VPN Protocols

Transcribed on July 30, 2025 at 9:57 AM by Minutes AI

Speaker 1 (00:04)

Bienvenidos a esta nueva sesión.

En esta sesión vamos a tratar el tema de las Redes Privadas Virtuales o VPN un poco más en profundidad, dada su gran importancia dentro de la seguridad de una arquitectura de red de datos.

También veremos una introducción a la solución de implementaciones VPN llamada WireGuard, con la cual haremos algún ejercicio más adelante.

Una VPN tiene como objetivo actuar como si fuera una red privada pero sobre una red pública y actualmente es Internet.

Esto implica que la VPN debe estar perfectamente configurada y optimizada para evitar que nadie de la red pública pueda acceder a la información que estamos transmitiendo.

Las tecnologías que se utilizan para crear una VPN y asegurar la información de los cortafuegos, de los firewalls, la autenticación, el cifrado y y el tunnelink son algunos de los elementos que conforman esta arquitectura.

La gestión de la calidad del servicio también se convierte en una tarea crítica asociada a la disponibilidad del servicio.

Recordemos que una VPN funciona sobre Internet, por lo tanto es posible que no tengamos control sobre posibles problemas relacionados con el tráfico de información.

Hay una gran variedad de protocolos VPN para utilizar dentro de la infraestructura.

La elección del más adecuado es importante para asegurarnos ofrecer la máxima calidad y la seguridad de conexión para los clientes que acceden a través de la red en este método de conexión.

Antes de continuar quiero puntualizar que en esta sección lo que voy a tratar son protocolos VPN que se usan habitualmente y actualmente hay otros protocolos clásicos como SSL, SSPT o PPTP que ya están en desuso y no se recomienda su utilización excepto en casos muy concretos.

Bien, pues comenzaremos por el primero que es IPSec, que es el Internet Protocol Security.

IPSec tiene básicamente dos modos de operación, en modo transporte y en modo túnel.

En modo transporte el origen y el destino efectúan ambos procesos de cifrado, es decir, cada host tiene que preparar la información cifrando los datos para luego enviarlos a través de un túnel tipo LTP.

El modo túnel es el segundo método, donde el procedimiento que sigue IPSec es crear una nueva encapsulación para que el paquete original sea cifrado y lo añada a una nueva cabecera IP, enviándolo finalmente al destinatario.

Este modo es más utilizado para conexiones tipo VPN to VPN.

Este protocolo de IPSec viene por defecto aplicado en la configuración de IPV como ya hemos visto en capítulos anteriores.

Algunas de las ventajas de utilizar IPSec es que es el protocolo más utilizado, por lo tanto tenemos una amplia documentación disponible.

También sabemos que soporta varios métodos de autenticación, además el cifrado por paquetes en vez de por bloques.

Además de la seguridad añade más granularidad al poder gestionarlos individualmente.

También es perfecta para configurar un acceso completo a una intranet, aunque esto puede suponer también algún tipo de problema de seguridad.

Al ser un tipo de conexión basada en el cliente, es posible gestionar y controlar qué tipo de dispositivos están accediendo a la red y si cumplen con los requisitos de seguridad.

Finalmente no depende de la aplicación utilizada ya que este funciona en la capa de red.

Ahora iré un poco más por encima, pero quería profundizar más en IPSec porque es uno de los más utilizados.

Bien, pues el siguiente es LTP ipsec LTP es un protocolo muy antiguo, pero ha superado bien el paso del tiempo en lo que a seguridad se refiere, entre otras muchas cosas porque utiliza el cifrado AES de 256 bits.

Por eso hoy día se utiliza junto a IPSec para crear túneles VPN, aunque cada vez más se está dejando de utilizar.

La gran ventaja de esta unión es la compatibilidad, ya que añadimos ipsec a multitud de servicios que llevan tiempo utilizando LTP.

Y bueno, como parte negativa en lo referente a la operatividad, LTP utiliza un número muy pequeño de puertos de red, por lo que es fácilmente detectable y podría ser fácilmente bloqueado por un ISP.

Otro es el IKEV IPSec.

Esta es otra VPN que utiliza la unión de dos el IKEV y el IPSec.

Ike al ser un protocolo más o menos nuevo aún no está muy extendido, por lo que tenemos que estar seguros que los dispositivos que utilicemos sean compatibles con él.

Tiene algunas ventajas como por ejemplo un cifrado más fuerte, también tiene auto reconexión o quizás también una mayor velocidad y bueno, también se recomienda mucho para dispositivos móviles.

OpenVPN es muy conocido y quizás el más nuevo dentro del mundo de las VPN y está muy extendido y funciona sobre UDP y TCP, lo que hace que sea muy difícil de detectar y de bloquear.

Es muy seguro ya que utiliza OpenSSL y TLS y además de ser bastante rápido, esto le da una capa mayor de seguridad.

Por otro lado no tiene soporte nativo en ningún sistema operativo, por lo que significa que tenemos que utilizar una herramienta externa para poder utilizarlo, con los problemas de seguridad que esto puede acarrear.

Por este motivo este protocolo es el más flexible y seguro que podemos utilizar a día de hoy.

Y por último Wildcard, este sí que es nuevo, este de los últimos y además ha demostrado ser de los más rápidos, estables e incluso tan seguro o más como OpenVPN o IKEV, aunque contrapartida aún es demasiado nuevo, aunque ya está bastante establecido y sus implementaciones no son 100% seguras al contener algún tipo de bugs o de problemas de seguridad en la misma implementación.

De hecho haremos un pequeño ejercicio de cómo configurarlo en Linux más adelante.

El concepto de Site to Site VPN merece una pequeña mención porque este tipo de configuración o este concepto permite a múltiples oficinas dentro de la misma empresa establecer conexiones seguras entre ellas a través de Internet.

La diferencia con una VPN de acceso es que estas configuraciones se realizan directamente en los dispositivos de red para crear la conexión que sea continu, continua o fija entre las diferentes ubicaciones u oficinas.

Por este motivo los usuarios de las oficinas pueden acceder a todos los recursos de forma transparente y sin tener que utilizar ningún cliente de VPN.

Tenemos dos tipos de VPN side to la intranet, que se basa en crear una intranet VPN a la cual se conectará el resto de LANs o de redes sociales dentro de una única one.

Este es el método lógico para conectar oficinas en la misma empresa.

Y después tenemos la Extranet, que se utiliza para crear VPN externas compartidas con otras empresas creando una red compartida.

Pues bien, Site to Site VPN tiene muchas ventajas, por ejemplo, y quizás esta es la principal, es que son más seguras.

Un túnel de este tipo de configuración podemos centralizar y gestionar todas las opciones de conexión para todos los clientes.

Por ejemplo se podría aplicar por defecto a todo el mundo, certificados, etc.

Después, otro punto que tiene muy ventajoso es que son muy escalables, algo totalmente esencial para una empresa a la hora de abrir oficinas nuevas y conectarlas a su red principal.

En cambio, como parte negativa pero necesaria para implementar una red VPN de este tipo, esto implica más recursos iniciales, sobre todo inversión en dispositivos, pero sobre todo un diseño que esté muy muy claro.

Aquí podéis ver en esta diapositiva una implementación gráfica de estos dos tipos de la Extranet VPN y de la Intranet VPN.

Bien, pues ahora nos centraremos en los tipos de redes VPN.

La primera que podemos ver es la red Peer to peer o PP.

Una red PP lo que nos permite son conexiones directas entre usuarios sin necesidad de coordinación central, lo que facilita el intercambio seguro de datos directamente entre los dispositivos.

Esta red es ideal para establecer enlaces seguros entre usuarios remotos o sucursales sin que haga falta un servidor centralizado, y esto promueve una estructura de red descentralizada y muy eficiente en la distribución de recursos.

La siguiente es la red de acceso remoto.

Una red de acceso remoto permite a los usuarios individuales conectarse a una red privada desde una ubicación remota como si estuvieran directamente conectados a un servidor de la red, y esto proporciona acceso seguro a los recursos de la red a través de Internet.

Se utiliza mucho por trabajadores remotos para acceder de manera segura a recursos corporativos, garantizando la confidencialidad e integridad de la información transmitida.

La tercera que vemos en la diapositiva es el Multi Protocol Label Switching o MPLS.

MPLS es una técnica de enrutamiento que dirige los datos de un nodo a otro basándose en etiquetas de rutas cortas en lugar de direcciones de red largas, lo que aumenta la velocidad de transmisión de datos.

Esta tecnología es empleada por proveedores de servicio para dirigir eficientemente varios tipos de tráfico de red como box y datos a través de una infraestructura de red compartida, y esto mejora muchísimo la gestión del tráfico y la escalabilidad.

Aquí podéis ver una representación gráfica de las tres VPN que hemos visto, la PP, el Remote Access VPN y la MPLS.

Bien, ahora veremos algo un poco más práctico.

Vamos a ver cómo se configura de forma muy genérica wireguard, porque wireguard es un moderno y eficiente protocolo de VPN que es muy simple, tiene mucha velocidad y tiene unas características de seguridad muy muy buenas para aplicar en nuestro entorno.

Bien, pues ahora vamos a ver de forma genérica y a nivel de configuración de ficheros, etcétera, la aplicación WireGuard.

La configuración de WireGuard se basa en la noción de pares o peers, donde cada extremo de la conexión VPN puede actuar tanto como cliente o como servidor, y esto facilita que es una configuración muy flexible que se puede adaptar a una gran variedad de casos de uso, desde conexiones punto a punto hasta redes más complejas que involucran múltiples nodos, por ejemplo.

Una de las características más destacadas de WireGuard es su simplicidad, tanto en la configuración como como en la gestión.

Se configura a través de archivos de texto plano sencillos que definen las llaves criptográficas, las direcciones IP y las opciones de los pares con los que se comunica.

Esta simplicidad ayuda a reducir el margen de error en la configuración y facilita la automatización y el despliegue a gran escala.

El paso principal será comprobar si tenemos instalados WireGuard en el sistema.

Para ello escribimos wg, vemos que no está, con lo cual procedemos a la instalación, como siempre con un apt update primero, siempre con el sudo delante.

Ahora lo que haremos será un sudo apt install y haremos wicar, decimos que sí y cuando acabe tendremos ya la aplicación instalada.

Bien, pues el primer paso a realizar es crear una llaves criptográficas.

Cada interfaz de conexión de Wygir o cada interfaz de red utiliza un par de llaves, una pública y una privada para la autenticación y el cifrado.

Para generar un par de claves tenemos que utilizar el comando wg y con la extensión henkey haremos wg genkey por ejemplo, este es un ejemplo, ponemos t y ahora private key hacemos otro pipe y ahora conectamos con wg pubkey y ya con esto acabamos direccionándolo a publickey.

Con este comando lo que hacemos es generar las dos claves, la pública y la privada.

Una vez ya tenemos las claves lo que tenemos que hacer es configurar la interfaz de wildcat.

Para ello tenemos que crear un archivo de configuración.

Por convención estos archivos se guardan en etc, esta sería un poco la ruta y tienen siempre la extensión conf.

Por ejemplo si tenemos una interfaz que se llama wg pues se llamará, que es justo lo que voy a hacer ahora.

Vamos a crear una con nano por ejemplo, etc wireguard y le vamos a llamar conf.

Aquí habría que añadir la configuración, que ya dependerá de cómo queramos conectarlo, de nuestra direcciones IP y todo eso.

Entonces lo primero que haremos será un apartado que llamaremos interface y aquí dentro podemos poner por ejemplo la dirección 10001 por ejemplo esta 3 es la dirección ip de la interfaz de wireguard en el servidor.

Después pondremos save config por ejemplo y le daremos el valor true saveconfig true es un comando bastante útil que sirve para preservar los cambios dinámicos así como la adición o el añadir pares o la modificación de parámetros durante el tiempo de ejecución.

El siguiente parámetro sería la clave privada private key Bien después list que es el puerto de escucha, aquí es el puerto en el que wireguard va a escuchar todas las conexiones entrantes, por defecto es el 51820.

Iremos a otra sección que llamaremos peer que es para configurar el nodo o el par o los pares igual ponemos public key con las que mayúsculas para que publicar nuestra clave pública y después haremos esto a la web y pondremos 10.0.0.232 bien lo que hacemos en.

Bueno la public key ya sabemos en la clave pública con allowed ip lo que estamos es definiendo las direcciones IP que serán enrutadas a través de esta conexión VPN específica, en este caso sería 10.002.32 esto indica que sólo el tráfico destinado a La dirección IP 10002 será enviado a través de este par o de este PIR.

El Basla 32 indica una máscara de subred que apunta a una única dirección IP.

Esta configuración se utiliza en la típica política de enrutamiento y determina qué tráfico se envía a través del túnel VPN.

Si por ejemplo quisiéramos enviar todo el tráfico de Internet a través de este par se podría configurar esta opción como Bien pues una vez tenemos ya definida la interfaz con sus parámetros lo que tenemos que hacer es habilitarla y para eso haremos un sudo wg quick app y el nombre de la interfaz para comprobar que está funcionando bien utilizaremos wgsow y esto nos mostrará el estado de wildcard.

Bien pues quiero añadir que es importante tener el puerto 51820 abierto entonces aunque después veremos más adelante cómo configurar diferentes firewall como pueden ser ufw o iptables.

Bien pues para hacerlo lo más sencillo posible he optado por ufw que es un cortafuego bastante fácil de configurar que veremos más adelante cuando hablemos de los cortafuegos y para habilitar el puerto 51820 haremos un sudo ufw allow el puerto 51820 y su protocolo que es UDP.

Con esto ya debería permitir esa regla y que funcionara a través de ese puerto.

Bien, pues aquí si os fijáis no he ejecutado cada una de las opciones porque eso lo vamos a dejar para el ejercicio que viene a continuación en el siguiente vídeo.

Entonces lo que sí os he querido dejar aquí son un poco las configuraciones básicas y lo que tenemos que tocar y adaptar para que wireguard funcione.

Después vamos a proponer un pequeño ejercicio para hacer la configuración y finalmente veréis cómo se resuelve paso a paso el ejercicio propuesto.

Ahora sí que nos enfocaremos en el hardening, en la securización de las VPN.

Además los conceptos que vamos a tratar ahora son aplicables a cualquier tipo de VPN para conseguir asegurar el máximo el tráfico que esté cifrado y securizado en nuestra red.

No tenemos que olvidar que debido al gran número de fabricantes de tecnología relacionada con las redes, es posible encontrar métodos concretos aplicables a estos dispositivos en función del fabricante.

Por ejemplo, uno de los puntos del hardening o de la securización es securizar al máximo la gestión remota, porque además de crear nuestra propia red de gestión, además del famoso equipo Bastión que ya vimos, tenemos que seguir algunas consideraciones adicionales, por ejemplo conectar solo usando SSH y HTTPs, además de desconectar el resto de protocolos de conexión remota que no nos hagan falta, como por ejemplo el famoso telnet.

También tenemos que centrarnos en el acceso a los dispositivos o también llamado AAA, porque debemos de implementar una correcta autenticación y autorización a los mismos, evitando por ejemplo contraseñas por defecto o algunas que sean demasiado débiles.

Para ello lo ideal es siempre integrar el acceso con los directorios de usuarios de la empresa si es posible y en caso contrario restringir el acceso al máximo y aplicando las políticas de seguridad que hay las contraseñas de nuestra organización.

Algunos de los protocolos que están orientados Algunos de los protocolos que están orientados al AAA tenemos la autenticación, el acceso y la autorización.

Algunos de estos son RADIUS, TACACS, EDWARD PPP, etc.

También tenemos que restringir servicios y protocolos, esto ya lo he repetido varias veces durante todo este curso o este apartado o este módulo de hardening de redes de datos.

Cualquier protocolo o servicio que no utilicemos tiene que ser deshabilitado.

Después también tenemos que aplicar reglas a las interfaces de red.

Los dispositivos de gestión de la VPN sólo tienen que usar protocolos VPN.

Por este motivo, a nivel de hardware o interfaz tenemos que restringir cualquier otro que no sea necesario.

También tenemos que securizar al máximo el protocolo VPN que hemos elegido.

Por ejemplo, Si hemos elegido IPSec, entonces tenemos que conocer a fondo las características de seguridad que nos ofrece este protocolo para que de esta forma podamos sacar el máximo partido a sus funciones de seguridad y eliminar aquellas que no nos hagan falta.

También tenemos que seleccionar muy bien los protocolos de cifrado.

En función de cada característica de la VPN tenemos que aplicar uno u otro cifrado de información.

Y ya para acabar quiero hacer un pequeño inciso, aunque parece obvio, pero hay que evitar utilizar elementos de red que no están orientados a empresas, sobre todo en configuraciones críticas como las VPN.

Ocurre lo mismo con el software.

Siempre tenemos que adquirir equipamiento orientado a la empresa, ya que éste va a cumplir ciertos requisitos, además de ofrecer garantía y soporte adicional.

Y esto último de la garantía y el soporte es fundamental para empresas.

Como conclusión, tenemos que saber que el hardening de las redes de datos a través de medidas como el uso de la VPN es crítico para proteger la confidencialidad, la integridad y la disponibilidad de la información.

La elección de una arquitectura VPN adecuada implica considerar factores como la escalabilidad, la compatibilidad con los tipos de dispositivos y la gestión eficiente de contraseñas y claves.

Al implementar una VPN se establece un túnel cifrado que protege la comunicación entre dispositivos, lo que refuerza la seguridad contra posibles ataques externos y garantiza la privacidad de los datos transmitidos a través de redes públicas como Internet.

Llegamos al final de la sesión.

Os esperamos en el siguiente vídeo.