**Honeynet**

**Parte uno. División uno.**

**Antecedentes.**

Durante los últimos años las intrusiones, así como los ataques informáticos, han ido en aumento de forma considerable. De la misma forma, han venido acompañados con una clara evolución respecto a las herramientas y técnicas utilizadas por los atacantes.

Entre los responsables de estas situaciones son usuarios avanzados que desarrollan sus propias aplicaciones y tienen la capacidad para introducirse dentro de otros sistemas gracias a la creación sofisticadas puertas traseras con tal de introducirse hacia otros sistemas.

Debido al hecho de que los ataques más sonados son sin dudas los de grandes corporativas, hace pues, que el público considere que estos intrusos solo tengan como foco de ataque aquellos equipos que contengan información trascendente. Sin embargo, esto es un grave error. Estos ataques selectivos dirigidos por expertos suponen un porcentaje muy pequeño de los que a diario se producen a través de la red. Por lo general, los ataques no van dirigidos contra equipos ni compañías específicas, sino que tienen como objetivo la víctima fácil. El blanco bien puede ser cualquier equipo que se encuentre conectado a la red que posea una debilidad específica que el atacante busca y es capaz de aprovechar con tal de obtener el acceso a la máquina.



En los últimos años, la frecuencia de la aparición de estos ataques indiscriminados se ha disparado, y este acontecimiento, junto al creciente número de vulnerabilidades descubiertas en todo tipo de sistemas operativos y aplicaciones, convierte a cualquier sistema conectado a Internet en una víctima potencial. Este panorama plantea la necesidad de disponer de instrumentos que permitan descubrir y analizar tanto los agujeros de seguridad que pueda presentar un sistema como las técnicas y herramientas utilizadas por la comunidad de atacantes que pueblan la Red.

Bajo este enfoque, se presenta un tipo de herramienta pensada para la detección y el análisis de ataques, donde se plantea el uso de honeypot y que este a su vez, permite generar la honeynet. Tema que nos interesa abordar.

**Parte dos. División dos.**

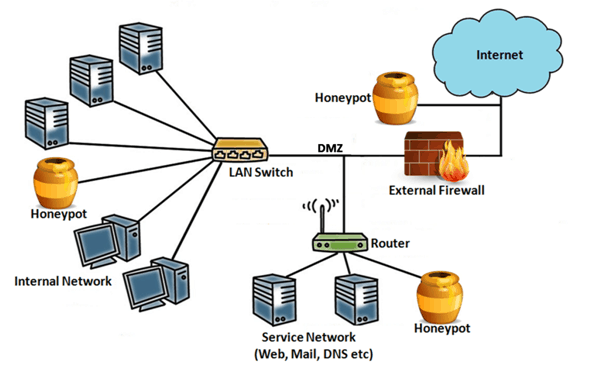
**Honeypots.**

El sistema de señuelo o bien, el honeypot, es una herramienta de seguridad diseñada para ser sondeada, atacada y comprometida, que tiene la capacidad de detectar y registrar tales acciones. Su funcionamiento se encuentra basado bajo tres simples conceptos.

1. Un honeypot no es un sistema de producción y, por tanto, nadie debería tratar de comunicarse con él. No habrá falsos positivos.
2. Cualquier tráfico que tenga por origen el honeypot significará que el sistema ha sido comprometido.

Este tipo de herramientas sirven para la ayuda en la prevención de ataques, la detección de intrusiones y la respuesta a este tipo de incidentes, siendo estas dos últimas tareas las que ofrecen mayores ventajas.

Ahora bien, entrado ya en contexto, se prosigue en hablar sobre el Honeynet, que es básicamente un honeypot, pero más complejo, ofrece un nivel de interacción más alto con el intruso, lo que permite mejorar la recopilación todavía superior a la acostumbrada bajo un ataque. Honeynet es una red completa que contiene un conjunto de sistemas dispuestos para ser atacados. Puede contener cualquier componente de red imaginable, incluyendo routers y switches, lo que le permite replicar la red de cualquier organización, no obstante, también emplea un subconjunto de honeypot para ponerse en funcionamiento así misma.



**División tres, parte tres.**

**Funcionamiento de la honeynet.**

Diseño y configuración:

Topología de red: Una honeynet suele constar de varios sistemas conectados entre sí, simulando una red real.

Sistemas operativos y servicios: Los sistemas en la honeynet pueden ejecutar diferentes sistemas operativos y servicios para atraer a una variedad de atacantes. Estos sistemas se conocen como honeypots.

Honeypots:

Sistemas de alto o bajo interacción: Los honeypots pueden ser de alto o bajo nivel de interacción. Los de alto nivel interactúan con los atacantes de manera más profunda, emulando servicios y aplicaciones reales. Los de bajo nivel simulan servicios básicos y son más seguros, pero menos informativos.

Atracción de atacantes: Los honeypots se configuran para atraer a los atacantes. Pueden simular servicios comunes como servidores web, bases de datos, sistemas de correo, etc.

Detección de actividad sospechosa:

Monitoreo de tráfico: Se implementa un sistema de monitoreo de red para registrar todo el tráfico que fluye hacia y desde la honeynet.

Análisis de registros: Los administradores analizan los registros para identificar patrones de tráfico inusuales o actividades sospechosas.

Análisis de atacantes:

Captura de malware: Si un atacante introduce malware en la honeynet, este se puede capturar y analizar para comprender sus características y métodos.

Seguimiento de tácticas y técnicas: Los expertos estudian las tácticas, técnicas y procedimientos utilizados por los atacantes para mejorar la comprensión de las amenazas.

Aprendizaje y mejora:

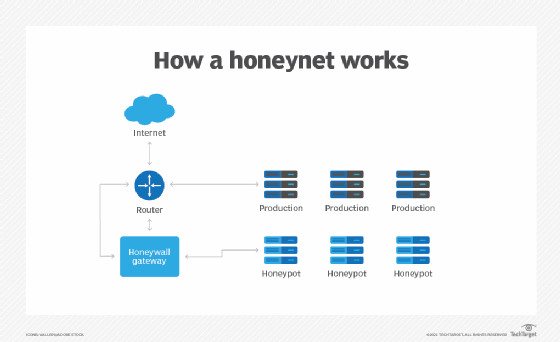
Refinamiento de la seguridad: La información recopilada se utiliza para mejorar las defensas de la red principal. Los conocimientos adquiridos permiten desarrollar medidas proactivas contra futuros ataques.

Actualizaciones de firmas y reglas: Las firmas de intrusiones y las reglas de seguridad se actualizan con la información obtenida, mejorando la capacidad de detectar y prevenir amenazas similares en el futuro.

Informes y colaboración:

Generación de informes: Se crean informes detallados sobre los ataques observados, las tácticas utilizadas y las lecciones aprendidas.

Compartir información: La información recopilada se puede compartir con la comunidad de seguridad cibernética para mejorar la conciencia y la respuesta a amenazas.



**Parte cuatro. División cuatro.**

**Implementación en un entorno virtual.**

Sin embargo, llevar a cabo esto en un conjunto de computadoras es bastante complejo y riesgoso. Por ende, se decide realizar honeynets virtuales, que son implementaciones de ataques dentro de una misma computadora, lo que facilita su aplicación haciendo que se tenga que configurar el equipo de trabajo para poder realizarlo. Entre los pasos a seguir se encuentran los siguientes.

Paso 1: Planificación y Diseño:

Objetivos: Define los objetivos de tu honeynet virtual. ¿Quieres estudiar ataques específicos, comprender tácticas de atacantes o probar la efectividad de ciertas medidas de seguridad?

Topología de red: Decide la topología de red para tu honeynet. Puedes usar una sola máquina virtual como honeypot o configurar una red de honeypots interconectados.

Paso 2: Selección de Herramientas:

Honeypot Software: Elige el software honeypot que se adapte a tus necesidades. Algunas opciones populares incluyen Honeyd, Dionaea, Snort, Cowrie, entre otros.

Plataforma de Virtualización: Decide si usarás máquinas virtuales (por ejemplo, VMware, VirtualBox) o contenedores (como Docker) para implementar tu honeynet virtual.

Paso 3: Configuración del Honeypot:

Instalación: Configura tu software honeypot en las máquinas virtuales o contenedores según las instrucciones del proveedor.

Personalización: Ajusta la configuración del honeypot según tus objetivos. Puedes simular servicios específicos, configurar señuelos y definir la interacción con atacantes.

Paso 4: Configuración de Red:

Red Interna: Configura una red interna para tu honeynet. Esto puede hacerse mediante la configuración de redes virtuales internas o segmentos de red en tu plataforma de virtualización.

Conectividad: Asegúrate de que tus honeypots puedan recibir tráfico desde la red externa o desde otros sistemas en tu entorno virtual.

Paso 5: Monitoreo y Registro:

Herramientas de Monitoreo: Utiliza herramientas de monitoreo de red y sistemas para registrar todo el tráfico que fluye hacia y desde tu honeynet.

Análisis de Registros: Implementa un sistema para analizar los registros de tus honeypots y detectar patrones de actividad sospechosa.

Paso 6: Seguridad:

Aislamiento: Asegúrate de que tu honeynet esté aislado de la red principal para evitar posibles daños.

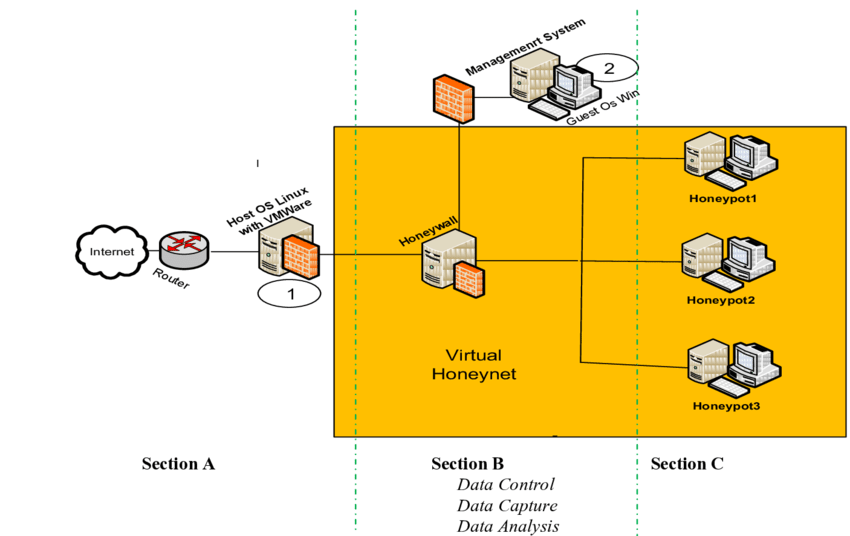
Actualizaciones: Mantén actualizado el software honeypot y el sistema operativo de tus honeypots para abordar posibles vulnerabilidades.

Paso 7: Análisis y Mejora:

Análisis de Atacantes: Examina los datos recopilados para entender las tácticas y técnicas de los atacantes.

Mejora Continua: Utiliza la información obtenida para mejorar las defensas de tu red principal y ajustar la configuración de tu honeynet.

Es fundamental recordar que la implementación de una honeynet virtual debe realizarse con precaución, ya que puede exponer sistemas a posibles riesgos de seguridad. Además, es esencial cumplir con las leyes y regulaciones pertinentes antes de realizar experimentos de este tipo.



**Establecimiento de un enlace seguro de red: Tunelización (Tunneling)**

**Parte uno, división uno.**

**Contexto.**

El tunneling VPN es una de las formas más seguras para protegerse mientras se navega en internet. Justamente, con sus infinitas posibilidades, la red global también ha traído consigo riesgos y desafíos.

Actualmente, los ataques cibernéticos a organizaciones se han vuelto más frecuentes y sofisticados. Solo en 2022, el grupo de extorsión LockBit publicó información sobre 801 organizaciones vulneradas en su web de filtraciones, un aumento del 95% en comparación con las entradas del año anterior. Este aumento en los ataques cibernéticos subraya la importancia de contar con conexiones seguras y cifradas, especialmente para las empresas y aquellos que trabajan de forma remota.

Ahí es donde entran en juego las VPN (Virtual Private Networks o Redes Privadas Virtuales), una herramienta esencial en el mundo cibernético moderno. Pero, ¿qué hace exactamente una VPN y cómo protege nuestros datos?



**Parte dos, división dos.**

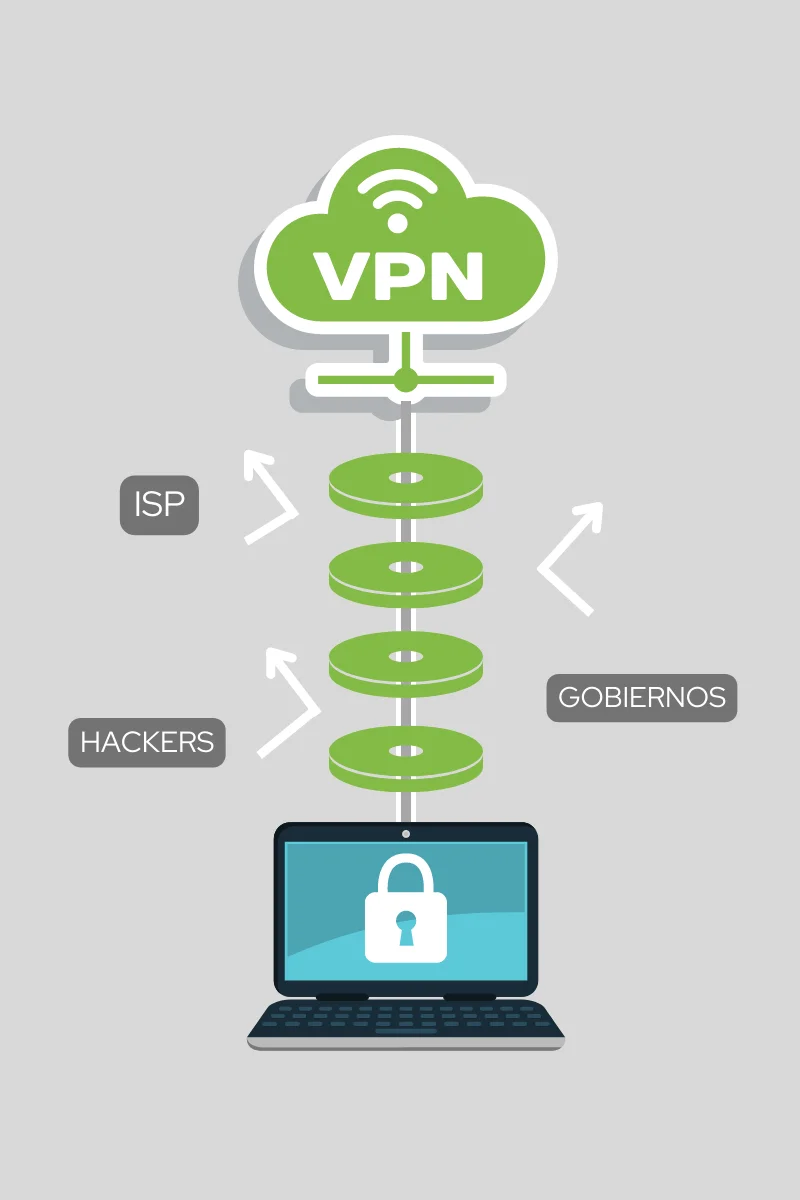
**Funcionamiento.**

Una técnica innovadora que encapsula un protocolo de red dentro de otro protocolo de red. De esta forma, se crea una suerte de túnel de información en el interior de una red de computadoras. De esta forma, se permite el transporte de un protocolo específico a través de una red que, en circunstancias regulares, no lo admitiría. Unos de los focos más interesantes de aplicar esta técnica se basan en la creación de diferentes tipos de redes privadas virtuales (VPN).

Imagina que estás en una cafetería, utilizando su red wifi pública. Sin un tunneling VPN, tu información de navegación, contraseñas y otros datos sensibles estarían expuestos. Esta tecnología comienza con la descomposición de los datos que deben viajar a través del túnel en fragmentos denominados “paquetes”. A continuación, estos paquetes se encapsulan dentro de otros paquetes de datos, un proceso que se conoce como “encapsulación”. En su esencia, esta encapsulación constituye una envoltura de protección para el contenido original, escondiendo la naturaleza de los datos transmitidos a observadores externos.

Posterior a la encapsulación, sigue la encriptación. En este paso, todos los datos encapsulados se cifran. En otras palabras, se convierten en un conjunto de caracteres aparentemente sin sentido que solo pueden volver a su formato original con la clave de descifrado adecuada. Este proceso es crucial con tal de asegurar la conexión encriptada segura y privada, protegiendo los datos de miradas indiscretas.

El túnel VPN no solo protege la información contra ataques de hackers o entidades malintencionadas, sino que también defiende la privacidad del usuario de su propio proveedor de servicios de Internet y del gobierno. El resultado es un túnel privado y seguro que guarda todos los aspectos de la actividad en línea del usuario, ya sea navegación por la web, chat o cualquier otro tráfico de red.

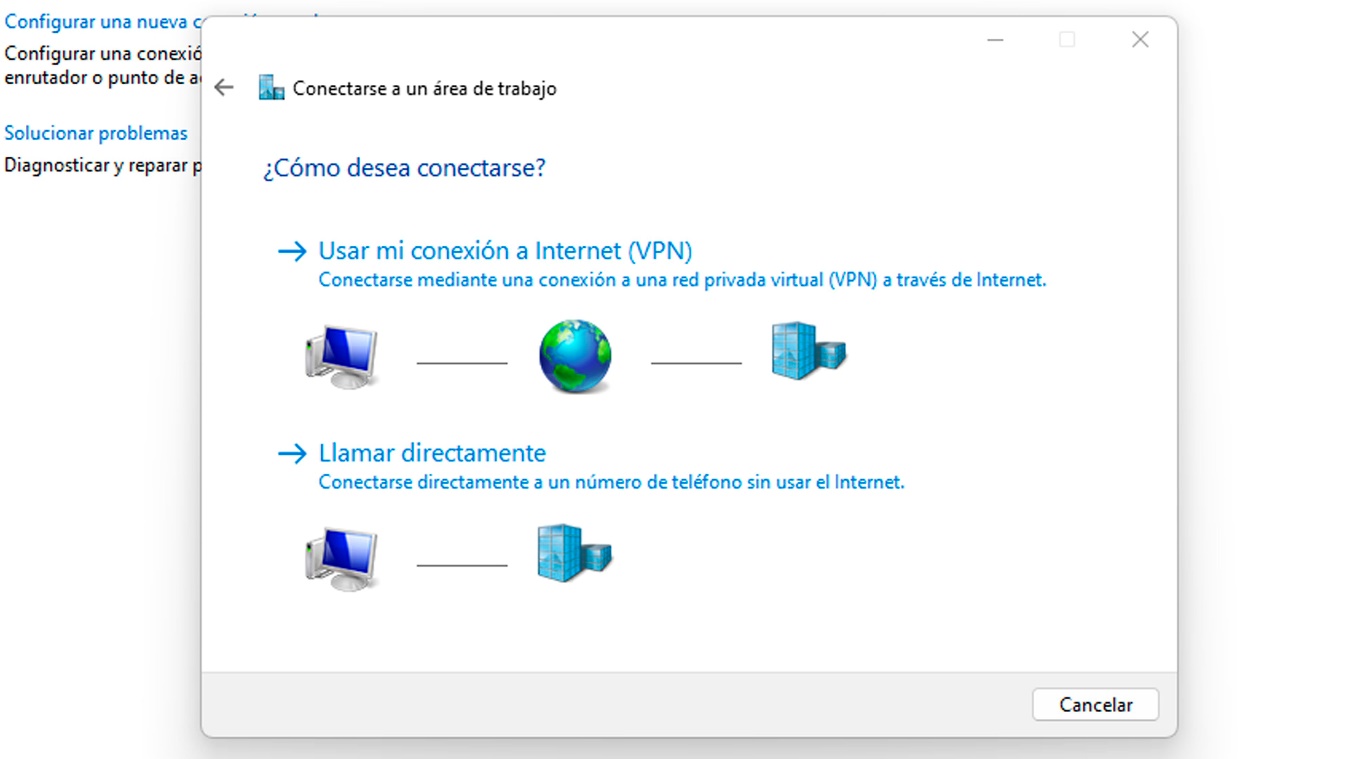


Por otro lado, es importante tener en cuenta el tipo de protocolo que ha de ser implementado. Los protocolos definen las reglas adecuadas para un tránsito seguro y fluido de los datos a través de la red. Existe una variedad de protocolos disponibles para usar, cada uno con sus propias ventajas, niveles de seguridad, velocidades y características únicas. Entre protocolos que pueden emplearse, se encuentra:

* Open VPN
* IKEv2/IPSec.
* WireGuard.
* PPTP.
* SSTP.

**Parte tres, división tres.**

**Cómo crear un túnel VPN: dos formas de hacerlo**



No todos los proveedores de VPN o sistemas operativos funcionan de la misma manera, por lo que existen diferentes maneras de crear un túnel. En este caso, te daremos dos procedimientos: uno genérico que te dará una idea de cómo funciona el proceso y otro más específico en Google Cloud.

Método general.

Elige un proveedor de servicios VPN: El primer paso es decidir qué servicio de VPN utilizarás. Hay una amplia gama de opciones disponibles, cada una con sus propias ventajas y desventajas. Algunos proveedores de servicios VPN populares son NordVPN, Hyde my Ass, Tuxler, Surfshark, entre otros.

Descarga e instala el software de VPN: Una vez que hayas seleccionado un proveedor, tendrás que descargar e instalar su software. Generalmente, puedes encontrar el software en el sitio web del proveedor.

Inicia la aplicación VPN: Después de instalar el software, tendrás que iniciar la aplicación. En la mayoría de los casos, necesitarás crear una cuenta y pagar una suscripción, aunque hay algunas VPN que ofrecen una cantidad limitada de servicios gratuitos.

Configura tu conexión VPN: Cuando inicies la aplicación por primera vez, se te pedirá que configures tu conexión VPN. Aquí, podrás seleccionar la ubicación del servidor al que deseas conectarte, así como otras configuraciones avanzadas como la selección del protocolo de túnel VPN.

Conéctate a la VPN: Una vez que hayas configurado tu conexión VPN, simplemente tendrás que hacer clic en el botón de conectar para establecer la conexión VPN. A partir de este momento, todo tu tráfico de internet estará encriptado y será redirigido a través del servidor VPN que seleccionaste.

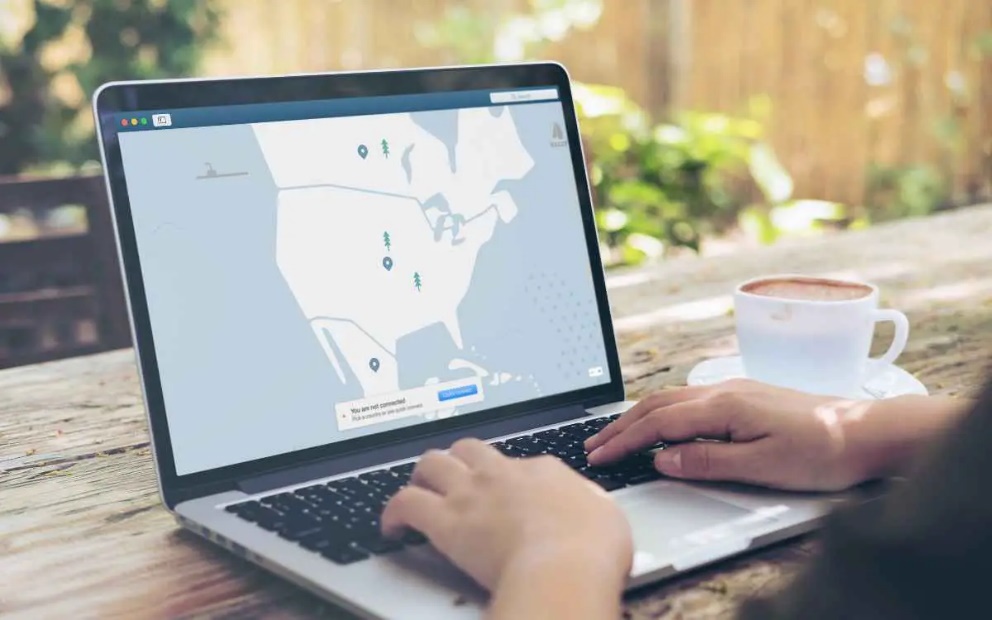
Verifica tu conexión VPN: Para asegurarte de que estás conectado a la VPN, puedes visitar un sitio web como ‘What Is My IP Address’ para confirmar que tu dirección IP ha cambiado a la ubicación del servidor VPN.

En resumen, la configuración de un túnel VPN puede variar según el proveedor y el sistema operativo, pero el procedimiento general es tal como te lo hemos explicado antes. Recuerda siempre hacer tu propia investigación para entender completamente las funciones y características del servicio de VPN que elijas.

Túnel VPN en Google Cloud

Crear un tunneling VPN puede parecer una tarea compleja, pero con una guía detallada y siguiendo las instrucciones cuidadosamente, puede ser una tarea bastante accesible. En este punto, se explica el otro método para crear un túnel VPN a través de Google Cloud.

* Primero, inicia sesión en la consola de Google Cloud y dirígete a la sección VPN. En la sección VPN, verás una opción que dice ‘Crear túnel VPN’.
* Luego, un menú desplegable te pedirá que selecciones la puerta de enlace que necesita el nuevo túnel. Una vez que hayas hecho tu selección, haz clic en ‘Continuar’.
* A continuación, tendrás que seleccionar un Cloud Router. Si no has configurado uno aún, sigue los pasos indicados en el procedimiento titulado ‘Crea túneles VPN’.
* El siguiente paso es seleccionar el tipo de Puerta de enlace de VPN de intercambio de tráfico. Aquí tendrás dos opciones: Local o ajena a Google Cloud.
* Luego, para el Nombre de la puerta de enlace de VPN de intercambio de tráfico, elige el recurso de puerta de enlace de VPN de intercambio de tráfico que utilizará el nuevo túnel. Para ver los nombres existentes de puertas de enlace de VPN de intercambio de tráfico en esta puerta de enlace de Cloud VPN, haz clic en ‘Ver todos los túneles existentes’ en la parte superior de la página. Es posible que recibas una advertencia de que un túnel con la misma interfaz de puerta de enlace de VPN de intercambio de tráfico ya está asociado con la misma interfaz de puerta de enlace local de Cloud VPN. Para solucionar este problema, en ‘Interfaz de puerta de enlace de Cloud VPN asociada’, selecciona la otra interfaz de VPN de alta disponibilidad.
* Para finalizar la configuración del túnel, completa el resto de los pasos como se indica en el procedimiento ‘Crea túneles VPN’.

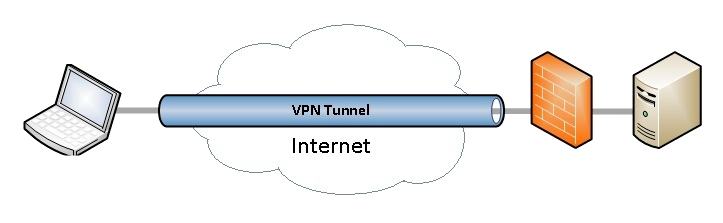


**Parte cuatro, división cuatro.**

**Conclusiones.**

En resumen, el **tunneling VPN** es una herramienta poderosa para la protección de la privacidad y la seguridad en línea. Sin embargo, su uso debe estar enmarcado siempre en el respeto por las leyes y regulaciones aplicables. Así, garantizaremos un entorno digital seguro y ético para todos.

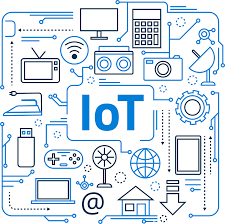
Ya sea que se busque proteger información personal o la de una empresa, un **túnel VPN**puede ofrecer esa capa adicional de seguridad. Como hemos visto, su implementación puede ser más sencilla de lo que se imagina, siempre y cuando se cuente con la guía adecuada.  
Teniendo en cuenta todos estos aspectos, el **tunneling VPN** es una gran herramienta para garantizar la privacidad y seguridad en un contexto donde las filtraciones de datos son cada vez más avanzadas.



**Internet de las cosas (IoT).**

**Parte uno, división uno.**

**Historia del IoT.**

****

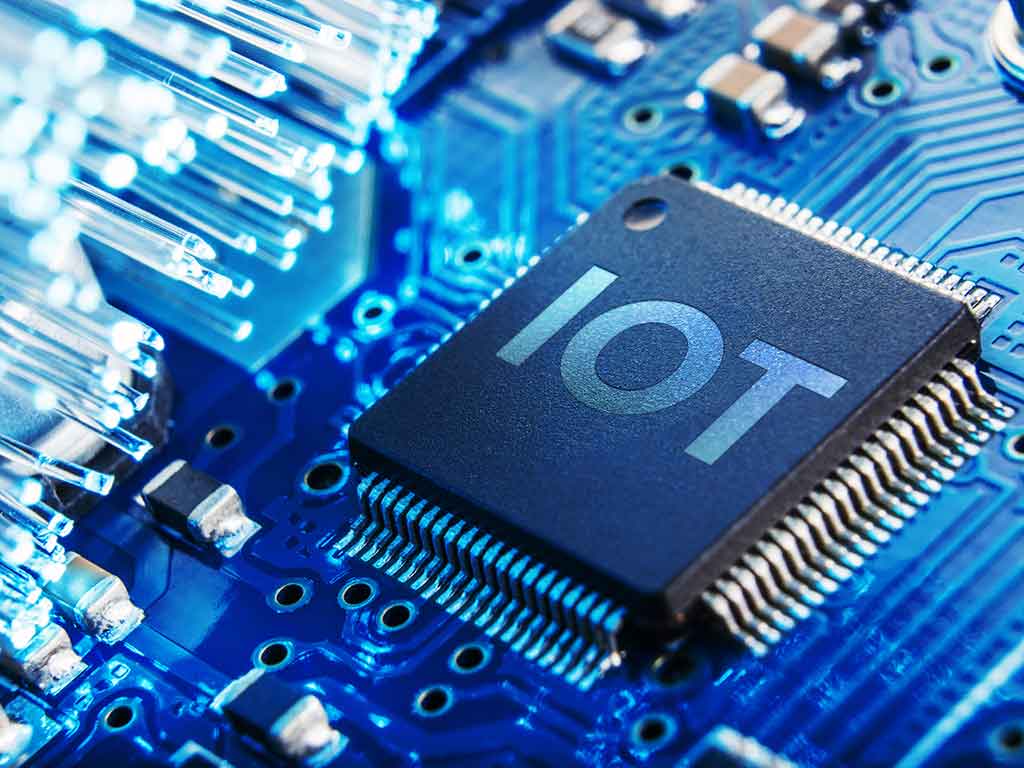
En el año de 2021 más de 10.000 millones de dispositivos de IoT en el mundo se encontraban en existencia. Para el año 2025, se espera que la generación de datos globales supere los 73 zettabytes, lo cual equivale a 73 billones de gigabytes. Aunque, en realidad no se puede cuantificar los datos digitales en términos físicos. Sin embargo, se puede decir que, si todos los datos se convirtieran a discos flexibles de la década de 1990, y se colocaran uno sobre el otro, se habría dado unas 5000 vueltas hacia la luna tanto de ida como de vuelta.

En tan solo unas décadas, los datos de IoT han crecido de manera significativa y es probable que eso se mantenga así. Entonces, para que pudiera surgir este concepto, varias tecnologías tuvieron que entrelazarse con tal de poder avanzar de manera conjunta. Entre estos ejemplos, se tiene en cuenta:

* Conectividad. Con una evolución que va de humildes módems hasta el actual internet y la nube, la conectividad se volvió lo suficientemente rápida y sólida como para enviar y recibir enormes volúmenes de datos y dar soporte al crecimiento exponencial de IoT.
* Tecnología de sensores. Bajo la constante demanda de innovación para los sensores de IoT, el mercado ha pasado de ser un grupo de pocos y costosos proveedores de nicho a ser una industria de fabricación de sensores altamente globalizada y competitiva en precios. Desde 2004, el promedio de precios de sensores de IoT cayó más de un 70%, acompañado por un aumento impulsado por la demanda de una mejor funcionalidad y diversidad en estos productos.
* Poder de computación. Para usar y aprovechar todo el potencial, las empresas modernas exigen cantidades siempre crecientes de memoria y potencia de procesamiento. La carrera para lograrlo ha sido rápida y competitiva, y ha impulsado la creciente relevancia y aplicabilidad de IoT.
* Tecnología de Big Data: desde la década de 1980, los datos del mundo, así como la tecnología computacional necesaria para almacenarlos, han crecido exponencialmente. Los avances en bases de datos y herramientas de análisis han permitido procesar y analizar en tiempo real volúmenes masivos de datos generados a partir de dispositivos de IoT, vehículos inteligentes, y equipamiento. Esta velocidad y capacidad son esenciales para internet de las cosas.
* IA y machine learning: estas tecnologías brindan la capacidad no solo de gestionar y procesar grandes cantidades de datos de IoT, sino de analizarlos y aprender de ellos. Big Data es el alimento favorito de la inteligencia artificial y el machine learning. Cuanto más grandes y diversos sean los data sets, más sólida y precisa será la información estratégica e inteligencia que pueden brindar las analíticas avanzadas potenciadas por IA. El auge de los dispositivos de IoT ha crecido mucho, junto con el avance de la inteligencia artificial y su apetito por los datos que ellos brindan.
* Computación en la nube: así como la conectividad fue esencial en el desarrollo de internet de las cosas, el auge de la computación en nube también ha estado estrechamente ligado a su evolución. Con la capacidad de entregar on-demand un procesamiento poderoso y un almacenamiento de alto volumen, los servicios de IoTen la nube allanaron el camino para que los dispositivos de IoT recopilen y transmitan data sets cada vez más grandes y complejos.

**Parte dos, división dos.**

**¿Cómo funciona IoT?**



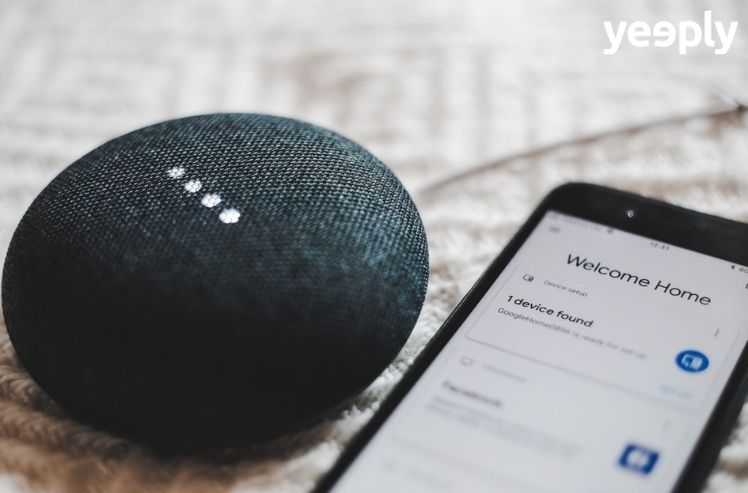
Los dispositivos de IoT son nuestros ojos y oídos cuando no podemos estar allí físicamente –capturan cualquier dato para el cual estén programados–. Estos datos se pueden recopilar y analizar para ayudarnos a fundamentar y automatizar las acciones o decisiones posteriores. Hay cuatro etapas clave en este proceso:

Cuatro etapas clave de internet de las cosas

1. **Capturar los datos.** A través de sensores, los dispositivos de IoT capturan datos desde sus entornos. Esto podría ser algo tan simple como la temperatura o tan complejo como un feed de video en tiempo real.
2. **Compartir los datos.** Mediante conexiones de red disponibles, los dispositivos IoT envían estos datos a un sistema en la nube pública o privada (dispositivo-sistema-dispositivo), a otro dispositivo (dispositivo-dispositivo), o los almacenan localmente como se indica para el procesamiento edge.
3. **Procesar los datos.** En este punto, el software se programa para que haga algo en base a esos datos –como encender un ventilador o enviar una advertencia–.
4. **Actuar a partir de los datos.** Se analizan los datos acumulados desde todos los dispositivos de una red de IoT. Esto brinda información estratégica poderosa para fundamentar acciones y decisiones de negocio confiables.

**Parte tres, división tres.**

**Ejemplos de IoT en acción.**



Las redes de IoT y los datos que producen están operando en prácticamente todos los aspectos de la vida moderna en nuestras casas, autos, tiendas, e incluso en nuestros cuerpos.

* Hogares inteligentes: muchas personas ya están íntimamente familiarizadas con las redes de IoT en sus propias casas. Mediante conmutadores, sensores y dispositivos inteligentes que se comunican a través de protocolos como Z-Wave o Zigbee, los sistemas de automatización del hogar se pueden usar para monitorear y controlar cosas como iluminación, climatización, sistemas de seguridad, electrodomésticos.
* Redes inteligentes: combinadas con IA y tecnología de analíticas avanzadas, las redes inteligentes usan soluciones de IoT para facilitar la integración de tecnología con el fin de ayudar a los consumidores a mejorar el racionamiento y comprender la energía que están usando.
* Ciudades inteligentes: según el índice de ciudades inteligentes (SCI), se trata de “un entorno urbano que aplica tecnología para potenciar los beneficios y disminuir las deficiencias de la urbanización”.
* Automóviles conectados: hoy, prácticamente todos los autos nuevos salen al mercado con IoT y funcionalidad inteligente, y se espera que la ubicuidad de los autos 5G crezca durante los próximos cinco años y más allá.
* IoT en el comercio minorista: las soluciones de IoT orientadas al cliente se usan cada vez más para mejorar las experiencias en la tienda.
* Telesalud: cada vez es más común ver dispositivos médicos de consumo impulsados por IoT, tales como relojes inteligentes y dispensadores de medicación que ayudan a los profesionales a monitorear a los pacientes de forma remota.
* Gestión del tránsito: a través de una red de sensores, cámaras y otros dispositivos, la tecnología de IoT se puede usar para reducir la congestión del tránsito y ayudar a brindar opciones viables de nuevas rutas.

**Parte cuatro, división cuatro.**



**El futuro de IoT.**

En un futuro no tan lejano, se puede esperar una integración muchos más fluida entre la tecnología y la experiencia humana. Si bien el metaverso aún pude tardar algunos años, o inclusive ser reemplazado por otra cosa similar, el audio 3D, la realidad virtual avanzada, las sensaciones hápticas y la personalización en tiempo real potenciada por IA significarán que nuestra interacción con los dispositivos que nos rodean permitirá experiencias sensoriales cada vez más reales. Además, con el auge del 5G y la conectividad rápida, tendremos una capacidad cuántica para compartir nuestras experiencias hacia cualquier distancia.