AIEP
DE LA UNIVERSIDAD ANDRES BELLO

SEGURIDAD EN NETWORKING

Unidad

Seguridad para las redes

ESCUELA DE INGENIERÍA Y CONSTRUCCIÓN

Director: Marcelo Lucero Yáñez

ELABORACIÓN

Experto disciplinar: Luis Jaque Zúñiga

Diseñadora instruccional: Luisa García Ospina

Editora instruccional: Emilia De la Cruz Barrés

VALIDACIÓN

Experto disciplinar: Rodrigo Orellana Núñez

Jefa de Diseño Instruccional: Alejandra San Juan Reyes

EQUIPO DE DESARROLLO

Welearn

AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Implementan soluciones mediante redes privadas virtuales, considerando normativa vigente.

Fuente: Freepik (s.f)

Introducción

Durante esta primera semana abordaremos conceptos relacionados con la implementación de soluciones de seguridad, a través de redes privadas virtuales (VPN), tomando en consideración la normativa legal vigente.

Así podrán:

- **¿Cómo identificar terminologías de arquitecturas de red VPN, según estándares de seguridad de Cisco System?**
- **¿Cómo caracterizar seguridad de soluciones VPN gratuitas y estandarizadas, según normativa vigente?**
- **¿Cómo implementar seguridad de soluciones VPN IPSEC en topología de red, considerando software de simulación?**
- **¿Cómo implementar soluciones VPN Site-to-Site en topología de red, considerando software de simulación?**

1. Tecnología Redes privadas virtuales (VPN)[1]

Para proteger el tráfico de red entre sitios y usuarios, las organizaciones usan redes privadas virtuales (VPN) para crear conexiones de red privada de extremo a extremo. Una VPN es virtual porque transporta la información dentro de una red privada, pero, en realidad, esa información se transporta usando una red pública. Una VPN es privada porque el tráfico se encripta para preservar la confidencialidad de los datos mientras se los transporta por la red pública.

La figura, muestra una colección de varios tipos de VPN administrados por el sitio principal de una empresa. El túnel permite a los sitios remotos y a los usuarios acceder a los recursos de red del sitio principal de forma segura.

[1] Cisco Networking Academy. (2022). *Redes empresariales, Seguridad y Automatización.* Capítulo 8: Tecnología VPN.

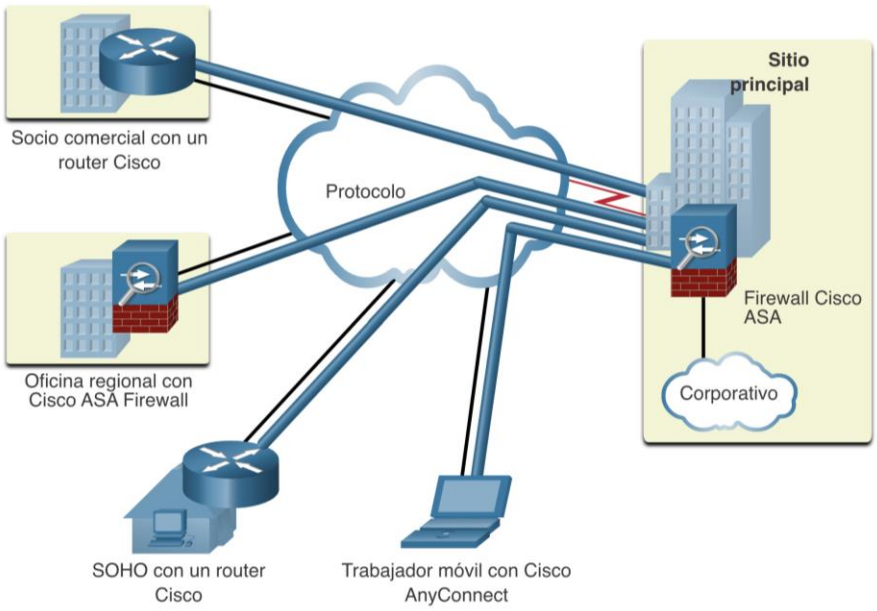


Figura 1: Ejemplo de Topología VPN de sitio a sitio.
Fuente: *Cisco Networking Academy* (2022).

- Un *firewall de Cisco Adaptive Security Appliance* (ASA) ayuda a las organizaciones a proporcionar conectividad segura y de alto rendimiento, incluidas VPN y acceso siempre activo para sucursales remotas y usuarios móviles.

- SOHO significa pequeña/oficina en casa donde un enrutador (*router*) habilitado para VPN puede proporcionar conectividad VPN de vuelta al sitio principal de la empresa.

- Cisco *AnyConnect* es un *software* que los trabajadores remotos pueden usar para establecer una conexión VPN basada en el cliente con el sitio principal.

Los primeros tipos de VPN eran estrictamente túneles IP que no incluían autenticación o encriptación de los datos. Por ejemplo, *Generic Routing Encapsulation* (GRE) es un protocolo de túnel desarrollado por Cisco y que no incluye servicios de encriptación. Se utiliza para encapsular el tráfico IPv4 e IPv6 dentro de un túnel IP para crear un enlace virtual punto a punto.

1.1. Beneficios del VPN

Las VPN modernas ahora admiten funciones de encriptación, como el Internet *Protocol Security* (IPsec) y las VPN de *Secure Socket Layer* (SSL) para proteger el tráfico de red entre sitios.

Los principales beneficios de las VPN se muestran en la tabla.

Ventaja	Descripción
Ahorro de costos	Con la llegada de tecnologías rentables y de gran ancho de banda, las organizaciones pueden usar VPN para reducir sus costos de conectividad mientras incrementa simultáneamente el ancho de banda de la conexión remota.
Seguridad	Las VPN proporcionan el mayor nivel de seguridad disponible, mediante el uso de encriptación avanzada y protocolos de autenticación que protegen los datos de acceso no autorizado.
Escalabilidad	Las VPN permiten a las organizaciones usar Internet, lo que facilita la adición de nuevos usuarios sin agregar infraestructura significativa.
Compatibilidad	Las VPN se pueden implementar en una amplia variedad de opciones de enlace WAN incluidas todas las tecnologías populares de banda ancha. Los trabajadores remotos pueden aprovechar estas conexiones de alta velocidad para obtener acceso seguro a sus redes corporativas.

Tabla 1: Ventajas de las VPN.

Fuente: *Cisco Networking Academy* (2022).

1.2. VPN de sitio a sitio y acceso remoto

Las VPN se implementan comúnmente en una de las siguientes configuraciones: **sitio a sitio o acceso remoto.**

- **VPN de sitio a sitio**: Se crea una VPN de sitio a sitio cuando los dispositivos de terminación de VPN, también llamados puertas de enlace VPN, están preconfigurados con información para establecer un túnel seguro. El tráfico VPN solo se cifra entre estos dispositivos. Los usuarios internos no tienen conocimiento de que se está utilizando una VPN.

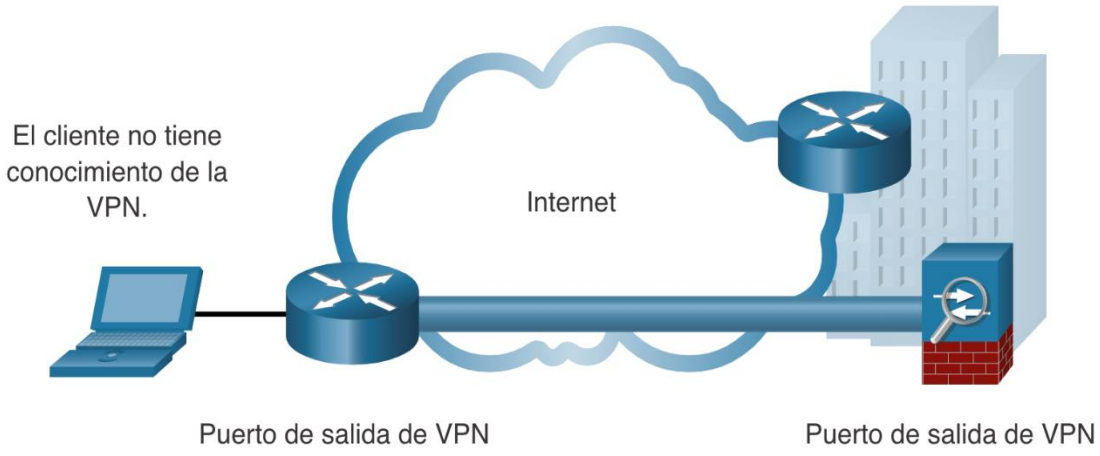


Figura 2: Ejemplo de VPN de Sitio a Sitio.
Fuente: *Cisco Networking Academy* (2022).

- **VPN de acceso remoto**: Una VPN de acceso-remoto se crea dinámicamente para establecer una conexión segura entre un cliente y un dispositivo de terminación de VPN. Por ejemplo, se utiliza una VPN SSL de acceso remoto cuando verifica su información bancaria en línea.

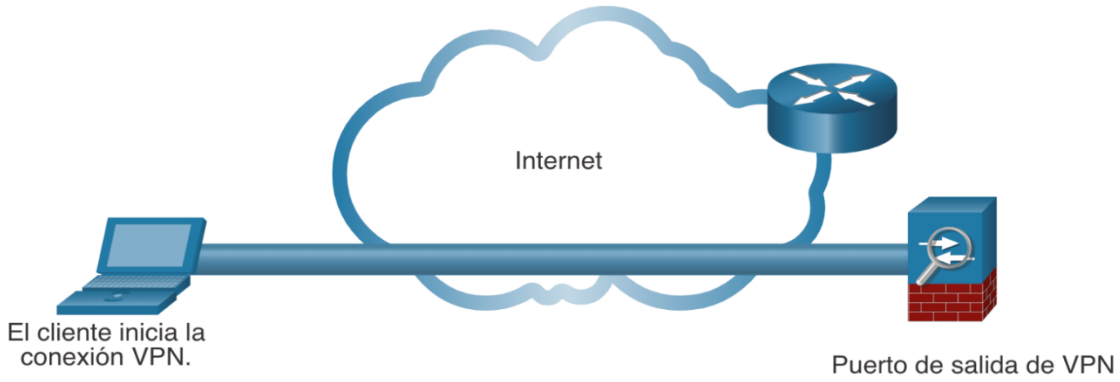


Figura 3: Ejemplo de VPN de acceso remoto.

Fuente: *Cisco Networking Academy* (2022).

1.3. VPN de empresas y proveedores de servicios

Hay muchas opciones disponibles para asegurar el tráfico empresarial. Estas soluciones varían según quién administra la VPN.

Las VPN se pueden administrar e implementar como:

- **VPNs Empresariales:** Las VPN administradas por empresas son una solución común para proteger el tráfico empresarial a través de Internet. Las VPN de sitio a sitio y de acceso remoto son creadas y administradas por la empresa utilizando tanto VPN IPsec como SSL.

- **VPNs de Proveedor de Servicios:** Las VPN administradas por el proveedor de servicios se crean y administran a través de la red del proveedor. El proveedor utiliza *Multiprotocol Label Switching* (MPLS) en la capa 2 o la capa 3 para crear canales seguros entre los sitios de una empresa. MPLS es una tecnología de enrutamiento que el proveedor utiliza para crear rutas virtuales entre sitios. Esto efectivamente segrega el tráfico del

tráfico de otros clientes. Otras soluciones heredadas incluyen *Frame Relay* y VPN de *Asynchronous Transfer Mode* (ATM).

La figura, enumera los diferentes tipos de implementaciones de VPN administradas por la empresa y por el proveedor de servicios.

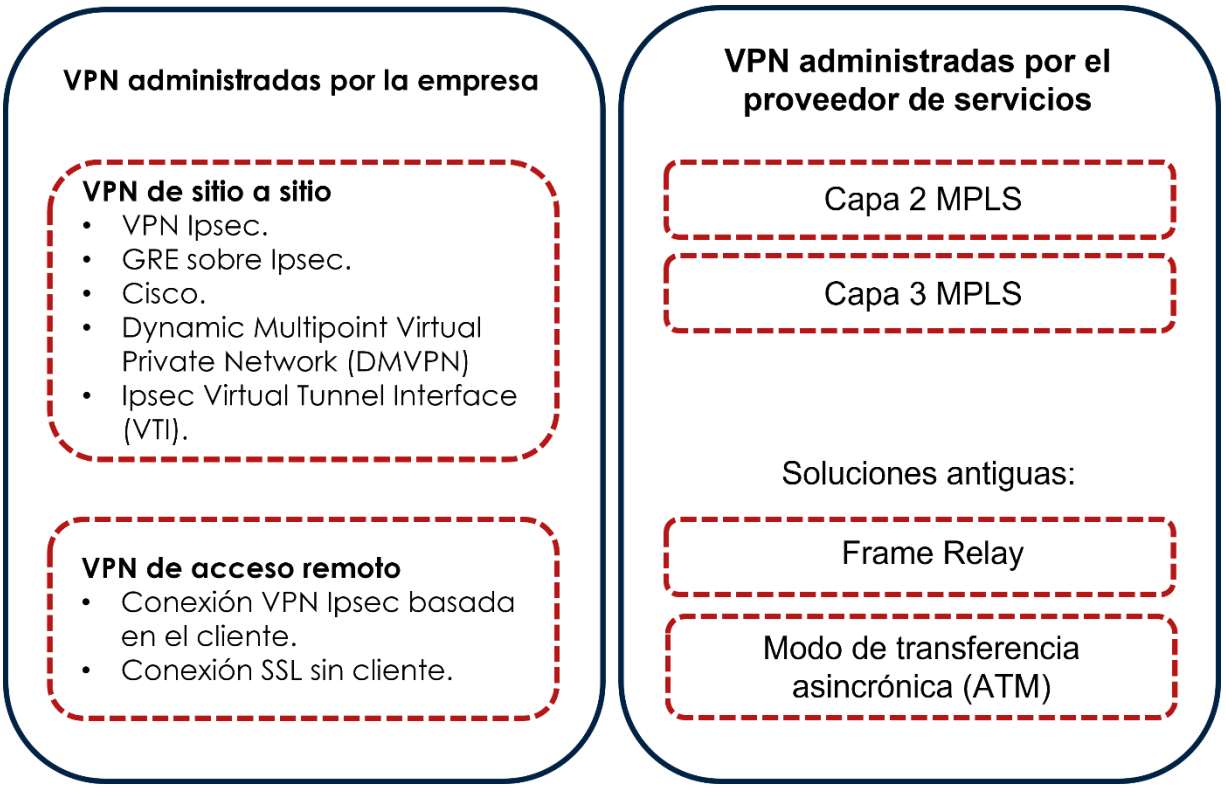


Figura 4: Tipos de implementaciones de VPN.

Fuente: *Cisco Networking Academy* (2022).

2. Tipos de VPN

2.1. VPN de acceso remoto

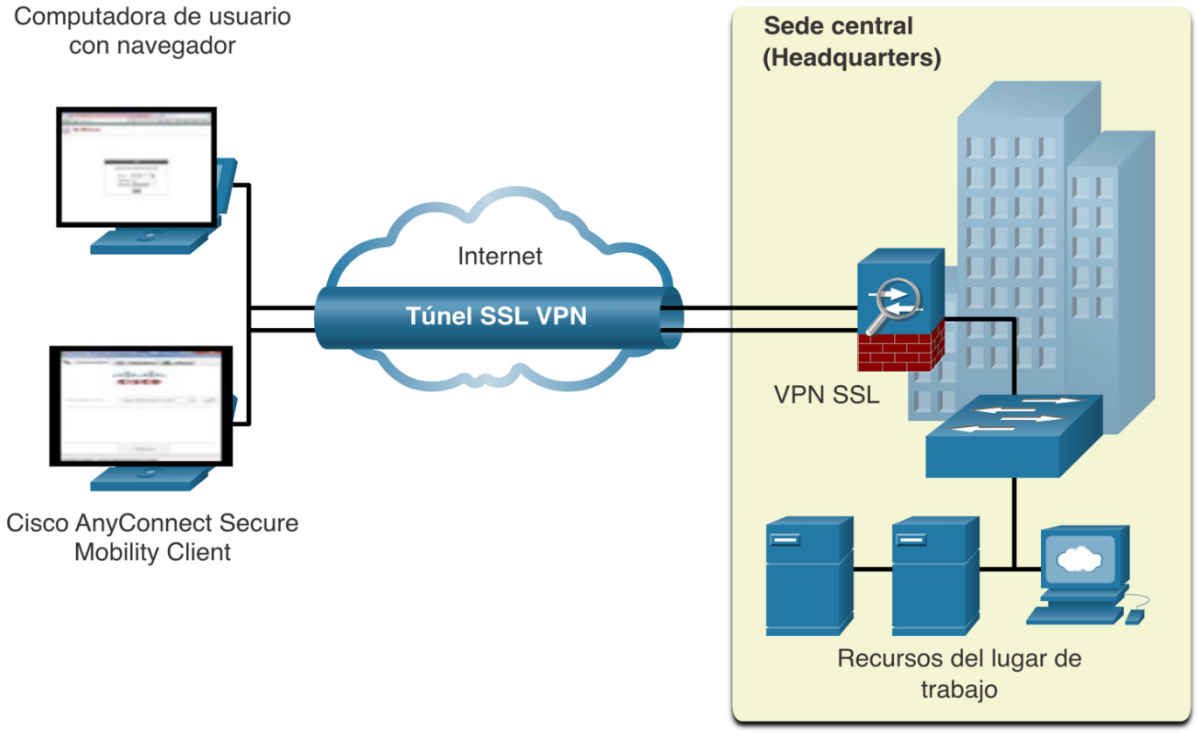
En el tema anterior se aprendieron los conceptos básicos de una VPN. Aquí aprenderá sobre los tipos de VPN.

Las VPN se han convertido en la solución lógica para la conectividad de acceso remoto por muchas razones. Como se muestra en la figura, las VPN de acceso remoto permiten a los usuarios remotos y móviles conectarse de forma segura a la empresa mediante la creación de un túnel encriptado. Los usuarios remotos pueden replicar de forma segura su acceso de seguridad empresarial, incluidas las aplicaciones de correo electrónico y de red. Las VPN de acceso remoto también permiten a los contratistas y socios tener acceso limitado a servidores, páginas web o archivos específicos según sea necesario. Esto significa que estos usuarios pueden contribuir a la productividad empresarial sin comprometer la seguridad de la red.

Las VPN de acceso remoto generalmente se habilitan dinámicamente por el usuario cuando es necesario. Las VPN de acceso remoto se pueden crear utilizando IPsec o SSL. Como se muestra en la figura, un usuario remoto debe iniciar una conexión VPN de acceso remoto.

La figura, muestra dos formas en que un usuario remoto puede iniciar una conexión VPN de acceso remoto: VPN sin cliente y VPN basada en el cliente.

Figura 5: Formas de iniciar una conexión VPN.



Fuente: *Cisco Networking Academy* (2022).

- **Conexión VPN sin cliente:** La conexión se asegura utilizando una conexión SSL de navegador web. SSL se utiliza principalmente para proteger el tráfico HTTP (HTTPS) y los protocolos de correo electrónico como IMAP y POP3. Por ejemplo, HTTPS es en realidad HTTP usando un túnel SSL. Primero se establece la conexión SSL y luego se intercambian los datos HTTP a través de la conexión.

- **Conexión VPN basada en el cliente:** El software de cliente VPN, como Cisco *AnyConnect Secure Mobility Client*, debe instalarse en el dispositivo final del usuario remoto. Los usuarios deben iniciar la conexión VPN utilizando el cliente VPN y luego autenticarse en la puerta de enlace

VPN de destino. Cuando los usuarios remotos se autentican, tienen acceso a archivos y aplicaciones corporativos. El software del cliente VPN encripta el tráfico usando IPsec o SSL y lo reenvía a través de Internet a la puerta de enlace VPN de destino.

2.2. SSL VPNs

Cuando un cliente negocia una conexión VPN SSL con la puerta de enlace VPN, en realidad se conecta utilizando *Transport Layer Security* (TLS). TLS es la versión más nueva de SSL y a veces se expresa como SSL / TLS. Sin embargo, ambos términos a menudo se usan indistintamente.

SSL utiliza la infraestructura de llave pública y los certificados digitales para autenticar a sus pares. Ambas tecnologías IPsec y SSL VPN ofrecen acceso a prácticamente cualquier aplicación o recurso de red. Sin embargo, cuando la seguridad es un problema, IPsec es la mejor opción. Si el soporte y la facilidad de implementación son los problemas principales, considere SSL. El tipo de método VPN implementado se basa en los requisitos de acceso de los usuarios y los procesos de TI de la organización. La tabla compara las implementaciones de acceso remoto IPsec y SSL.

Característica	IPsec	SSL
Aplicaciones soportadas	**Extensiva:** Todas las aplicaciones basadas en IP son compatibles	**Limitada:** Solo aplicaciones y archivos basados en la web compartidos y soportados
Fuerza de autenticación	**Fuerte:** Utiliza autenticación bidireccional con llaves compartidas o certificados digitales	**Moderado:** Uso de autenticación unidireccional o bidireccional
Fuerza de encriptación	**Fuerte:** Utiliza longitudes de llave de 56 bits a 256 bits	**Moderado a fuerte:** Con longitudes de llave de 40 bits a 256 bits
Complejidad de conexión	**Medio:** Porque requiere un cliente VPN preinstalado en un usuario	**Bajo:** Solo requiere un navegador web en una terminal
Opción de conexión	**Limitado:** Solo se pueden conectar dispositivos específicos con configuraciones específicas	**Extensivo:** Cualquier dispositivo con un navegador web puede conectarse

Tabla 2: Características de implementaciones de acceso remoto.

Fuente: *Cisco Networking Academy* (2022).

Es importante comprender que las VPN IPsec y SSL no son mutuamente excluyentes. En cambio, son complementarios; ambas tecnologías resuelven diferentes problemas, y una organización puede implementar IPsec, SSL o ambos, según las necesidades de sus teletrabajadores.

2.3. VPN IPsec de sitio a sitio

Las VPN de sitio a sitio se utilizan para conectar redes a través de otra red no confiable como Internet. En una VPN de sitio a sitio, los usuarios finales envían y reciben tráfico normal de TCP/IP sin encriptar a través de un dispositivo VPN de terminación. La terminación de VPN generalmente se denomina puerta de enlace VPN. Un dispositivo de puerta de enlace VPN podría ser un enrutador o un firewall, como se muestra en la figura. Por ejemplo, el Cisco *Adaptive Security Appliance* (ASA) que se muestra en el lado derecho de la figura, es un dispositivo de firewall independiente que combina firewall, concentrador de VPN y funcionalidad de prevención de intrusiones en una imagen de software.

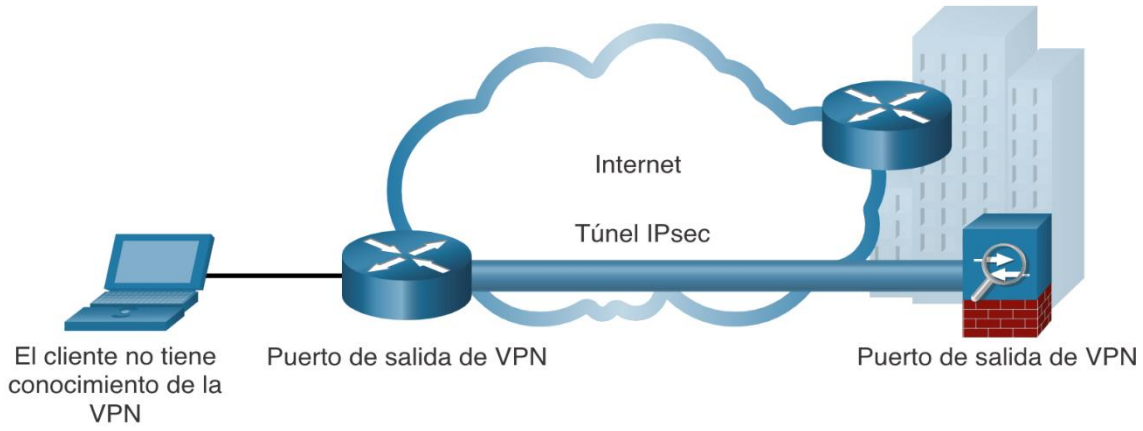


Figura 6: VPN IPsec de sitio a sitio.

Fuente: *Cisco Networking Academy* (2022).

La puerta de enlace VPN encapsula y encripta el tráfico saliente para todo el tráfico de un sitio en particular. Luego envía el tráfico a través de un túnel VPN a través de Internet a una puerta de enlace VPN en el sitio de destino. Al recibirlo, la puerta de enlace VPN receptora despoja los encabezados, desencripta el contenido y retransmite el paquete hacia el usuario de destino dentro de su red privada.

Las VPN de sitio a sitio generalmente se crean y protegen mediante el *IP Security* (IPsec).

2.4. GRE sobre IPsec

Generic Routing Encapsulation (GRE) es un protocolo túnel de VPN de sitio a sitio básico y no seguro. Puede encapsular varios protocolos de capa de red. También es compatible con el tráfico de *multicast y broadcast* que puede ser necesario si la organización requiere protocolos de enrutamiento para operar a través de una VPN. Sin embargo, GRE no admite de forma predeterminada el encriptado; y, por lo tanto, no proporciona un túnel VPN seguro.

Una VPN IPsec estándar (no GRE) solo puede crear túneles seguros para el tráfico de unicast. Por lo tanto, los protocolos de enrutamiento no intercambiarán información de enrutamiento a través de una VPN IPsec.

Para resolver este problema, podemos encapsular el tráfico del protocolo de enrutamiento utilizando un paquete GRE y luego encapsular el paquete GRE en un paquete IPsec para reenviarlo de forma segura a la puerta de enlace VPN de destino.

Los términos utilizados para describir la encapsulación de GRE sobre el túnel IPsec son protocolo pasajero (*passenger protocol)*, protocolo operador (*carrier protocol)* y protocolo transporte (*transport protocol)*, como se muestra en la figura.

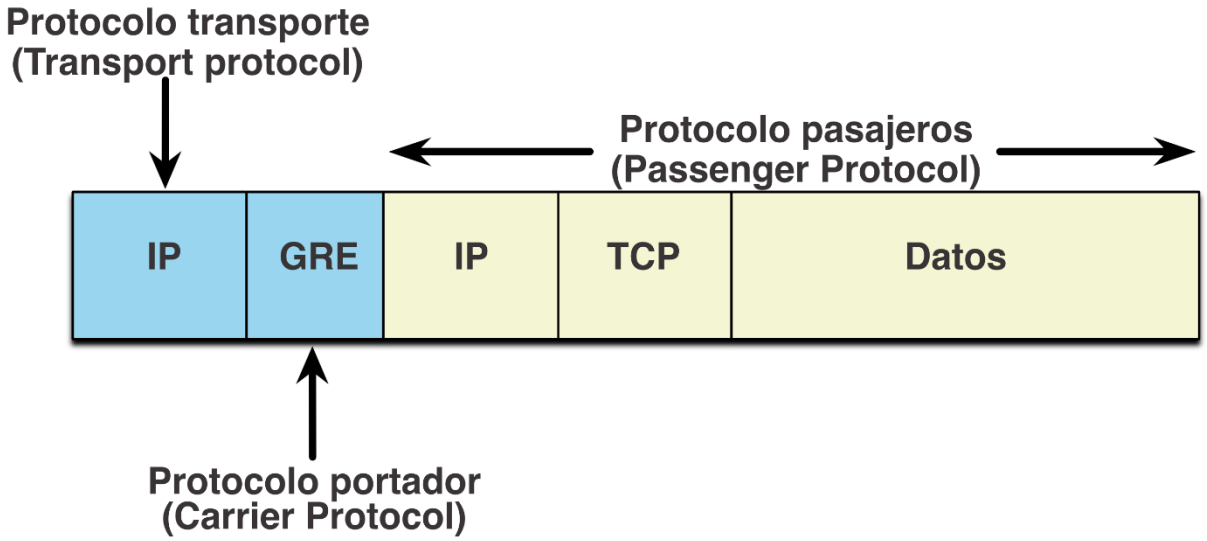


Figura 7: Encapsulación de GRE sobre el túnel IPsec.
Fuente: *Cisco Networking Academy* (2022).

- **Protocolo Pasajero (*Passenger Protocol*):** Este es el paquete original que debe ser encapsulado por GRE. Podría ser un paquete IPv4 o IPv6, una actualización de enrutamiento y más.
- **Protocol Operador (*Carrier protocol*):** GRE es el protocolo operador que encapsula el paquete pasajero original.
- **Protocolo transporte (*Transport protocol*):** Este es el protocolo que realmente se usará para reenviar el paquete. Esto podría ser IPv4 o IPv6.

Por ejemplo, en la figura que muestra una topología, *Branch* y HQ desean intercambiar información de enrutamiento OSPF sobre una VPN IPsec. Sin embargo, IPsec no admite tráfico de tipo multicast. Por lo tanto, GRE sobre IPsec se usa para admitir el tráfico del protocolo enrutamiento (*routing protocol*) sobre la VPN de IPsec. Específicamente, los paquetes OSPF (es decir, el protocolo pasajero) serían encapsulados por GRE (es decir, el protocolo operador) y posteriormente encapsulados en un túnel VPN IPsec.

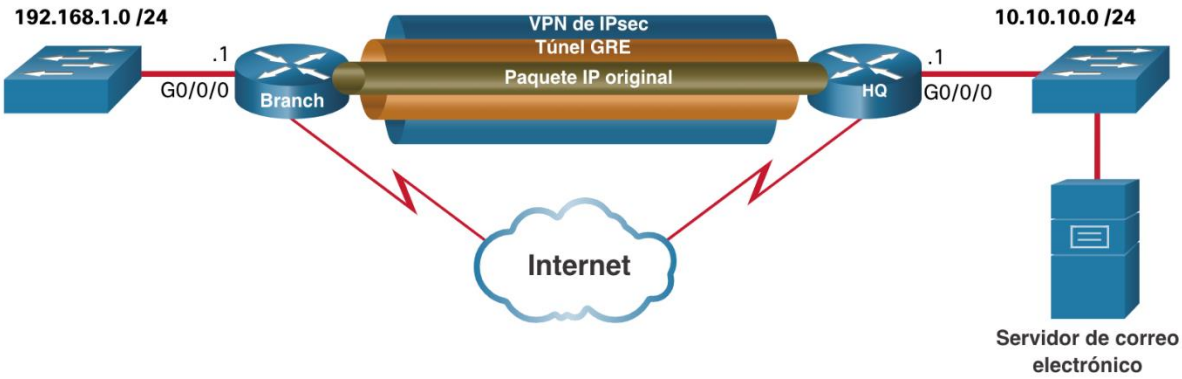


Figura 8: Topología en que se desean intercambiar información de enrutamiento OSPF sobre una VPN IPsec.

Fuente: *Cisco Networking Academy* (2022).

La captura de pantalla de Wireshark en la figura muestra un paquete de saludo "*Hello*" OSPF que se envió utilizando GRE sobre IPsec. En el ejemplo, el paquete original de multicast OSPF *Hello* (el protocolo pasajero) se encapsuló con un encabezado GRE (el protocolo operador), que posteriormente se

encapsula con otro encabezado IP (protocolo transporte). Este encabezado IP se reenviaría a través de un túnel IPsec.

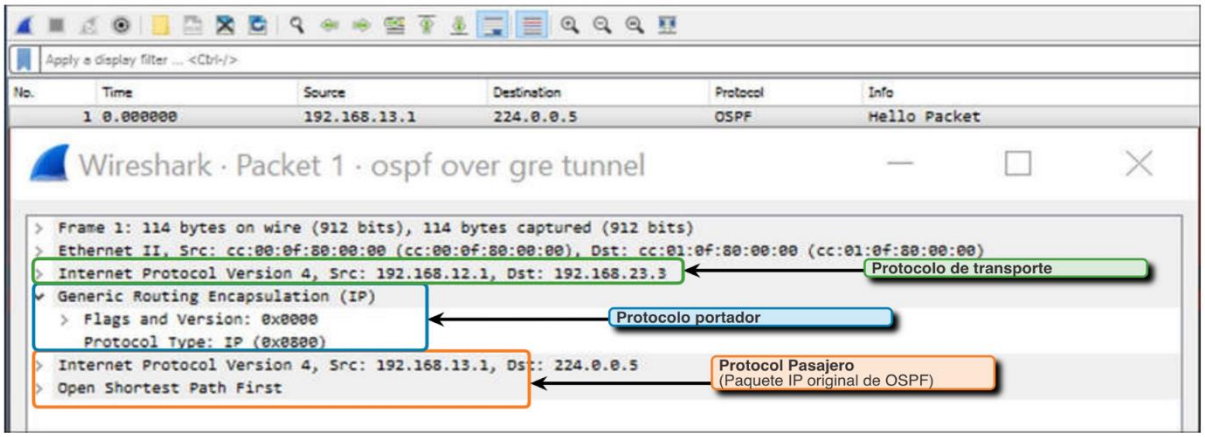


Figura 9: Captura de pantalla de Wireshark de un paquete Hello OSPF.

Fuente: *Cisco Networking Academy* (2022).

2.5. VPN dinámicas multipunto

Las VPN de IPsec de sitio a sitio y GRE sobre IPsec son adecuadas para usar cuando solo hay unos pocos sitios para interconectarse de forma segura. Sin embargo, no son suficientes cuando la empresa agrega muchos más sitios. Esto se debe a que cada sitio requeriría configuraciones estáticas para todos los demás sitios o para un sitio central.

La VPN dinámica multipunto (DMVPN) es una solución de Cisco para crear VPN múltiples de forma fácil, dinámica y escalable. Al igual que otros tipos de VPN, DMVPN depende de IPsec para proporcionar un transporte seguro a través de redes públicas, como Internet.

DMVPN simplifica la configuración del túnel VPN y proporciona una opción flexible para conectar un sitio central con sitios de sucursales. Utiliza una configuración de *hub-and-spoke* para establecer una topología de malla

completa *(full mesh)*. Los sitios de *spoke* establecen túneles VPN seguros con el sitio central, como se muestra en la figura.

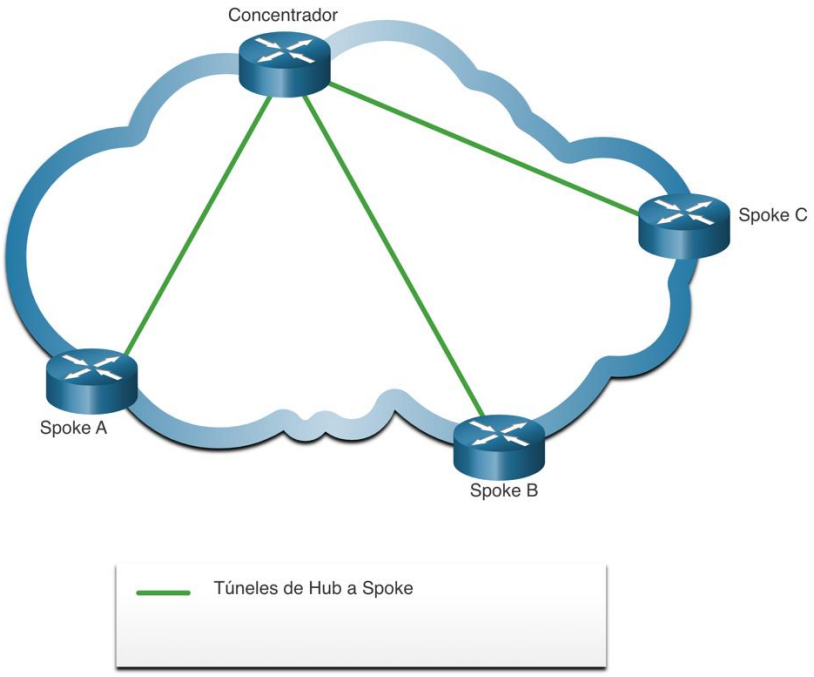


Figura 10: Túneles de Hub a Spoke y entre Spoke de DMVPN.
Fuente: *Cisco Networking Academy* (2022).

Cada sitio se configura usando *Multipoint Generic Routing Encapsulation* (mGRE).La interfaz del túnel mGRE permite que una única interfaz GRE admita dinámicamente múltiples túneles IPsec. Por lo tanto, cuando un nuevo sitio requiere una conexión segura, la misma configuración en el sitio del *hub* admitiría el túnel. No se requerirá configuración adicional.

Los sitios *Spoke* también podrían obtener información sobre sitios remotos desde el sitio central. Pueden usar esta información para establecer túneles VPN directos, como se muestra en la figura.

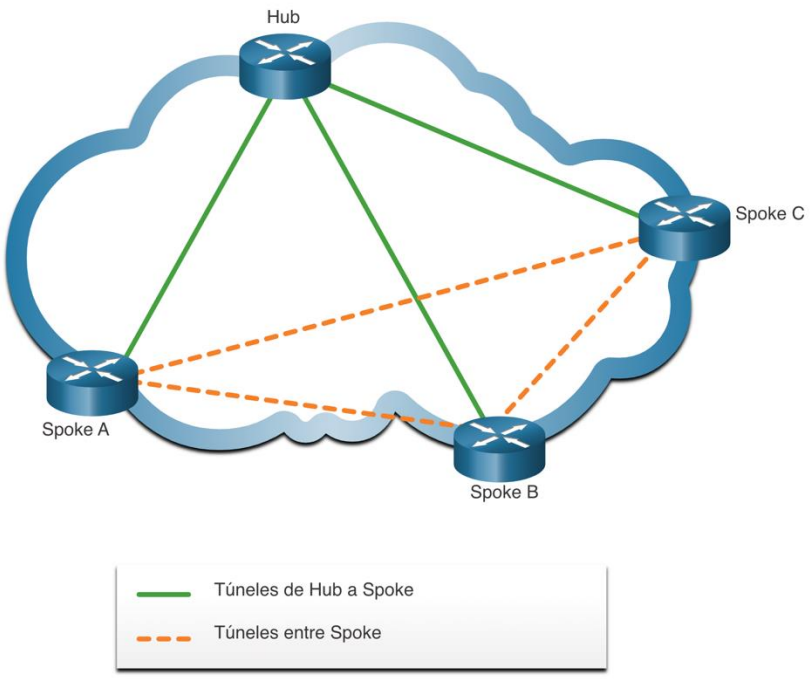


Figura 11: Túneles de Hub a Spoke y entre Spoke de DMVPN.
Fuente: *Cisco Networking Academy* (2022).

2.6. Interfaz virtual del túnel IPsec

Al igual que los DMVPN, IPsec *Virtual Tunnel Interface* (VTI) simplifica el proceso de configuración requerido para admitir múltiples sitios y acceso remoto. Las configuraciones de IPsec VTI se aplican a una interfaz virtual en lugar de la asignación estática de las sesiones de IPsec a una interfaz física.

IPsec VTI es capaz de enviar y recibir tráfico IP encriptado de unicast y multicast. Por lo tanto, los protocolos de enrutamiento son compatibles automáticamente sin tener que configurar túneles GRE.

IPsec VTI se puede configurar entre sitios o en una topología de *hub-and-spoke*.

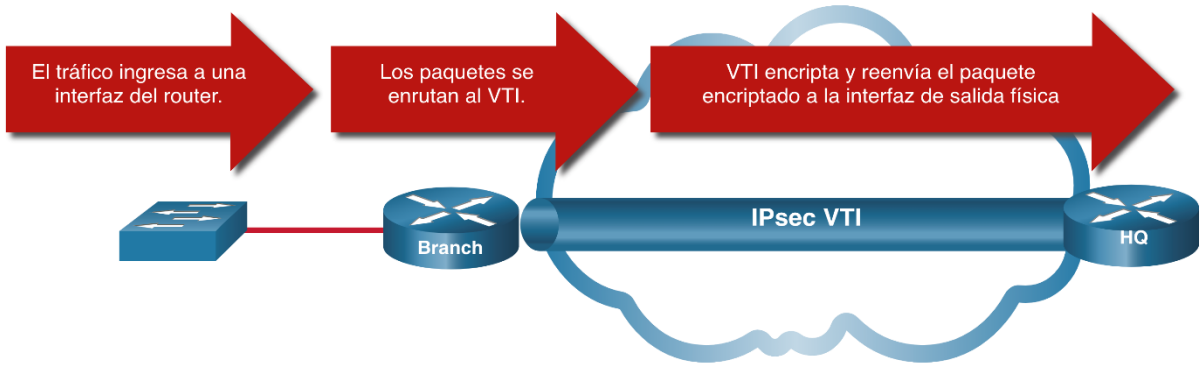


Figura 11: Interfaz virtual del túnel IPsec.

Fuente: *Cisco Networking Academy* (2022).

2.7 Proveedor de servicios VPN MPLS

Las soluciones WAN tradicionales de los proveedores de servicios, como líneas alquiladas, *Frame Relay* y conexiones ATM, eran inherentemente seguras en su diseño. Hoy, los proveedores de servicios usan MPLS en su red principal. El tráfico se reenvía a través de la red principal del MPLS *(backbone)* utilizando etiquetas que se distribuyeron previamente entre los *routers* principales. Al igual que las conexiones WAN heredadas, el tráfico es seguro porque los clientes del proveedor de servicios no pueden ver el tráfico de los demás.

MPLS puede proporcionar a los clientes soluciones VPN administradas; por lo tanto, asegurar el tráfico entre los sitios del cliente es responsabilidad del proveedor del servicio. Hay dos tipos de soluciones VPN MPLS compatibles con los proveedores de servicios:

- **VPN MPLS Capa 3**: El proveedor de servicios participa en el enrutamiento del cliente al establecer un intercambio entre los *routers* del cliente y los *routers* del proveedor. Luego, las rutas de los clientes que recibe el *router* del proveedor se redistribuyen a través de la red MPLS a las ubicaciones remotas del cliente.

- **VPN MPLS Capa 2**: El proveedor de servicios no participa en el enrutamiento del cliente. En cambio, el proveedor implementa un *Virtual Private* LAN *Service* (VPLS) para emular un segmento LAN de acceso múltiple de Ethernet a través de la red MPLS. No hay enrutamiento involucrado. Los *routers* del cliente pertenecen efectivamente a la misma red de acceso múltiple.

La figura, muestra un proveedor de servicios que ofrece VPN MPLS de capa 2 y capa 3.

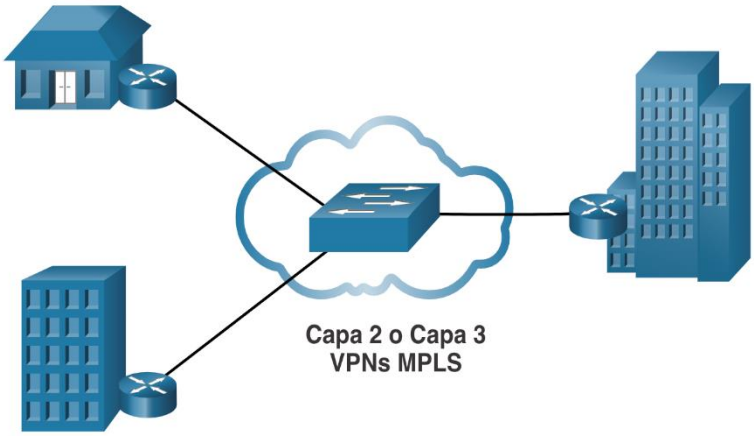


Figura 12: VPN MPLS de capa 2 y capa 3.
Fuente: *Cisco Networking Academy* (2022).

3. Tecnologías IPsec

IPsec es un estándar IETF (RFC 2401-2412) que define cómo se puede asegurar una VPN a través de redes IP. IPsec protege y autentica los paquetes IP entre el origen y el destino. IPsec puede proteger el tráfico de la Capa 4 a la Capa 7.

Usando el marco de IPsec, IPsec proporciona estas funciones de seguridad esenciales:

- **Confidencialidad:** IPsec utiliza algoritmos de encriptación para evitar que los delincuentes cibernéticos lean el contenido del paquete.
- **Integridad**: IPsec utiliza algoritmos de hash para garantizar que los paquetes no se hayan modificado entre el origen y el destino.
- **Autenticación de Origen:** IPsec utiliza el protocolo *Internet Key Exchange* (IKE) para autenticar el origen y el destino. Métodos de autenticación que incluyen el uso de llaves previamente compartidas (contraseñas), certificados digitales o certificados RSA.
- ***Diffie-Hellman*:** Intercambio seguro de llaves, generalmente varios grupos del algoritmo DH.

IPsec no está sujeto a ninguna regla específica para comunicaciones seguras. Esta flexibilidad del marco permite a IPsec integrar fácilmente nuevas tecnologías de seguridad sin actualizar los estándares existentes de IPsec. Las tecnologías actualmente disponibles están alineadas a su función de seguridad específica. Las ranuras abiertas que se muestran en el marco de

IPsec en la figura pueden llenarse con cualquiera de las opciones disponibles para esa función de IPsec para crear una asociación de seguridad (SA) única.

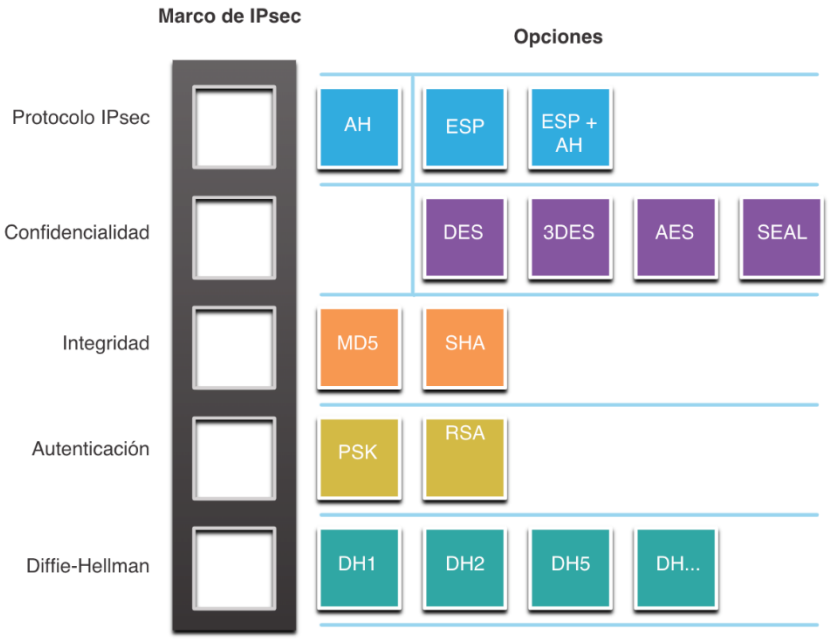


Figura 13: Funciones de seguridad IPsec.

Fuente: *Cisco Networking Academy* (2022).

Las funciones de seguridad se enumeran en la tabla:

Función IPsec	Descripción
Protocolo IPsec	Las opciones para el protocolo IPsec incluyen Encabezado de autenticación (AH) o Encapsulation Security Protocol (ESP). AH autentica el paquete de Capa 3 . ESP encripta el paquete de Capa 3. **Nota**: ESP + AH rara vez se usa ya que esta combinación no atraviesa con éxito un dispositivo NAT.
Confidencialidad	La encriptación garantiza la confidencialidad del paquete de capa 3. Opciones que incluye *Data Encryption Standard (DES), Triple DES (3DES), Advanced Encryption Standard (AES), o Software-Optimized Encryption Algorithm (SEAL)*. Sin encriptación también es una opción.
Integridad	Asegura que los datos lleguen sin cambios al destino utilizando un algoritmo hash, como *message-digest 5 (MD5) o Secure Hash Algorithm (SHA)*.
Autenticación	*IPsec utiliza Internet Key Exchange (IKE)* para autenticar usuarios y dispositivos que pueden llevar a cabo la comunicación de forma independiente. IKE utiliza varios tipos de autenticación, incluidos nombre de usuario y contraseña, contraseña de un solo uso, datos biométricos, llaves pre-compartidas (PSK) y certificados digitales utilizando el algoritmo *Rivest, Shamir y Adleman (RSA)*.
Diffie-Hellman	IPsec utiliza el algoritmo DH para proporcionar un método de intercambio de llave pública para que dos pares establezcan una llave secreta compartida. Hay varios grupos diferentes para elegir, incluidos DH14, 15, 16 y DH 19, 20, 21 y 24. DH1, 2 y 5 ya no se recomiendan.

Tabla 3: Detalle de Funciones de seguridad IPsec.
Fuente: *Cisco Networking Academy* (2022).

La figura muestra ejemplos de SA para dos implementaciones diferentes. Una SA es el bloque básico de construcción de IPsec. Al establecer un enlace VPN, los pares deben compartir la misma SA para negociar los parámetros de intercambio de llaves, establecer una llave compartida, autenticarse mutuamente y negociar los parámetros de encriptación. Tenga en cuenta que en el Ejemplo 1 de SA no se utiliza encriptación.

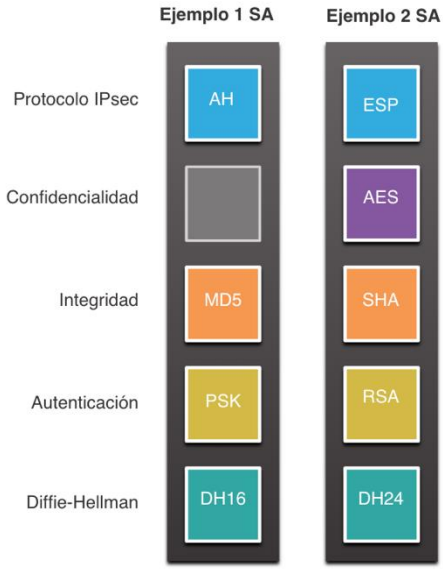


Figura 14: Ejemplos de asociaciones de seguridad IPsec.
Fuente: Cisco Networking Academy (2022).

3.1. Protocolo de Encapsulación Ipsec

La elección del protocolo de encapsulación IPsec es el primer bloque de construcción del marco. IPsec encapsula paquetes usando *Authentication Header* (AH) o el *Encapsulation Security Protocol* (ESP).

La elección de AH o ESP establece qué otros bloques de construcción están disponibles.

- AH es apropiado sólo cuando la confidencialidad no es requerida o permitida. Proporciona autenticación e integridad de datos, pero no proporciona confidencialidad de datos (encriptación). Todo el texto se transporta sin cifrar.

- ESP proporciona confidencialidad y autenticación. Proporciona confidencialidad al realizar la encriptación en el paquete IP. ESP proporciona autenticación para el paquete IP interno y el encabezado ESP. La autenticación proporciona autenticación de origen de datos e integridad de datos. Aunque tanto la encriptación como la autenticación son opcionales en ESP, como mínimo, se debe seleccionar uno de ellos.

3.2. Confidencialidad

La confidencialidad se logra encriptando los datos, como se muestra en la figura. El grado de confidencialidad depende del algoritmo de encriptación y la longitud de la llave utilizada en el algoritmo de encriptación. Si alguien intenta *hackear* la clave a través de un ataque de fuerza bruta, la cantidad de posibilidades para intentar es una función de la longitud de la llave. El tiempo para procesar todas las posibilidades es una función de la potencia de la computadora del dispositivo atacante. Cuanto más corta es la llave, más fácil es romperla. Una llave de 64 bits puede tardar aproximadamente un año en romperse con una computadora relativamente sofisticada. Una llave de 128 bits con la misma máquina puede tardar aproximadamente 1019 o 10 quintillones de años en desencriptarse.

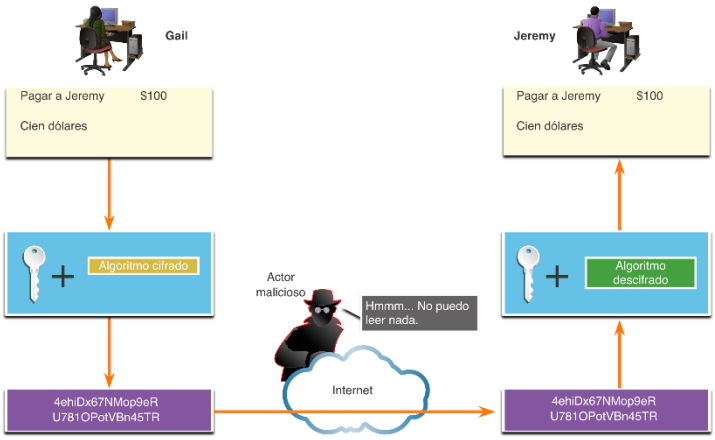


Figura 15: Confidencialidad IPsec.

Fuente: *Cisco Networking Academy* (2022).

Los algoritmos de encriptación resaltados en la figura son todos criptosistemas de llave simétrica.

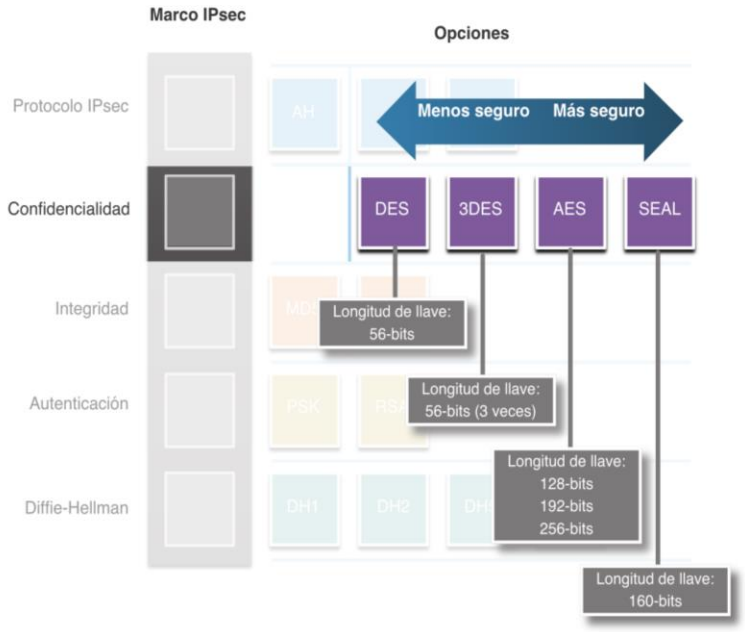


Figura 16: Marco IPsec.
Fuente: *Cisco Networking Academy* (2022).

- DES usa una llave de 56 bits.
- 3DES es una variante del DES de 56 bits. Utiliza tres claves de encriptación independientes de 56 bits por bloque de 64 bits, lo que proporciona una fuerza de encriptación significativamente más fuerte que DES.
- AES proporciona seguridad más fuerte que DES y es informáticamente más eficaz que 3DES. AES ofrece tres longitudes de llave diferentes: 128 bits, 192 bits y 256 bits.

- SEAL es un cifrado de flujo, lo que significa que encripta datos continuamente en lugar de encriptar bloques de datos. SEAL utiliza una llave de 160 bits.

3.3. Integridad

La integridad de los datos significa que los datos que se reciben son exactamente los mismos datos que se enviaron. Potencialmente, los datos podrían ser interceptados y modificados. Por ejemplo, en la figura, suponga que un cheque por $100 dólares está escrito para Alex. El cheque se envía por correo a Alex, pero es interceptado por un actor de amenaza. El actor de la amenaza cambia el nombre del cheque a Jeremy y el monto del cheque a $1000 dólares e intenta cobrarlo. Dependiendo de la calidad de la falsificación en el cheque alterado, el atacante podría tener éxito.

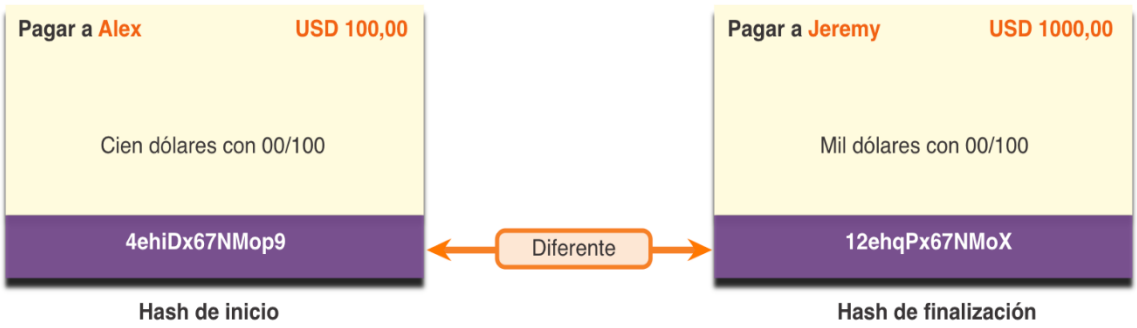


Figura 17: Integridad Marco IPsec.
Fuente: *Cisco Networking Academy* (2022).

Debido a que los datos VPN se transportan a través de Internet público, se requiere un método para probar la integridad de los datos, para garantizar que el contenido no se haya alterado. El *Hashed Message Authentication Code* (HMAC) es un algoritmo de integridad de datos que garantiza la integridad del mensaje utilizando un valor *hash*. La figura destaca los dos

algoritmos HMAC más comunes. Haga clic en cada algoritmo para más información.

Nota: Cisco ahora califica a SHA-1 como legado y recomienda al menos SHA-256 para integridad.

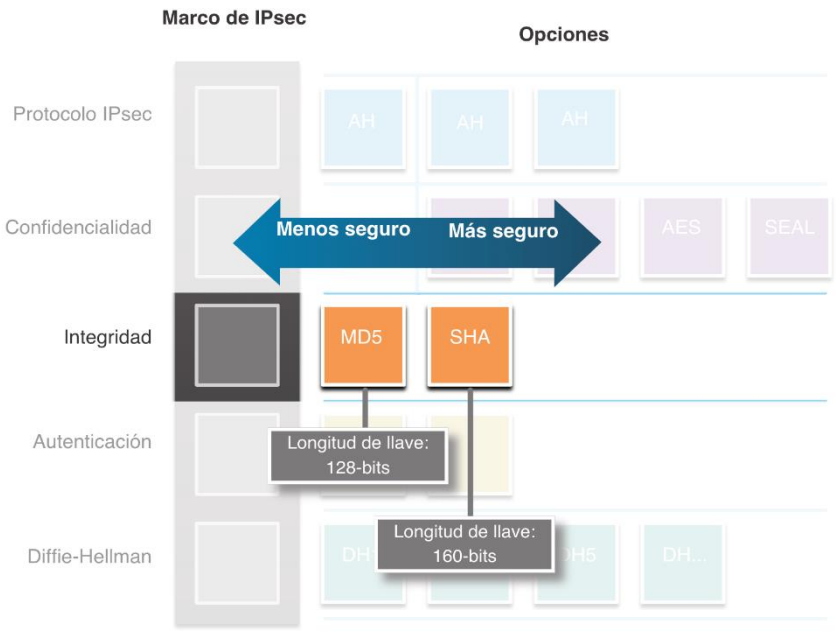


Figura 18: MD5 y SHA en Marco IPsec.
Fuente: *Cisco Networking Academy* (2022).

- *Message-Digest* 5 (MD5) utiliza una llave secreta compartida de 128 bits. El mensaje de longitud variable y la llave secreta compartida de 128 bits se combinan y se ejecutan a través del algoritmo hash HMAC-MD5. La salida es un hash de 128 bits.

- El *Secure Hash Algorithm* (SHA) utiliza una llave secreta de 160 bits. El mensaje de longitud variable y la llave secreta compartida de 160 bits son combinados y se ejecutan a través del algoritmo HMAC-SHA-1. La salida es un *hash* de 160 bits.

3.4. Servidor

Al realizar negocios a larga distancia, debe saber quién está al otro lado del teléfono, correo electrónico o fax. Lo mismo sucede con las redes VPN. El dispositivo en el otro extremo del túnel VPN se debe autenticar antes de que la ruta de comunicación se considere segura. La figura destaca los dos métodos de autenticación de pares.

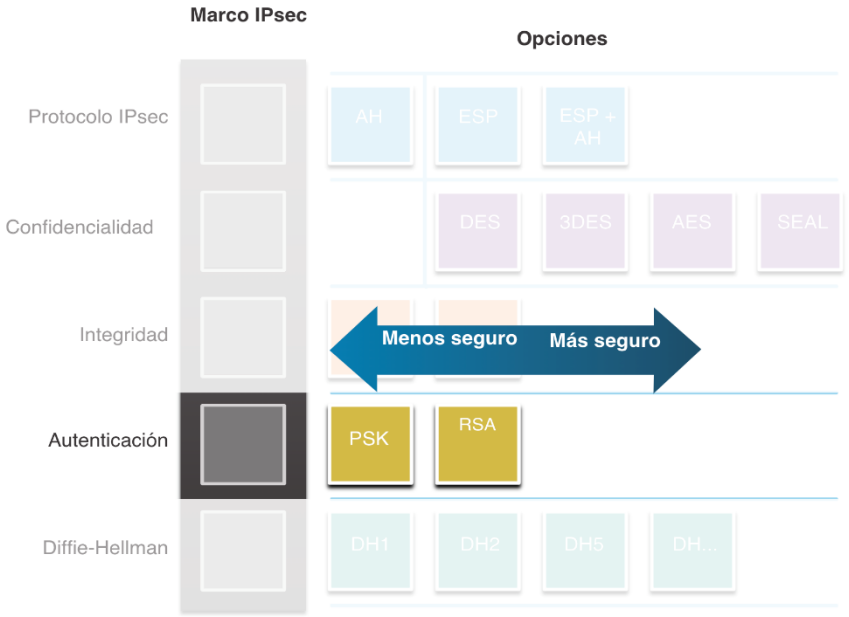


Figura 19: Métodos de autentificación en Marco IPsec.

Fuente: *Cisco Networking Academy* (2022).

- Un valor de *pre-shared secret key* (PSK) se ingresa manualmente en cada par. El PSK se combina con otra información para formar la clave de autenticación. Los PSK son fáciles de configurar manualmente, pero no se escalan bien, porque cada par IPsec debe configurarse con el PSK de todos los demás pares con los que se comunica.

- La autenticación de *Rivest, Shamir y Adleman* (RSA) utiliza certificados digitales para autenticar a los pares. El dispositivo local deriva un hash y lo cifra con su clave privada. El hash encriptado se adjunta al mensaje y se reenvía al extremo remoto y actúa como una firma. En el extremo remoto, se descifra el hash cifrado con la clave pública del extremo local. Si el *hash* descifrado coincide con el *hash* recalculado, la firma es genuina. Cada par debe autenticar a su par opuesto antes de que el túnel se considere seguro.

La figura muestra un ejemplo de autenticación PSK. En el dispositivo local, la llave de autenticación y la información de identidad se envían a través de un algoritmo *hash* para formar el *hash* para el par local (*Hash* _L). La autenticación unidireccional se establece enviando *Hash* _L al dispositivo remoto. Si el dispositivo remoto puede crear independientemente el mismo *hash*, el dispositivo local se autentica. Después que el dispositivo remoto autentica el dispositivo local, el proceso de autenticación comienza en la dirección opuesta, y todos los pasos se repiten desde el dispositivo remoto al dispositivo local.

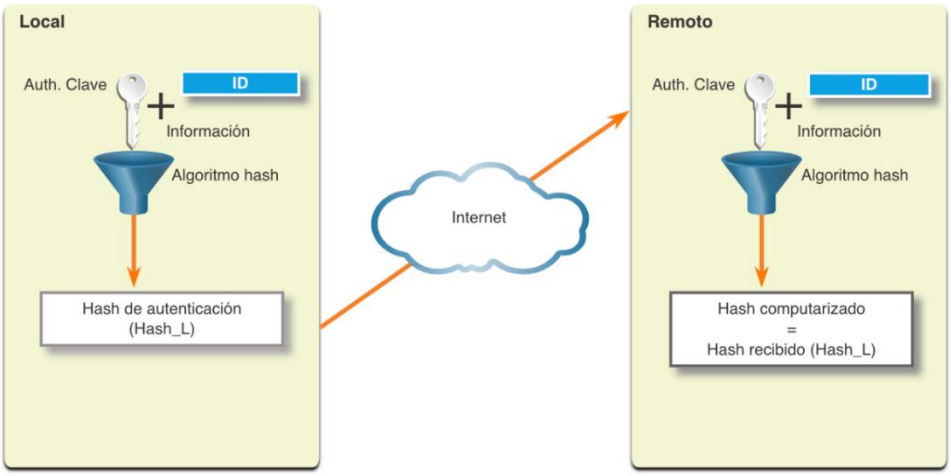


Figura 20: Autentificación PSK.

Fuente: *Cisco Networking Academy* (2022).

La figura muestra un ejemplo de autenticación RSA. En el dispositivo local, la llave de autenticación y la información de identidad se envían a través del algoritmo hash para formar el hash para el par local. (*Hash*_L). Luego, *Hash* _L se encripta utilizando la llave de encriptación privada del dispositivo local. Esto crea una firma digital. La firma digital y un certificado digital se envían al dispositivo remoto. La llave de encriptación pública para descifrar la firma se incluye en el certificado digital. El dispositivo remoto verifica la firma digital descifrándola con la llave de cifrado pública. El resultado es *Hash*_L. A continuación, el dispositivo remoto crea *Hash* _L de forma independiente a partir de la información almacenada. Si el *Hash* _L calculado es igual al *Hash* _L desencriptado, el dispositivo local se autentica. Después de que el dispositivo remoto autentica el dispositivo local, el proceso de autenticación comienza en la dirección opuesta, y todos los pasos se repiten desde el dispositivo remoto al dispositivo local.

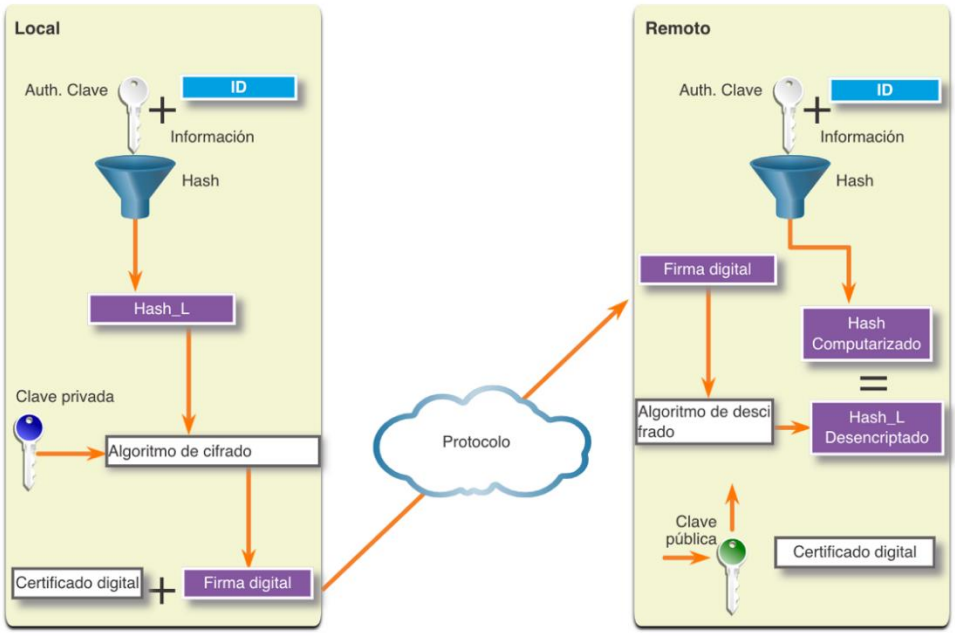


Figura 21: Autentificación RSA.

Fuente: *Cisco Networking Academy* (2022).

Intercambio seguro de llaves con *Diffie-Hellman*.

Los algoritmos de encriptación requieren una llave secreta simétrica y compartida para realizar el encriptado y desencriptado. ¿Cómo obtienen la llave secreta compartida los dispositivos de encriptado y desencriptado? El método más sencillo de intercambio de llaves es utilizar un método de intercambio de llaves públicas, como *Diffie-Hellman* (DH), como se muestra en la figura.

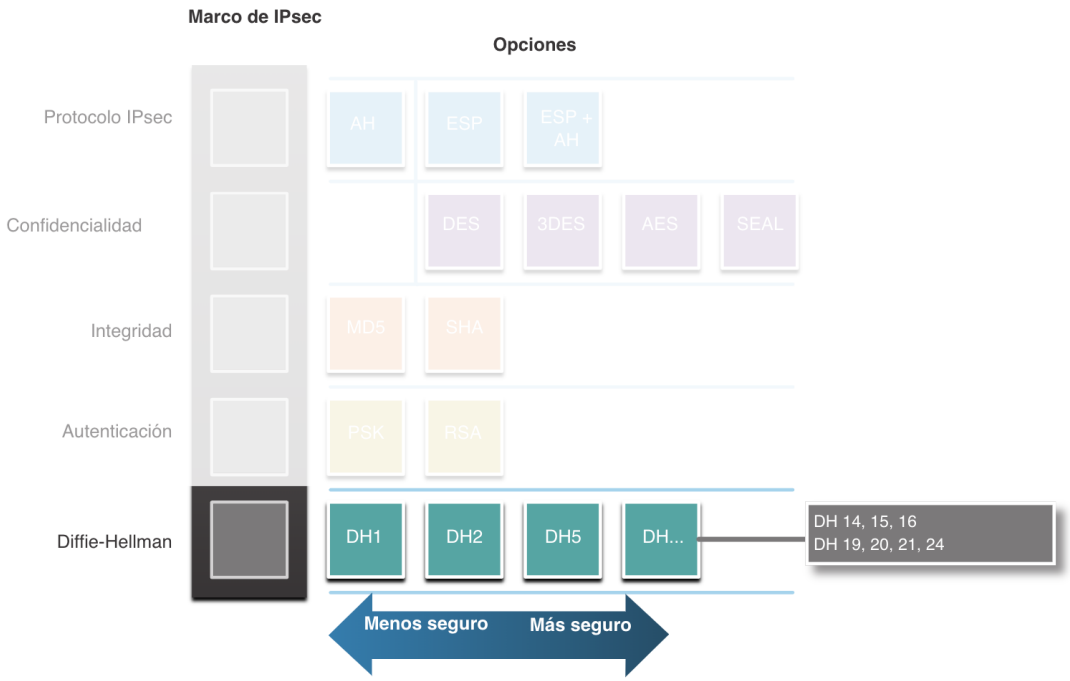


Figura 22: Diffie-Hellman.

Fuente: *Cisco Networking Academy* (2022).

DH proporciona una forma para que dos pares establezcan una llave secreta compartida que solo ellos conocen, a pesar de que se comunican a través de un canal inseguro. Las variaciones del intercambio de llaves DH se especifican como grupos DH:

- Los grupos DH 1, 2 y 5 ya no deberían usarse. Estos grupos admiten un tamaño de llave de 768 bits, 1024 bits y 1536 bits, respectivamente.

- Los grupos DH 14, 15 y 16 usan tamaños de llave más grandes con 2048 bits, 3072 bits y 4096 bits, respectivamente, y se recomienda su uso hasta 2030.

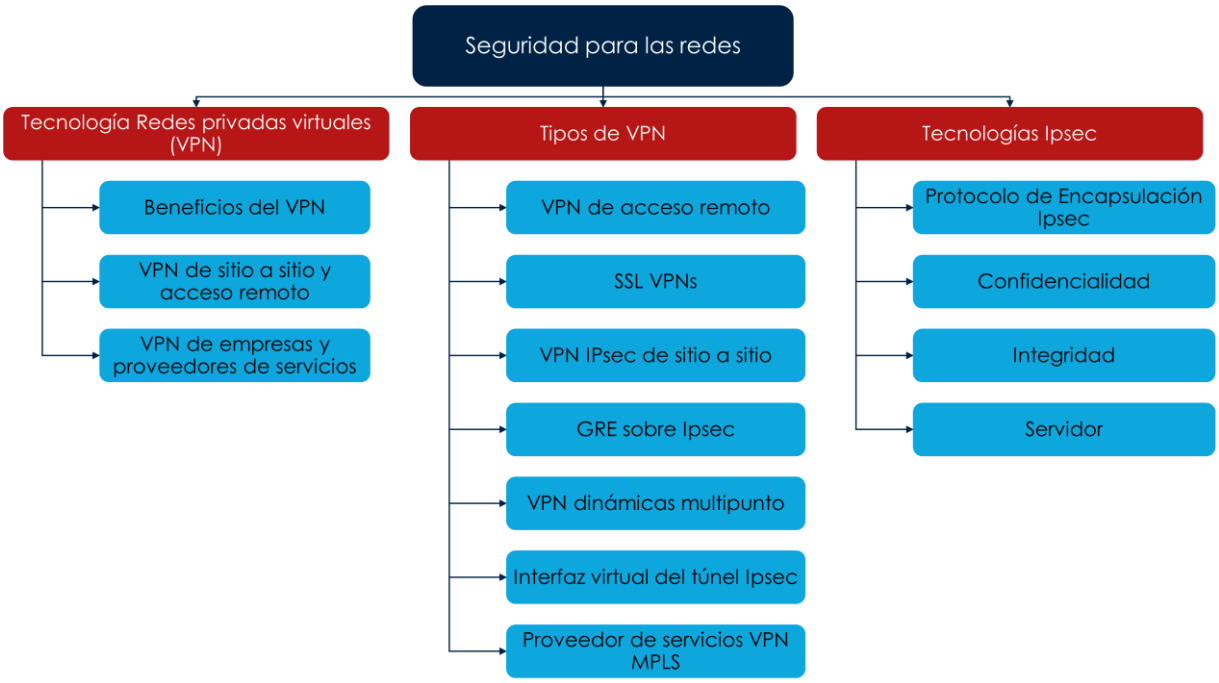
- Los grupos DH 19, 20, 21 y 24 con tamaños de llave respectivos de 256 bits, 384 bits, 521 bits y 2048 bits admiten la criptografía de curva elíptica

(ECC), que reduce el tiempo necesario para generar llaves. El grupo DH 24 es la encriptación preferida de próxima generación.

El grupo DH que elija debe ser lo suficientemente fuerte o tener suficientes bits para proteger las llaves IPsec durante la negociación. Por ejemplo, el grupo DH 1 es lo suficientemente fuerte como para admitir la encriptación DES y 3DES, pero no AES. Por ejemplo, si los algoritmos de cifrado o autenticación usan una clave de 128 bits, use el grupo 14, 19, 20 o 24. Sin embargo, si los algoritmos de cifrado o autenticación usan una clave de 256 bits o superior, use el grupo 21 o 24.

Cierre

Por medio del siguiente organizador gráfico, se destacan las ideas clave de esta semana:



Una VPN es virtual porque transporta la información dentro de una red privada, pero, en realidad, esa información se transporta usando una red pública. Una VPN es privada porque el tráfico se encripta para preservar la confidencialidad de los datos mientras los transporta por la red pública. Los beneficios de las VPNs son el ahorro de costos, la seguridad, la escalabilidad y la compatibilidad. Las VPNs se implementan comúnmente en una de las siguientes configuraciones: sitio a sitio o acceso remoto. Las VPNs se pueden administrar e implementar como VPN empresariales y VPN de proveedor de servicios.

Como se muestra en la figura, las VPNs de acceso remoto permiten a los usuarios remotos y móviles conectarse de forma segura a la empresa mediante la creación de un túnel encriptado. Las VPNs de acceso remoto se pueden crear utilizando IPsec o SSL. Cuando un cliente negocia una conexión VPN SSL con la puerta de enlace VPN, realmente se conecta mediante TLS. SSL utiliza la infraestructura de llave pública y los certificados digitales para autenticar a sus pares. Las VPNs de sitio a sitio se utilizan para conectar redes a través de otra red no confiable como Internet. En una VPN de sitio a sitio, los usuarios finales envían y reciben tráfico normal de TCP/IP sin encriptar a través de un dispositivo VPN de terminación. La terminación de VPN generalmente se denomina puerta de enlace VPN. Una puerta de enlace VPN podría ser un enrutador o un firewall. GRE es un protocolo de túnel VPN no seguro de sitio a sitio. DMVPN es una solución de software de Cisco para construir fácilmente VPN múltiples, dinámicas y escalables. Al igual que los DMVPN, IPsec *Virtual Tunnel Interface* (VTI) simplifica el proceso de configuración requerido para admitir múltiples sitios y acceso remoto. Las configuraciones de IPsec VTI se aplican a una interfaz virtual en lugar de la asignación estática de las sesiones de IPsec a una interfaz física. IPsec VTI puede enviar y recibir el tráfico IP unicast y multicast encriptado. MPLS puede proporcionar a los clientes soluciones VPN administradas; por lo tanto, asegurar el tráfico entre los sitios del cliente es responsabilidad del proveedor del servicio. Hay dos tipos de soluciones MPLS VPN soportadas por los proveedores de servicios, Capa 3 MPLS VPN y Capa 2 MPLS VPN.

IPsec protege y autentica los paquetes IP entre el origen y el destino. IPsec puede proteger el tráfico de la Capa 4 a la Capa 7. Utilizando el marco IPsec, IPsec proporciona confidencialidad, integridad, autenticación de origen y *Diffie-Hellman*. La elección del protocolo de encapsulación IPsec es el primer

bloque de construcción del marco. IPsec encapsula paquetes usando AH o ESP. El grado de confidencialidad depende del algoritmo de encriptación y la longitud de la llave utilizada en el algoritmo de encriptación. El *Hashed Message Authentication Code* (HMAC) es un algoritmo que garantiza la integridad del mensaje mediante un valor *hash*. El dispositivo en el otro extremo del túnel VPN se debe autenticar antes de que la ruta de comunicación se considere segura. Se introduce un valor PSK en cada par manualmente. El PSK se combina con otra información para formar la clave de autenticación. La autenticación RSA utiliza los Certificados digitales para autenticar a los pares. El dispositivo local deriva un hash y lo cifra con su clave privada. El hash encriptado se adjunta al mensaje y se reenvía al extremo remoto y actúa como una firma. DH proporciona una forma para que dos pares establezcan una llave secreta compartida que solo ellos conocen, a pesar de que se comunican a través de un canal inseguro.

Referencias bibliográficas

- Cisco Networking Academy (2022). Recuperado en agosto de 2022, disponible en: www.netacad.com