su libertad de elección y posiblemente afectando su experiencia de usuario. La dependencia de tecnologías que requieren plugins o complementos adicionales también plantea preocupaciones de seguridad, ya que estos pueden ser vulnerables a ataques o explotaciones.

Túneles cifrados

Introducción

Un túnel cifrado en el contexto de redes informáticas es un método de transmisión de datos entre dos redes de manera segura. Este proceso implica la "encapsulación" de un protocolo de red dentro de otro, permitiendo que los datos viajen seguros y privados a través de una red pública como Internet. La encapsulación funciona al envolver los datos originales en un paquete adicional de datos, con información sobre cómo deben ser transmitidos y procesados, similar a poner un sobre dentro de otro en el mundo físico.

Este enfoque es fundamental para la creación y operación de las VPNs, que permiten establecer conexiones seguras y cifradas a través de Internet, como si estuvieran en la misma red privada. Los túneles cifrados aseguran que la información enviada sea inaccesible e ilegible para cualquiera que intente interceptarla, ya que la información viaja cifrada.

Dentro de los protocolos de tunelado que incluyen cifrado, los más comunes son SSL (Secure Sockets Layer), IPSec (Internet Protocol Security) y SSH (Secure Shell). Estos protocolos no solo transportan datos de manera segura, sino que también los cifran para proteger la información de accesos no autorizados.

Aunque existen otros protocolos de tunelado como el GRE (Generic Routing Encapsulation), que no incluyen cifrado por defecto, se utilizan principalmente para encapsular diferentes tipos de tráfico de red a través de entornos incompatibles, como la transición de IPv6 a IPv4. Sin embargo, la seguridad puede mejorarse mediante la implementación de capas adicionales de cifrado.

Los túneles cifrados son esenciales para la seguridad en la comunicación de datos a través de redes no seguras, proporcionando una base sólida sobre la cual operan las VPNs modernas, permitiendo la comunicación segura y privada entre dispositivos separados por Internet.

Túneles cifrados

Protocolos

PPTP (Protocolo de Túnel Punto a Punto) es un protocolo de red que permite la implementación de redes privadas virtuales (VPN) de manera segura entre dos puntos a través de una red pública, como Internet. Desarrollado por un consorcio fundado por Microsoft, PPTP se utilizó por primera vez en Windows 95. El protocolo permite a los usuarios acceder a una red corporativa de forma segura desde una ubicación remota, creando un túnel privado y cifrado a través de Internet.

El funcionamiento de PPTP se basa en encapsular los paquetes de datos del protocolo de punto a punto (PPP) dentro de paquetes IP (Internet Protocol) para su transmisión a través de la red. Aunque inicialmente PPTP no incluía cifrado por sí mismo, se podía combinar con el cifrado Microsoft Point-to-Point Encryption (MPPE) para proporcionar una capa de seguridad adicional a las conexiones.

Uno de los principales beneficios de PPTP es su simplicidad y facilidad de implementación, ya que es soportado de forma nativa por una amplia gama de dispositivos y sistemas operativos, incluyendo Windows, macOS, y algunas versiones de Linux, lo que facilita la configuración de conexiones VPN para los usuarios.

Sin embargo, con el paso del tiempo, PPTP ha sido criticado por sus vulnerabilidades de seguridad. Las debilidades en su algoritmo de cifrado y otros aspectos de seguridad han sido expuestas, lo que ha llevado a que muchos expertos en seguridad desaconsejen su uso para la protección de datos sensibles. Protocolos más modernos y seguros, como L2TP/IPSec, OpenVPN, o IKEv2, han ganado popularidad para la creación de VPNs debido a sus mejoras en la seguridad y la privacidad.

Túneles cifrados

Protocolos

PPTP (Protocolo de Túnel Punto a Punto)

Ventajas

- Rapidez: Es uno de los protocolos VPN más rápidos disponibles.
- Facilidad de configuración: Simple y fácil de implementar en varios dispositivos.
- Compatibilidad: Es prácticamente compatible con todos los sistemas operativos y dispositivos.
- Disponibilidad: Ampliamente soportado por una variedad de proveedores de servicios VPN.

Desventajas

- Seguridad limitada: Considerado como menos seguro en comparación con protocolos VPN más recientes debido a vulnerabilidades conocidas.
- Estabilidad cuestionable: Problemas de estabilidad pueden surgir en algunas configuraciones, especialmente en conexiones de larga duración.
- Capacidad de bloqueo: Algunos servicios y redes pueden bloquear el tráfico PPTP debido a su reputación de seguridad inferior.
- Limitaciones de cifrado: Ofrece opciones de cifrado limitadas en comparación con protocolos más modernos.

Túneles cifrados

Protocolos

L2F, o Layer 2 Forwarding, es un protocolo de tunelado desarrollado por Cisco Systems para soportar la creación de túneles VPN (Red Privada Virtual). L2F fue uno de los primeros protocolos diseñados para permitir que las conexiones de red privadas se extendieran a través de una red pública, como Internet, permitiendo así que los datos viajen de manera segura entre dos puntos a través de un "túnel" cifrado.

Este protocolo opera en la capa 2 del modelo OSI (Interconexión de Sistemas Abiertos), lo que significa que trabaja con marcos de datos (frames) antes de que sean convertidos en paquetes para su transmisión a través de la red. Al funcionar en esta capa, L2F es capaz de encapsular y enviar datos sin importar el tipo de protocolo de la capa 3 utilizado, lo que lo hace bastante versátil para transportar diferentes tipos de tráfico de red a través de un túnel VPN.

Una de las principales características de L2F es que no proporciona por sí mismo mecanismos de cifrado o autenticación. En su lugar, se espera que estas funciones sean proporcionadas por otros medios, como un protocolo de cifrado separado o a través de la seguridad inherente en la red privada a la que se accede a través del túnel.

L2F ha sido en gran parte superado por protocolos más nuevos y más seguros como L2TP (Layer 2 Tunneling Protocol), que combina características de L2F y PPTP (Protocolo de Túnel Punto a Punto) de Microsoft, incluyendo soporte para mecanismos de cifrado y autenticación. L2TP ha sido adoptado como un estándar de la industria y es ampliamente utilizado en la actualidad para la creación de VPNs, mientras que L2F es menos común y se considera obsoleto para nuevos desarrollos.

Túneles cifrados

Protocolos

L2F, o Layer 2 Forwarding,

Ventajas

- Compatibilidad: L2F es compatible con una amplia gama de sistemas y dispositivos, lo que facilita su implementación en diversas infraestructuras de red.
- Facilidad de implementación: Es relativamente fácil de configurar y desplegar, lo que lo hace accesible incluso para usuarios menos experimentados.
- Flexibilidad: Permite a los usuarios acceder a redes privadas virtuales (VPN) a través de conexiones de red pública, lo que proporciona flexibilidad en el acceso remoto.

Desventajas

- Falta de encriptación: L2F no proporciona cifrado por sí mismo, lo que puede hacer que los datos sean susceptibles a ataques de interceptación y comprometer la seguridad de la red.
- Dependencia de otro protocolo de cifrado: Para garantizar la seguridad de la comunicación, L2F necesita depender de otros protocolos de cifrado, lo que puede aumentar la complejidad y los costos de implementación.
- Limitaciones de escalabilidad: Puede enfrentar desafíos en entornos de red más grandes debido a limitaciones en la capacidad de escalabilidad y gestión de conexiones simultáneas.

Túneles cifrados

Protocolos

IPSec (Internet Protocol Security) es un conjunto de protocolos cuya función es asegurar las comunicaciones a través de redes IP mediante la autenticación y el cifrado de cada paquete de datos en una sesión de comunicación. IPSec puede ser utilizado para proteger flujos de datos entre un par de hosts (modo transporte), entre un par de redes (modo túnel), o entre un host y una red.

IPSec opera en la capa de red del modelo OSI, lo que le permite ofrecer seguridad a nivel de paquete, lo que significa que la seguridad se aplica a los paquetes de datos antes de que estos sean transmitidos y después de que son recibidos. Por esta razón, IPSec es ampliamente utilizado para establecer VPNs (Redes Privadas Virtuales), ya que permite la creación de conexiones seguras y cifradas sobre Internet.

Los componentes clave de IPSec incluyen:

- AH (Authentication Header): Proporciona autenticación de la fuente y garantiza la integridad de los datos, pero no cifra la información. Ayuda a proteger contra la manipulación de los paquetes de datos.
- ESP (Encapsulating Security Payload): Proporciona confidencialidad (cifrado de datos), así como autenticación de origen e integridad de los datos. Es el componente más utilizado para la mayoría de las aplicaciones de IPSec porque cifra el contenido del paquete para ocultarlo de cualquier persona excepto del destinatario.
- IKE (Internet Key Exchange): Es un protocolo utilizado para establecer una seguridad compartida y una gestión de claves entre dos partes que comunican. IKE permite que los hosts negocien IPSec SA (Security Association) sin la necesidad de intervención manual, proporcionando una forma de cambiar las claves y cifrados utilizados para proteger los datos transmitidos.

Túneles cifrados

Protocolos

IPSec (Internet Protocol Security)

IPSec soporta dos modos de operación:

- Modo Transporte: En este modo, solo se cifra el payload (contenido) del paquete IP, dejando intactos los encabezados del paquete original. Este modo se utiliza principalmente para la comunicación de extremo a extremo entre dos sistemas.
- Modo Túnel: En este modo, el paquete IP original se cifra y se encapsula en un nuevo paquete IP, con un nuevo encabezado. Esto protege la identidad de los paquetes de datos originales, haciendo este modo ideal para usar en VPNs, donde se requiere privacidad para la transferencia de datos entre diferentes redes.

Túneles cifrados

Protocolos

IPSec (Internet Protocol Security)

Ventajas

- Seguridad robusta: IPSec ofrece un alto nivel de seguridad mediante la autenticación y el cifrado de datos, lo que garantiza la confidencialidad e integridad de la información transmitida.
- Compatibilidad: Es compatible con una amplia gama de dispositivos y sistemas operativos, lo que facilita su implementación en entornos heterogéneos.
- Flexibilidad: IPSec puede utilizarse tanto para conexiones de sitio a sitio como para conexiones de cliente a sitio, lo que brinda flexibilidad en la configuración de redes privadas virtuales (VPN).

Desventajas

- Configuración compleja: Configurar IPSec puede ser complejo y requerir conocimientos técnicos avanzados, lo que puede dificultar su implementación para usuarios menos experimentados.
- Posibles problemas de interoperabilidad: En entornos donde se utilizan diferentes implementaciones de IPSec, pueden surgir problemas de interoperabilidad que dificulten la conectividad entre sistemas.
- Rendimiento: Aunque IPSec proporciona un alto nivel de seguridad, el procesamiento adicional necesario para cifrar y descifrar datos puede afectar al rendimiento de la red.

Túneles cifrados

Protocolos

L2TP (Layer 2 Tunneling Protocol) es un protocolo de red que se utiliza para soportar redes privadas virtuales (VPNs) o como parte de la entrega de servicios por ISPs. Combina características de dos protocolos: el Protocolo de Punto a Punto (PPP) y el Protocolo de Reenvío de Capa 2 (L2F) desarrollado por Cisco. A diferencia de PPTP, que solo permite el encapsulamiento de paquetes PPP, L2TP permite el encapsulamiento de paquetes PPP sobre varios tipos de medios, incluidas IP, Frame Relay y ATM.

Una característica distintiva de L2TP es que no proporciona cifrado ni confidencialidad por sí mismo. Sin embargo, se utiliza comúnmente en combinación con IPSec (Internet Protocol Security) para añadir una capa de seguridad a través del cifrado. Esto se debe a que, mientras L2TP encapsula los datos, IPSec se encarga de su cifrado y autenticación, proporcionando una solución segura para el tráfico de VPN.

L2TP utiliza el concepto de "túneles" para pasar datos. Un túnel L2TP es una conexión controlada entre dos puntos finales sobre una red pública (como Internet), donde el intercambio de paquetes PPP se encapsula dentro de paquetes L2TP y luego se envían a través del túnel. Este proceso ayuda a mantener la privacidad de los datos al pasar a través de una red pública.

En una sesión L2TP, dos tipos de mensajes se intercambian entre los puntos finales: mensajes de control para gestionar la sesión y mensajes de datos para el contenido de la comunicación. L2TP establece una sesión de control antes de comenzar a enviar paquetes de datos.

Los usos comunes de L2TP incluyen:

- Establecimiento de VPNs para conectar sucursales de una empresa a través de Internet.
- Permitir a los empleados acceder a la red corporativa de forma remota.
- Los ISPs lo utilizan para permitir el acceso a internet a través de una red VPN para mejorar la seguridad.

Túneles cifrados

Protocolos

L2TP (Layer 2 Tunneling Protocol)

Ventajas

- Compatibilidad: L2TP es compatible con una amplia variedad de dispositivos y sistemas operativos, lo que facilita su implementación en diferentes entornos.
- Seguridad: Al combinarse con IPSec, L2TP proporciona un nivel adicional de seguridad, garantizando la confidencialidad e integridad de los datos transmitidos.
- Estabilidad: Es conocido por ser estable y confiable, lo que lo hace adecuado para aplicaciones que requieren una conexión constante y sin interrupciones.

Desventajas

- Velocidad: En comparación con otros protocolos VPN, L2TP puede ser más lento debido al proceso adicional de encapsulación y cifrado de datos.
- Bloqueos potenciales: Algunos servicios de redes pueden bloquear fácilmente las conexiones L2TP/IPSec, lo que puede dificultar su uso en determinados entornos.
- Configuración más compleja: La configuración de L2TP puede ser más compleja que otros protocolos VPN, lo que puede requerir un nivel de experiencia técnica más avanzado para su implementación.

Túneles cifrados

Protocolos

SSL VPN (Secure Sockets Layer Virtual Private Network) es una forma de VPN que proporciona acceso remoto seguro a los recursos de una red corporativa a través de una conexión cifrada. A diferencia de las VPN tradicionales que utilizan protocolos como IPsec o L2TP, las SSL VPN utilizan el protocolo SSL (o su sucesor TLS - Transport Layer Security) para asegurar la conexión. Esto es significativo porque el SSL/TLS está profundamente integrado en la mayoría de los navegadores web modernos, lo que permite a los usuarios establecer una conexión segura sin la necesidad de instalar software cliente adicional.

Las VPN SSL se pueden implementar de dos maneras principales:

- VPN SSL Portal: Este enfoque permite al usuario acceder a una página web segura (el portal) a través de su navegador web. Después de autenticarse, el usuario puede acceder a aplicaciones y servicios específicos que se presentan dentro de este portal. Este método es ideal para proporcionar acceso a recursos específicos y es fácil de usar.
- VPN SSL Túnel: A diferencia del portal, que proporciona acceso a aplicaciones seleccionadas a través de una página web, una VPN SSL de túnel ofrece al usuario acceso a la red completa a través de una aplicación cliente descargable o a través de un navegador habilitado para SSL. Esto permite una experiencia más integrada y es útil para usuarios que necesitan un acceso más amplio a la red.

Una de las ventajas principales de las SSL VPN es su compatibilidad y facilidad de uso. Dado que se basan en el SSL/TLS, que es soportado por casi todos los navegadores web, los usuarios pueden acceder de forma segura a sus redes corporativas desde cualquier computadora o dispositivo móvil sin configuraciones especiales. Además, SSL VPN proporciona un gran nivel de seguridad mediante cifrado de extremo a extremo, autenticación sólida y, en muchos casos, funcionalidades adicionales como la inspección de contenido y la protección contra malware.

Sin embargo, también hay consideraciones a tener en cuenta con las SSL VPN, como la seguridad del navegador del cliente y la posible limitación del control sobre el cliente en comparación con las soluciones VPN basadas en IPsec.

Túneles cifrados

Protocolos

SSL VPN (Secure Sockets Layer Virtual Private Network)

Ventajas

- Seguridad: SSL VPN ofrece un alto nivel de seguridad al utilizar tecnologías estándar como SSL/TLS para cifrar el tráfico y proteger la información confidencial.
- Acceso Remoto: Permite a los usuarios acceder a la red corporativa de forma segura desde cualquier ubicación, utilizando un navegador web estándar, lo que facilita el acceso remoto a recursos corporativos.
- Facilidad de Implementación: No requiere la instalación de software adicional en los dispositivos cliente, ya que utiliza navegadores web estándar para establecer la conexión VPN, lo que simplifica su implementación y administración.

Desventajas

- Dependencia del Navegador: Requiere que los dispositivos cliente tengan un navegador web para establecer la conexión VPN, lo que puede limitar la accesibilidad en dispositivos que no admiten navegadores web o en entornos controlados donde el uso del navegador está restringido.
- Rendimiento: En comparación con otros tipos de VPN, SSL VPN puede tener un rendimiento inferior debido al cifrado adicional y la encapsulación del tráfico, lo que puede provocar una menor velocidad de conexión.

Túneles cifrados

Protocolos

VPNaaS, abreviatura de "Virtual Private Network as a Service" (Red Privada Virtual como Servicio), es una solución que permite a las organizaciones acceder de forma segura a su red y recursos digitales desde cualquier ubicación, mediante un servicio basado en la nube. Este modelo de servicio elimina la necesidad de que las empresas instalen y mantengan su propia infraestructura de VPN, simplificando la gestión y reduciendo los costos asociados.

El servicio VPNaaS proporciona funcionalidades de VPN a través de la nube, lo que significa que los usuarios pueden conectarse a la red de su empresa de forma segura y cifrada a través de Internet. Esto es especialmente útil para fuerzas laborales remotas y distribuidas, ya que permite un acceso seguro a aplicaciones, datos y otros recursos de red como si estuvieran conectados directamente a la red local de la empresa.

Algunas características clave de VPNaaS incluyen:

- Acceso remoto seguro: Los usuarios pueden acceder a la red de su empresa desde cualquier lugar, siempre que tengan una conexión a Internet, manteniendo la seguridad de los datos mediante el cifrado.
- Escalabilidad: VPNaaS puede escalar fácilmente para adaptarse al crecimiento de una empresa, permitiendo agregar más usuarios o recursos según sea necesario sin una inversión significativa en hardware o infraestructura.
- Gestión simplificada: Al ser un servicio basado en la nube, VPNaaS reduce la carga de gestión y mantenimiento de la infraestructura de VPN, ya que el proveedor del servicio se encarga de estos aspectos.
- Compatibilidad y flexibilidad: VPNaaS suele ser compatible con una amplia gama de dispositivos y sistemas operativos, lo que permite a los empleados utilizar sus propios dispositivos (BYOD) para acceder a la red de la empresa.

BYOD significa "Bring Your Own Device", que se traduce al español como "Trae tu propio dispositivo". Es una política empresarial que permite a los empleados llevar dispositivos personales (teléfonos, tabletas, laptops) al lugar de trabajo y utilizarlos para acceder a recursos de la empresa, como el correo electrónico, archivos y aplicaciones.

Túneles cifrados

Protocolos

VPNaaS, abreviatura de "Virtual Private Network as a Service" (Red Privada Virtual como Servicio)

Ventajas

- Acceso Remoto Seguro: VPNaaS (VPN as a Service) permite a los usuarios acceder de forma segura a la red corporativa desde ubicaciones remotas, garantizando la protección de datos confidenciales durante la transferencia de información.
- Facilidad de Implementación: Al ser un servicio en la nube, VPNaaS ofrece una implementación rápida y sencilla, sin necesidad de configuraciones complejas de hardware o software, lo que reduce los costos operativos y el tiempo de implementación.
- Escalabilidad: Los servicios VPN como VPNaaS son altamente escalables, lo que permite adaptarse fácilmente a las necesidades cambiantes de la empresa, ya sea para agregar nuevos usuarios o expandir la infraestructura de red según sea necesario.

Desventajas

- Dependencia de Proveedor: El funcionamiento y la disponibilidad de VPNaaS están sujetos al proveedor del servicio, lo que puede generar preocupaciones sobre la confidencialidad y la privacidad de los datos almacenados en servidores de terceros.
- Rendimiento Variado: La calidad del rendimiento de VPNaaS puede variar dependiendo de la infraestructura y la capacidad del proveedor, lo que podría afectar la velocidad y la estabilidad de la conexión VPN.

Túneles cifrados

Protocolos

IKEv2/IPSec (Intercambio de Claves por Internet versión 2 / Protocolo de Seguridad IP) es una combinación de dos tecnologías de seguridad que se emplean para establecer conexiones VPN seguras.

IKEv2 (Intercambio de Claves por Internet v2) es la segunda versión del protocolo IKE, que se utiliza para establecer un acuerdo de seguridad y autenticar a los dos extremos de la conexión antes de que la comunicación VPN comience. Este protocolo es responsable de la negociación de los parámetros de la sesión, la gestión de las claves y la renovación de las mismas para mantener una conexión segura. IKEv2 es conocido por su capacidad de reconexión rápida, lo que lo hace útil para dispositivos móviles que cambian frecuentemente de red (por ejemplo, de datos móviles a Wi-Fi).

IPSec (Protocolo de Seguridad IP) es un conjunto de protocolos que aseguran las comunicaciones sobre el protocolo IP al autenticar y cifrar cada paquete de datos de una sesión de comunicación. Funciona en la capa de red, lo que permite proteger todas las aplicaciones que transmiten datos a través de IP, sin necesidad de aplicaciones especiales. IPSec utiliza dos modos de operación: el modo de transporte, que protege los mensajes entre dos dispositivos, y el modo túnel, que protege los datos entre dos redes diferentes.

La combinación de IKEv2 con IPSec ofrece una VPN segura y confiable, proporcionando robustas capacidades de negociación de claves y cifrado de datos. Esta combinación se utiliza comúnmente en conexiones VPN corporativas debido a su seguridad mejorada y capacidad de mantener conexiones estables incluso cuando las redes subyacentes son inestables o cambian.

Túneles cifrados

Protocolos

IKEv2/IPSec (Intercambio de Claves por Internet versión 2 / Protocolo de Seguridad IP)

Ventajas:

- Estabilidad en conexiones móviles: Funciona bien al cambiar entre redes (por ejemplo, de Wi-Fi a datos móviles).
- Soporte nativo: Muchos sistemas operativos tienen soporte integrado.
- Seguridad: Utiliza una variedad de algoritmos de cifrado fuertes.

Desventajas:

- Bloqueo: Puede ser bloqueado por ciertos firewalls debido al uso del puerto 500.
- Configuración: Puede ser complejo de configurar sin herramientas adicionales.

Túneles cifrados

Protocolos

OpenVPN es un protocolo de VPN de código abierto utilizado para crear conexiones seguras en Internet. Es uno de los protocolos más seguros y versátiles disponibles, siendo compatible con una gran variedad de dispositivos y sistemas operativos. La fortaleza de OpenVPN reside en su capacidad para funcionar a través de cualquier puerto, lo que significa que puede ser configurado para eludir firewalls y redes que bloquean puertos específicos.

El protocolo utiliza la biblioteca OpenSSL, que brinda una robusta criptografía. Soporta múltiples métodos de autenticación, incluyendo certificados, claves precompartidas, y autenticación de usuario/contraseña.

Además, OpenVPN es capaz de atravesar Network Address Translators (NAT) y firewalls, ya que puede encapsular el tráfico en una capa TLS/SSL, ofreciendo una conexión segura de punto a punto o de sitio a sitio.

La naturaleza de código abierto de OpenVPN permite que sea ampliamente auditado y examinado por seguridad, lo que es una ventaja significativa sobre los protocolos propietarios.

Además, OpenVPN es altamente configurable, permitiendo ajustes detallados para adaptarse a diversas necesidades de red y requisitos de seguridad. Esta flexibilidad y seguridad hacen de OpenVPN una opción popular para las VPN empresariales, así como para los usuarios individuales que buscan proteger su privacidad en línea.

OpenSSL es una herramienta de código abierto para la implementación de los protocolos criptográficos SSL (Secure Sockets Layer) y TLS (Transport Layer Security). El proyecto OpenSSL incluye una biblioteca de criptografía que ofrece una amplia gama de funciones criptográficas, tales como algoritmos de cifrado y descifrado, generación de certificados digitales y llaves criptográficas, así como herramientas para la creación y gestión de estos componentes criptográficos.

OpenSSL es ampliamente utilizado por aplicaciones y servidores web para habilitar comunicaciones cifradas y es conocido por ser utilizado en sistemas operativos basados en Unix y Linux, aunque también es compatible con otros sistemas, incluyendo Windows. Es una parte integral de muchos servicios en la web, proporcionando medidas de seguridad para proteger contra el espionaje electrónico y otros tipos de ataques informáticos.

Túneles cifrados

Protocolos

OpenVPN

Ventajas:

- Alta seguridad: Utiliza bibliotecas de criptografía fuerte.
- Alta configurabilidad: Se puede configurar para satisfacer necesidades específicas.
- Compatibilidad: Funciona en la mayoría de los sistemas operativos.
- Gran comunidad: Al ser de código abierto, tiene una comunidad activa y muchos recursos.

Desventajas:

- Complejidad de configuración: Puede ser complejo de configurar para usuarios no técnicos.
- Velocidad: A veces puede ser más lento que otras alternativas debido a su complejidad criptográfica.

Túneles cifrados

Protocolos

SoftEther VPN (Software Ethernet VPN) es una de las soluciones de VPN más poderosas y fáciles de usar que existen. Es un software de código abierto desarrollado por la Universidad de Tsukuba en Japón. SoftEther es reconocido por su versatilidad y rendimiento ya que puede correr sobre diferentes sistemas operativos como Windows, Linux, Mac, FreeBSD y Solaris.

SoftEther VPN utiliza SSL (Secure Sockets Layer) para cifrar el tráfico de la red, lo que lo hace muy seguro. Una de sus principales ventajas es que permite la creación de VPNs tanto a nivel de sitio a sitio como de acceso remoto.

También es compatible con diferentes protocolos de VPN como L2TP/IPsec, OpenVPN, MS-SSTP y su propio protocolo VPN que también utiliza SSL/TLS para el intercambio de claves, pero se dice que es más rápido y estable que otros protocolos.

Este software se destaca por ser bastante fácil de configurar y administrar, y su arquitectura de multi-hilo hace que sea muy rápido y eficiente en el manejo de múltiples conexiones simultáneas.

Además, SoftEther incluye un número de características avanzadas, tales como la resistencia al bloqueo de firewall mediante la realización de operaciones a través de un puerto TCP 443, la misma utilizada por el tráfico HTTPS, lo que hace que sea difícil de bloquear.

No necesita que el servidor tenga IP Fija, ya que que SoftEther cuenta con su propio sistema de DNS dinámico.

Túneles cifrados

Protocolos

SoftEther VPN (Software Ethernet VPN)

Ventajas:

- Flexibilidad: Soporta múltiples protocolos VPN, incluyendo SSTP, L2TP/IPsec y OpenVPN.
- Plataformas múltiples: Compatible con una variedad de sistemas operativos.
- Cifrado fuerte: Proporciona seguridad robusta.

Desventajas:

- Complejidad: Puede ser complejo para usuarios principiantes.
- Adopción: No tan ampliamente adoptado como OpenVPN o IPSec.

Túneles cifrados

Protocolos

WireGuard es un protocolo de VPN relativamente nuevo y moderno que busca ofrecer mejores velocidades y una criptografía más fiable que sus predecesores como IPSec y OpenVPN. Es conocido por su diseño simple y por ofrecer un alto rendimiento. WireGuard fue desarrollado con el objetivo de ser fácil de configurar, rápido y seguro.

El protocolo utiliza criptografía de última generación y ha sido elogiado por su capacidad para proporcionar conexiones seguras manteniendo una huella mínima de código, lo cual lo hace fácil de revisar y auditar. WireGuard se ejecuta como un módulo dentro del núcleo de Linux, lo que le proporciona una velocidad superior. También está disponible en otros sistemas operativos y plataformas.

Una de las ventajas clave de WireGuard es que solo usa una clave pública para establecer una conexión segura con un servidor VPN, simplificando la gestión de claves en comparación con otros protocolos. Además, está diseñado para automatizar y simplificar el proceso de manejo de conexiones, reduciendo la posibilidad de errores humanos durante la configuración.

¿Cómo funciona?

- Cifrado moderno: WireGuard utiliza técnicas de cifrado contemporáneas como Curve25519 para el intercambio de claves, ChaCha20 para el cifrado simétrico, Poly1305 para la autenticación de mensajes y BLAKE2s para el hashing.
- Intercambio de claves: Antes de establecer la comunicación, WireGuard intercambia claves públicas entre el cliente y el servidor, de forma similar a como se hace con SSH. Esto facilita la creación de túneles VPN seguros sin la necesidad de complejas configuraciones de certificados.
- Establecimiento de túneles: Una vez que las claves se han intercambiado y verificado, se establece un túnel seguro por donde pueden viajar los datos. El proceso es bastante eficiente y se realiza prácticamente sin intervención del usuario.

Túneles cifrados

Protocolos

WireGuard ¿Cómo funciona?

- Minimalismo: El código de WireGuard es intencionalmente minimalista, lo que lo hace fácil de auditar y menos propenso a errores de seguridad. Tiene aproximadamente 4.000 líneas de código, en comparación con las decenas de miles de líneas que componen otros protocolos VPN.
- Velocidad y rendimiento: Al estar integrado en el kernel de sistemas operativos como Linux, WireGuard puede ofrecer altas velocidades y un rendimiento consistente, superando a menudo a otros protocolos en términos de rapidez y eficiencia.
- Mantenimiento de la conexión: WireGuard maneja muy bien los cambios en la conexión, como el traspaso de datos entre datos móviles y Wi-Fi o el cambio de IP en redes móviles. Esto hace que sea una opción robusta para conexiones en dispositivos móviles que cambian frecuentemente de red.
- Operación en cualquier puerto: WireGuard opera sobre UDP y puede configurarse para usar cualquier puerto, incluido el puerto 53, que es el utilizado para el DNS, lo que puede ayudar a evitar ciertos tipos de bloqueos de red.

Túneles cifrados

Protocolos

WireGuard

Ventajas

- Eficiencia y Ligereza: WireGuard es conocido por su eficiencia y ligereza, con aproximadamente 4000 líneas de código, lo que lo hace más fácil de auditar y mantener en comparación con otros protocolos VPN más complejos.
- Mayor Rendimiento: Proporciona un mejor rendimiento en términos de velocidad y latencia en comparación con protocolos como IPsec y OpenVPN, lo que lo hace ideal para conexiones VPN rápidas y estables.
- Seguridad Avanzada: Ofrece características de seguridad avanzadas, incluyendo cifrado robusto y autenticación de claves, lo que garantiza la privacidad y la integridad de los datos transmitidos a través de la red VPN.

Desventajas

- Falta de Amplia Adopción: Aunque WireGuard está ganando popularidad, aún no ha sido ampliamente adoptado en comparación con protocolos VPN más establecidos como OpenVPN, lo que puede limitar su disponibilidad en algunas plataformas y servicios VPN.
- Compatibilidad Limitada: Aunque es compatible con una variedad de sistemas operativos, la compatibilidad total de WireGuard puede ser limitada en comparación con protocolos más establecidos, lo que puede dificultar su implementación en ciertos entornos de red.

Costes de implantación

Los posibles costos de implantación de una VPN pueden variar según varios factores, incluyendo el tipo de VPN (por ejemplo, VPN basada en hardware o software), el proveedor de servicios elegido y el alcance del despliegue. Aquí están algunos costos potenciales:

- Costos de Hardware o Software: Dependiendo de si se elige una solución VPN basada en hardware o software, puede haber costos asociados con la adquisición de hardware especializado o licencias de software VPN. Estos costos pueden incluir routers VPN, servidores VPN, o software VPN para dispositivos cliente.
- Costos de Configuración e Implementación: Pueden surgir costos relacionados con la configuración inicial y la implementación de la VPN. Esto podría implicar horas de trabajo de personal técnico para configurar y conectar los dispositivos, así como realizar pruebas para garantizar un funcionamiento correcto.
- Costos de Mantenimiento: Es importante considerar los costos continuos de mantenimiento, que pueden incluir actualizaciones de software, parches de seguridad, y el monitoreo y la gestión continua de la red VPN para garantizar su rendimiento y seguridad óptimos.
- Costos de Ancho de Banda: Dependiendo del proveedor de servicios y del nivel de tráfico de red esperado, puede haber costos asociados con el uso de ancho de banda para la transmisión de datos a través de la VPN. Algunos proveedores cobran por el uso de datos transmitidos a través de la red VPN.
- Costos de Capacitación: Si se requiere capacitación para el personal sobre el uso y la administración de la VPN, estos costos también deben ser considerados. Esto puede incluir la capacitación del personal en la configuración de clientes VPN o en la resolución de problemas relacionados con la conexión VPN.

Resumen

El establecimiento de canales seguros de comunicación es fundamental para el intercambio de datos. Las redes privadas virtuales (VPN) y los túneles de cifrado son esenciales para ello, permitiendo comunicaciones seguras entre entidades o usuarios sin necesidad de estar físicamente en la misma red. Protocolos como IPSec, SSL y SSH posibilitan su establecimiento.

IPSec opera en la capa de red y consta de los protocolos de Internet Key Exchange (IKE) y Encapsulating Security Payload (ESP). SSL, en cambio, opera en la capa de transporte e incluye los protocolos de Registro, Saludo, Cambio de especificación de cifrado y Aviso. SSH, también en la capa de transporte, es un protocolo de autenticación remota que incluye los protocolos de Capa de transporte, Autenticación de usuarios y Conexión.

Dos de las alternativas de VPN más comunes son VPN SSL y VPN IPSec. La elección entre ellas depende del contexto y las necesidades del usuario. Las VPN SSL son atractivas porque son discretas y utilizan el navegador web para establecer comunicaciones entre extremos.