Guía de Seguridad de las TIC
CCN-STIC-836

Seguridad en Redes Privadas Virtuales (VPN)



Febrero 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2022.02.04 12:55:30 +01'00'

Pº de la Castellana 109, 28046 Madrid
© Centro Criptológico Nacional, 2022
NIPO: 083-22-063-X

Fecha de Edición: febrero 2022

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

PRÓLOGO

En un mundo cada vez más complejo y globalizado, en el que las tecnologías de la información y la comunicación (TIC) desempeñan un papel de suma importancia, hemos de ser conscientes de que la gestión adecuada de la ciberseguridad constituye un reto colectivo al que necesariamente hemos de enfrentar. Resulta necesario garantizar la protección de la capacidad económica, tecnológica y política de nuestro país, máxime cuando la proliferación de ataques dirigidos y el robo de información sensible representan una realidad incontestable.

Por ello, resulta imprescindible estar al día de las amenazas y vulnerabilidades asociadas al uso de las nuevas tecnologías. El conocimiento de los riesgos que se ciernen sobre el ciberespacio ha de servir para implementar con garantías las medidas, tanto procedimentales como técnicas y organizativas, que permitan un entorno seguro y confiable.

La Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia (CNI), encomienda al Centro Nacional de Inteligencia el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información y de protección de la información clasificada, a la vez que confiere a su Secretario de Estado Director la responsabilidad de dirigir el Centro Criptológico Nacional (CCN).

Partiendo del conocimiento y la experiencia del CNI sobre amenazas y vulnerabilidades en materia de riesgos emergentes, el Centro realiza, a través del Centro Criptológico Nacional, regulado por el Real Decreto 421/2004, de 12 de marzo, diversas actividades directamente relacionadas con la seguridad de las TIC, orientadas a la formación de personal experto, al empleo de tecnologías de seguridad adecuadas y a la aplicación de políticas y procedimientos de seguridad.

Precisamente, esta serie de documentos CCN-STIC es un claro reflejo de la labor que este organismo lleva a cabo en materia de implementación de seguridad, permitiendo la aplicación de políticas y procedimientos, pues las guías han sido elaboradas con un claro objetivo: mejorar el grado de ciberseguridad de las organizaciones, conscientes de la importancia que tiene el establecimiento de un marco de referencia en esta materia que sirva de apoyo para que el personal de la Administración lleve a cabo la difícil tarea de proporcionar seguridad a los sistemas de las TIC bajo su responsabilidad.

Con esta serie de documentos, el Centro Criptológico Nacional, en cumplimiento de sus cometidos y de lo reflejado en el Real Decreto 3/2010 por el que se regula el Esquema Nacional en el ámbito de la Administración electrónica, contribuye a mejorar la ciberseguridad española y mantener las infraestructuras y los sistemas de información de todas las administraciones públicas con unos niveles óptimos de seguridad. Todo ello, con el fin de generar confianza y garantías en el uso de estas tecnologías, protegiendo la confidencialidad de los datos y garantizando su autenticidad, integridad y disponibilidad.

Febrero de 2022



Paz Esteban López
Secretaria de Estado
Directora del Centro Criptológico Nacional

ÍNDICE

1. INTRODUCCIÓN 7
2. OBJETO 9
3. ALCANCE 10
4. REDES PRIVADAS VIRTUALES (VPN) 11
4.1 DEFINICIÓN Y GENERALIDADES 11
4.2 TIPOS DE VPN 13
4.3 VPN CLOUD 15
4.4 TECNOLOGÍAS VPN 17
4.4.1 VPN DE NIVEL DE APLICACIÓN 19
4.4.2 VPN DE NIVEL DE TRANSPORTE 19
4.4.3 VPN DE NIVEL DE RED 20
4.4.4 VPN DE NIVEL DE ENLACE 21
4.4.5 COMPARATIVA DE VPN SEGÚN SU NIVEL DE OPERACIÓN 22
4.5 ARQUITECTURA DE VPN 24
4.5.1 MODO DE IMPLEMENTACIÓN 24
4.5.2 UBICACIÓN DE LOS CONCENTRADORES VPN 26
5. REQUISITOS GENERALES DEL SISTEMA VPN 27
6. PROCESO DE PLANIFICACIÓN Y DESPLIEGUE DE VPN 30
6.1 IDENTIFICACIÓN DE NECESIDADES Y REQUISITOS 30
6.2 DISEÑO DE LA VPN 31
6.3 SELECCIÓN DEL PRODUCTO VPN 33
6.4 PRUEBAS DE LA SOLUCIÓN VPN 33
6.5 IMPLANTACIÓN Y DESPLIEGUE 34
6.6 OPERACIÓN Y MANTENIMIENTO 35
7. ASPECTOS CRIPTOLÓGICOS 36
8. EJEMPLO DE PROCESO DE PLANIFICACIÓN Y DESPLIEGUE DE UNA VPN 37
8.1 IDENTIFICACIÓN DE NECESIDADES Y REQUISITOS. 37
8.2 DISEÑO DE LA VPN 38
8.3 SELECCIÓN DEL PRODUCTO VPN 41
8.4 PRUEBAS DE LA SOLUCIÓN VPN 41
8.5 IMPLANTACIÓN Y DESPLIEGUE 41
ANEXO A. VPN TLS 42
A.1 MODOS DE FUNCIONAMIENTO 43
A.2 FUNCIONAMIENTO DE TLS: *HANDSHAKE* & *RECORD PROTOCOLS* 44
A.2.1 *HANDSHAKE PROTOCOL* 44
A.2.2 RECORD PROTOCOL 47
A.3 *CIPHER SUITES* Y OTROS PARÁMETROS CRIPTOGRÁFICOS 48
A.3.1 TLS 1.2 48
A.3.2 TLS 1.3 52

ANEXO B. IPSEC 54
B.1 MODOS DE FUNCIONAMIENTO 55
B.1.1 MODO TRANSPORTE 55
B.1.2 MODO TÚNEL 56
B.2 ASOCIACIONES DE SEGURIDAD (SA) 57
B.3 PROTOCOLOS AH Y ESP 57
B.3.1 PROTOCOLO AH 57
B.3.2 PROTOCOLO ESP 58
B.4 PROTOCOLO IKE 59
B.4.1 IKEV2: INTERCAMBIOS 60
B.4.2 IKEV2: GENERACIÓN DE CLAVES 61
B.4.3 IKEV2: TIEMPO DE VIDA DE LAS SA 62
B.4.4 IKEV2: *PERFECT FORWARD SECRECY (PFS)* 62
B.5 USO DE NAT CON IPSEC 62
ANEXO C. MACSEC 64
C.1 FUNCIONAMIENTO 64
C.1.1 AUTENTICACIÓN Y DERIVACIÓN DE CLAVE CAK 65
C.1.2 DERIVACIÓN DE CLAVES ICK Y KEK 68
C.1.3 CIPHER SUITES Y PARÁMETROS CRIPTOGRÁFICOS 72
C.2 USOS DE MACSEC 74
C.2.1 MACSEC SOBRE LAN 74
C.2.2 MACSEC SOBRE WAN 76
ANEXO D. WIREGUARD 78
D.1 MODOS DE FUNCIONAMIENTO 80
D.2 FUNCIONAMIENTO DE WIREGUARD: CRYPTOKEY ROUTING 81
D.3 FLUJOS DE COMUNICACIÓN 82
D.3.1 REALIZACIÓN DE HANDSHAKE 82
D.3.2 ENVÍO DE INFORMACIÓN 83
D.3.3 RECIBIR INFORMACIÓN 83
D.4 PROTOCOLO Y CRIPTOGRAFÍA 84
D.4.1 EL SILENCIO COMO VIRTUD 84
D.4.2 MODO OPCIONAL DE PRE-SHARED KEY SIMÉTRICAS 85
D.4.3 MITIGACIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO Y COOKIES 85
D.4.4 TIPOS DE MENSAJES 86
D.5 RENDIMIENTO 87
D.6 VERIFICACIONES FORMALES 87
ANEXO E. GLOSARIO DE TÉRMINOS 88
ANEXO F. REFERENCIAS 92

ÍNDICE DE FIGURAS

Figura 1. VPN *site-to-site* 13
Figura 2. VPN de acceso remoto 14
Figura 3. VPN de equipo a equipo 15
Figura 4. Acceso a servicios en la nube con una VPN de acceso remoto tradicional 16
Figura 5. VPNaaS 17
Figura 6. Niveles de la familia de protocolos TCP/IP 18
Figura 7. Arquitectura VPN en DMZ dedicada 27
Figura 8. Arquitectura de la VPN TLS diseñada para la organización. 39
Figura 9. *TLS Handshake Protocol* 45
Figura 10. Estructura Paquete TLS Record 48
Figura 11. IPsec modo transporte 55
Figura 12. Construcción del paquete IPsec en modo transporte. 55
Figura 13. IPsec modo túnel 56
Figura 14. Construcción del paquete IPsec en modo túnel. 56
Figura 15. Construcción del paquete AH 58
Figura 16. Construcción del paquete ESP. 59
Figura 17. Diagrama de fases generales de MACsec 65
Figura 18. Diagrama de Autenticación y generación de CAK mediante 802.1X/EAP 67
Figura 19. Cifrado y cálculo del ICV MACsec 73
Figura 20. MACsec sobre LAN 74
Figura 21. MACsec sobre VXLAN 76
Figura 22. WAN MACsec ejemplo *site-to-site* 77
Figura 23. WireGuard: Tabla Cryptokey Routing 81
Figura 24. WireGuard: Handshake (1-RTT) en condiciones normales 82
Figura 25. WireGuard: Repetición de handshake por alta carga de CPU 82
Figura 26. WireGuard: Paquete iniciador de handshake 86
Figura 27. WireGuard: Paquete de respuesta de handshake 86
Figura 28. WireGuard: Paquete con valor cookie 86
Figura 29. WireGuard: Paquetes de datos 86
Figura 30. WireGuard: Comparativa de rendimiento con IPSec y OpenVPN 87

ÍNDICE DE TABLAS

Tabla 1. Comparativa de VPN según su nivel de operación 24
Tabla 2. Comparativa de VPN según Nivel de operación. 40
Tabla 3. Características de las VPN TLS 44
Tabla 4. Grupos DH y fortaleza (RFC 7919 Apéndice A) 49
Tabla 5. Comparación de Niveles de Seguridad y Longitudes de Claves 50
Tabla 6. Características de las VPN IPsec. 55
Tabla 7. Curvas Elípticas y Fortaleza 61
Tabla 8. *Cipher suite* aceptadas 72

1. INTRODUCCIÓN

1. Hoy en día, y dada la gran expansión de Internet a lo largo del mundo, las organizaciones han desarrollado nuevas necesidades de conectividad, aprovechando las ventajas que ofrecen las conexiones a través de Internet. Entre estas necesidades, se encuentran las de conectar entre sí sedes u oficinas de la organización, dar acceso a la red de la organización a proveedores externos, o permitir a sus propios empleados el acceso a los recursos internos de la organización desde lugares remotos.

2. Dado que los datos transmitidos viajan a través de redes públicas, es necesario implementar mecanismos de protección que aseguren la confidencialidad, integridad y disponibilidad del tráfico transmitido en la comunicación.

3. Las redes privadas virtuales o por su terminología en inglés *virtual private networks" (VPN*) son una serie de tecnologías que proporcionan una conexión segura para el acceso a información y recursos internos de una organización, utilizando como soporte de comunicaciones cualquier red del dominio público, como Internet.

4. A través de las VPN, la organización puede extender su red interna para permitir que sus sedes o usuarios remotos se conecten a sus recursos privados como si estuviesen dentro de la red. Al mismo tiempo dichos recursos permanecen inaccesibles desde las redes públicas que soportan la conexión.

5. Las principales ventajas de implementar VPN son las siguientes:

   a) **Seguridad** en los siguientes aspectos:

      - Confidencialidad de los datos al emplear mecanismos de cifrado.
      - Integridad de los datos, al emplear mecanismos de *hashing*.
      - Autenticación, al emplear mecanismos para que origen y destino se autentiquen mutuamente.

   b) Aplicación de políticas de seguridad corporativas, dado que el cliente remoto se convierte en miembro de la red interna de la organización..

   c) **Ahorro de costes** frente a otros mecanismos de implementación de comunicaciones seguras, como por ejemplo enlaces privados dedicados, o el alquiler de infraestructura proporcionada por un operador de telecomunicaciones. El uso de la infraestructura pública de Internet es mucho menos costoso. Se puede prescindir de enlaces privados adicionales.

   d) **Escalabilidad**, ya que la ampliación de la infraestructura para conexiones remotas se puede realizar de forma simple.

   e) **Flexibilidad**, ya que las VPN permiten múltiples parámetros y opciones de configuración para satisfacer los requisitos de seguridad de cada conexión remota.

f) **Simplicidad**, al emplearse una misma tecnología para todas las comunicaciones remotas, que además es la tecnología empleada para conexiones públicas (Internet) o internas (Intranet).

6. Las tecnologías VPN pueden ser implementadas mediante soluciones basadas únicamente en *software* (sobre un sistema operativo multipropósito), o mediante soluciones *software/hardware* en equipos dedicados (*appliance*).

7. Finalmente, es necesario indicar que, pese a todas las ventajas y mecanismos de seguridad que ofrecen las tecnologías VPN, la extensión de la red interna de la organización a través de Internet, no deja de añadir riesgos sobre la seguridad de las comunicaciones y de los equipos de la red interna. Estos riesgos deben ser tratados y mitigados, con el objetivo de garantizar la confidencialidad, integridad y disponibilidad de estas infraestructuras de comunicaciones y los datos que se transmiten a través de ellas.

2. OBJETO

8. El objeto del documento es describir las principales tecnologías VPN para el establecimiento de conexiones a través de redes de comunicación, principalmente Internet, y **proporcionar una guía de buenas prácticas que ayude a las organizaciones en el proceso de planificación, despliegue y configuración de VPN.** Para ello, se indicarán los requisitos que deben tenerse en cuenta a la hora de seleccionar e implementar una VPN, en el ámbito del Esquema Nacional de Seguridad y en el ámbito de sistemas que manejan información clasificada.

9. A lo largo de la guía, se identifican las características y ventajas de las tecnologías VPN mediante el análisis de los protocolos de seguridad empleados por cada una de ellas, así como las alternativas de configuración e implantación que estas tecnologías ofrecen.

10. Para tener una información más detallada de la instalación, configuración y administración de VPN, se deberán consultar las guías sobre equipos y soluciones concretas de cada fabricante.

11. Las pautas que se establecen son de carácter general, de forma que puedan resultar de aplicación a entidades de distinta naturaleza, dimensión y sensibilidad, sin entrar en casuísticas específicas. Por ello, es de esperar que cada organización las particularice para adaptarlas a su entorno singular.

3. ALCANCE

12. Esta guía se centra principalmente en las tecnologías VPN más extendidas, si bien siempre que sea posible se plantearán requisitos de seguridad que sean independientes de la tecnología concreta. No se referencia ninguna solución VPN concreta de fabricantes.

13. Esta guía contiene recomendaciones de aplicación al diseño, instalación y configuración de una infraestructura de acceso remoto segura, basada en tecnologías de redes privadas virtuales, tanto en entornos de red cerrados como en su interconexión a redes públicas, como Internet.

14. Las pautas y recomendaciones de la presente guía quedan sometidas a una continua revisión debido al constante avance tecnológico, así como a la aprobación de nuevos estándares y la aparición de nuevas vulnerabilidades y herramientas.

4. REDES PRIVADAS VIRTUALES (VPN)

4.1 DEFINICIÓN Y GENERALIDADES

15. Una Red Privada Virtual (VPN, *Virtual Private Network*) es una tecnología que establece una conexión virtual segura, conocida como "túnel", construida sobre una red física insegura (normalmente una red pública como Internet). Una VPN proporciona múltiples mecanismos de seguridad para proteger la información transmitida, y para permitir el acceso seguro y controlado a los recursos que protege.

16. Las VPN se establecen mediante servidores o *gateways* VPN, que son los elementos de red encargados de la creación o terminación de una o varias VPN. Se ubican, por lo tanto, en el extremo de la comunicación, y se encargan de realizar el encapsulado, desencapsulado, cifrado y descifrado del tráfico a través de la VPN y de darle validez en la red local. El concentrador VPN debe ser un equipo con altas medidas de seguridad, y con los mínimos servicios habilitados en el sistema.

17. Las VPN utilizan protocolos de seguridad criptográficos (*tunneling protocols*) que son los que proporcionan protección a la información transmitida. Los más extendidos son **TLS** (***Transport Layer Security Protocol***)[1] e **IPsec** (***Internet Protocol Security***).

18. Las principales propiedades de seguridad proporcionadas por las VPN son las que se indican a continuación. Algunas de ellas son proporcionadas por los protocolos de seguridad empleados, mientras que otras son proporcionadas por los servidores VPN:

    a) **Confidencialidad**. Protege los datos de accesos no autorizados. Esto es posible gracias a mecanismos de cifrado simétrico de datos, que utilizan algoritmos criptográficos y claves secretas (valores conocidos solo por dos partes entre las que se establece la comunicación). Los datos solo pueden ser descifrados por alguien que conozca la clave secreta.

    b) **Integridad y Autenticidad**. Protege los datos frente a modificaciones no autorizadas durante la comunicación. Del mismo modo, garantiza que el mensaje procede del emisor auténtico. Ambas características son posibles gracias a mecanismos que generan un valor de autenticación de mensaje (MAC, *Message Authentication Code*). Si los datos son alterados de forma no autorizada, el nuevo resultado calculado sobre el mensaje será distinto. Y el cálculo del valor MAC correcto solo es posible cuando emisor y receptor conocen la clave secreta correcta.

    c) **Autenticación mutua**. Garantiza que la comunicación se desarrolla entre los auténticos participantes. Esto es posible porque cada extremo de la comunicación confirma la identidad del otro. En general, la autenticación se

[1] También conocido como SSL, que es la versión antigua de TLS.

lleva a cabo mediante el uso de certificados de clave pública X.509 [1] emitidos por una CA reconocida por ambos extremos.

d) **Protección frente a reenvíos.** Garantiza que los datos no serán entregados más de una vez. De esta forma, un atacante no podrá interceptar y retirar alguno de los paquetes que componen el mensaje, e insertar otros paquetes malintencionados en la comunicación. Esto es posible gracias a mecanismos de secuencias asociados a los paquetes.

e) **Protección frente al análisis de tráfico**. Garantiza que no se podrá extraer información valiosa a través del análisis del tráfico de la comunicación (como datos sobre emisor y receptor, frecuencia de la comunicación, cantidad de datos transmitidos, etc.).

f) **Control de acceso**. Garantiza que sólo los usuarios autorizados podrán acceder a determinados recursos de la organización. Esto es posible gracias a mecanismos de filtrado, que permiten habilitar o bloquear ciertos tipos de tráfico de red, por ejemplo, permitiendo los accesos web, pero no la compartición de ficheros.

g) **Evaluación del estado de seguridad del dispositivo cliente (*Host Check*)**, chequeando las herramientas de protección de las que dispone, como un software antivirus actualizado, firewalls, y parches de seguridad. Según los resultados del chequeo, se puede permitir o denegar el acceso a la red interna, a cierta categoría de recursos o a recursos individuales.

h) **Características de proxy,** de forma que el servidor VPN hace de intermediario entre la red pública y los recursos de la red interna.

i) **Integración con otros elementos de seguridad corporativos,** a los que el servidor VPN puede enviar información sobre el tráfico, el usuario, el dispositivo y la actividad que se está realizando.

19. Aunque las VPN reducen el riesgo asociado a las comunicaciones realizadas a través de redes no seguras, es importante entender que no lo eliminan al completo. Se debe tener en cuenta lo siguiente:

a) Existen riesgos asociados a la fortaleza de la implementación de la VPN, como, por ejemplo, debilidades del algoritmo de cifrado o del *software* que lo implementa, que la clave secreta se vea comprometida, uso de valores aleatorios que no sean generados con suficiente aleatoriedad, etc.

b) **Medidas complementarias de vigilancia**. Hay escenarios en que los sistemas, por su origen y naturaleza, tienen grandes dificultades para cumplir con los requisitos de seguridad exigidos al tipo de información que manejan y servicios que prestan. En estos casos, es donde cobra importancia la posibilidad de implementar sistemas complementarios de vigilancia que equilibren la superficie de exposición.

- Una medida complementaria de viglancia importante en las conexciones VPN será la monitorización del tráfico intercambiado en la conexión VPN

para apoyar la identificación de anomalías en el comportamiento; flujos de comunicación en la red, protocolos utilizados y estadísticas en tiempo real.

4.2 TIPOS DE VPN

20. Una infraestructura VPN está, normalmente, formada por dos (2) elementos principales:

    a) **El servidor, concentrador o *gateway* VPN**. Es el elemento básico de la infraestructura VPN encargado de establecer las conexiones seguras (túnel VPN) con los dispositivos del usuario o con otros servidores VPN.

    b) **Cliente VPN**. Es el software que debe ser instalado en los dispositivos de usuario para poder establecer la conexión segura con el servidor VPN.

21. Los tres (3) escenarios de VPN más frecuentes son: VPN entre sedes remotas de la organización (VPN *site-to-site*), VPN entre cliente remoto y la sede de la organización (VPN de acceso remoto) y VPN entre equipos (VPN de equipo a equipo).

    a) **VPN *site-to-site***. Es la empleada para proteger las comunicaciones entre dos redes, a través de una red pública (como por ejemplo Internet), manteniendo la seguridad y enrutando las comunicaciones. Suele emplearse para conectar oficinas secundarias, con una sede central. Es más económico y seguro que utilizar redes de área extensas (WAN, *Wide Area Networks*).

    Normalmente se implementa con un servidor VPN en cada extremo de la comunicación, de forma que entre ambos servidores se establece la conexión VPN (ver Figura). Cuando un equipo en la red A, necesite establecer comunicación segura con otro equipo en la red B, el tráfico será enrutado automáticamente a través de la conexión VPN establecida entre los dos servidores VPN.

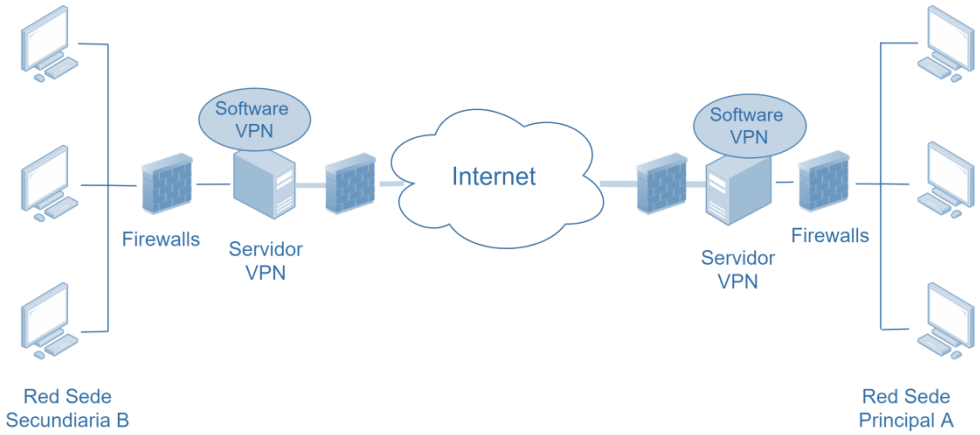


Figura 1. VPN *site-to-site*

El servidor VPN puede ser un dispositivo físico dedicado (*appliance*) o puede formar parte de otro dispositivo de red, como puede ser un enrutador (*router*) o un cortafuegos (*firewall*).

En este modelo, los equipos cliente no tienen que tener instalado ningún software VPN, ni requieren ningún tipo de configuración especial para el uso de la VPN.

b) **VPN de acceso remoto**. Es la empleada para proteger las comunicaciones entre un equipo individual de usuario y la red interna de la organización. Normalmente se emplean para los usuarios que trabajan de forma remota, y que requieren de un acceso a los recursos internos de la organización, a través de la infraestructura proporcionada por una red pública, como por ejemplo Internet.

El concentrador VPN puede ser un dispositivo físico dedicado (*appliance*) o puede formar parte de otro dispositivo de red, como puede ser un enrutador (*router*) o un cortafuegos (*firewall*).

En este modelo, los equipos cliente tienen que tener instalado y correctamente configurado el software VPN, y deben autenticarse antes de poder usar la VPN. En algunos casos (VPN SSL) el software cliente puede tratarse de un navegador o *browser*.

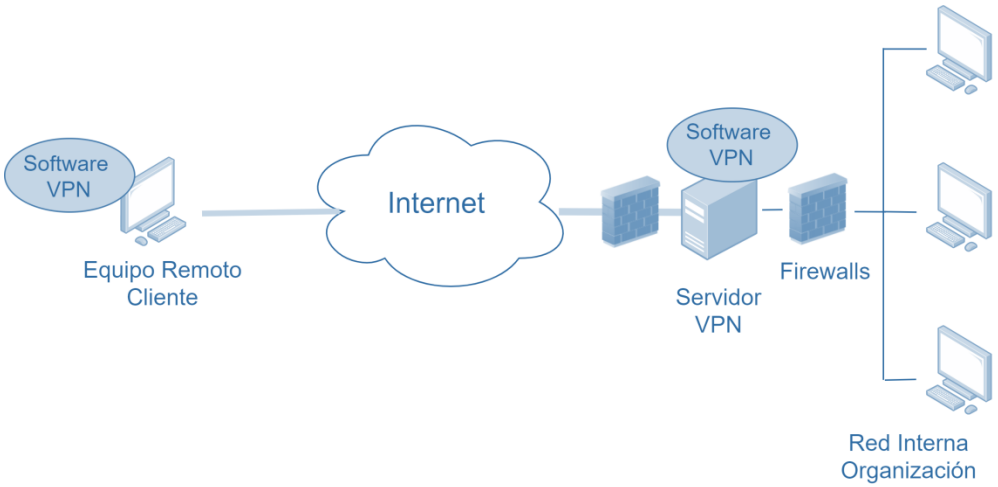


Figura 2. VPN de acceso remoto

c) **VPN de equipo a equipo**. Es la empleada para establecer conexiones seguras entre dos equipos, protegiendo el tráfico desde un extremo al otro. Normalmente se utilizan para realizar administración remota de servidores que usan protocolos inseguros, o que se encuentran en redes con riesgos de seguridad, como la DMZ.

En este escenario, las conexiones VPN se establecen entre el equipo origen (cliente) y el equipo destino (servidor). El servidor tendrá el software VPN instalado y configurado para proporcionar los servicios VPN y aceptar conexiones de los equipos cliente, que tendrán instalado y configurado el software cliente VPN. Cuando el equipo cliente solicita la conexión al equipo servidor, se realizará el proceso de autenticación y si ésta es correcta, se establecerá la conexión VPN entre ambos equipos.

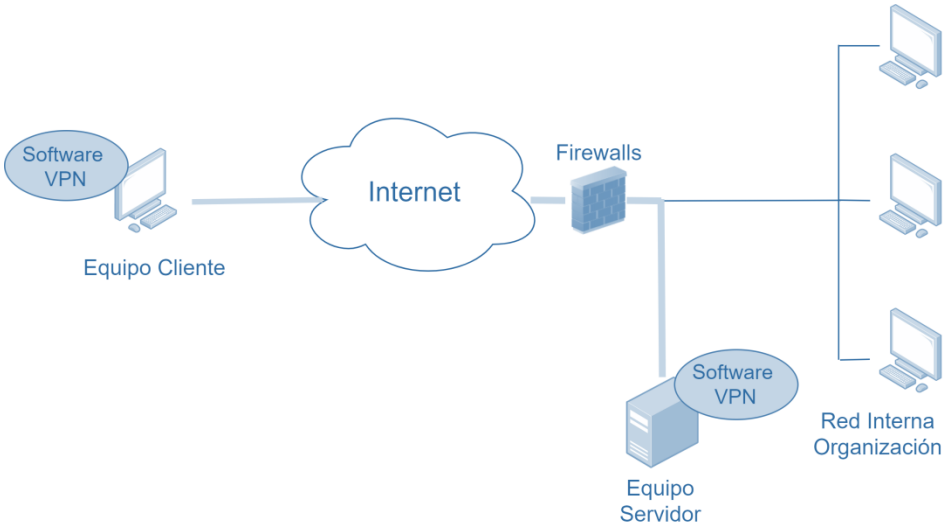


Figura 3. VPN de equipo a equipo

En este caso se protege el tráfico en todo su recorrido, desde el equipo origen, al equipo destino.

Los sistemas bajo el alcance del Esquema Nacional de Seguridad (ENS) o Sistemas Clasificados deberán utilizar productos recogidos en la familia Redes Privadas Virtuales IPsec o SSL **dentro del Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC).** Deberá tenerse en cuenta la categoría del ENS o el grado de clasificación para la cual está cualificado/aprobado el producto y seguir su Procedimiento de Empleo Seguro (PES).

4.3 VPN CLOUD

22. Las VPN Cloud vienen a solucionar el problema que se plantea cuando el usuario no solo requiere acceso a los recursos alojados en el centro de datos de la organización, sino también a otros que se encuentran fuera de la red corporativa, como es el caso de aplicaciones y recursos en la nube o cloud. Para acceder a este tipo de recursos, la arquitectura de VPN tradicional de acceso remoto no resulta eficiente.

23. Al usar la arquitectura tradicional de VPN, el tráfico del usuario hacia un servidor que es accesible desde internet, sigue un recorrido muy ineficiente: (1) la petición va del usuario al Servidor VPN de la sede, (2) de ahí sale por el cortafuegos perimetral hacia internet y la aplicación en la nube, (3) la respuesta de la nube llega al cortafuegos que la redirige al servidor VPN, y (4) el servidor al usuario.

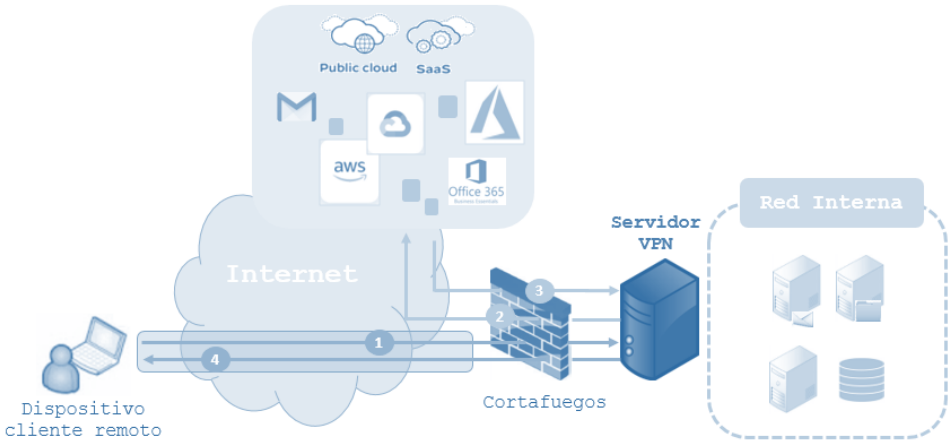


Figura 4. Acceso a servicios en la nube con una VPN de acceso remoto tradicional

24. Esta ineficiencia habitualmente hace que el usuario, tras una experiencia poco satisfactoria, no utilice la conexión VPN más que cuando tenga que conectarse a la red interna, y deje de utilizarla cuando tenga que acceder a recursos en internet. Cuando esto ocurre, la organización pierde visibilidad sobre el uso de aplicaciones y servicios por parte del usuario, además de no poder aplicar las políticas de seguridad corporativas a dicho tráfico.

25. Por ello, han surgido las soluciones de VPN en la nube (**VPN Cloud**), también llamadas *Hosted VPN* o *VPN as a Service (**VPNaaS**).* Este nuevo tipo de tecnologías están diseñadas exclusivamente para entornos cloud.

26. **VPNaaS** se utiliza, no solo para proporcionar al usuario remoto una conexión segura VPN con los servicios en la nube o recursos en Internet, sino también para establecer conexiones seguras VPN entre redes corporativas y proveedores de la nube, o conexiones *cloud to cloud*. En la actualidad, estas soluciones han evolucionado y ofrecen, también, conexión VPN a los recursos de la red interna corporativa (*on-premise*).

27. VPNaaS proporciona al usuario remoto un **punto único de acceso seguro VPN** ya sea al centro de datos, a Internet o a las aplicaciones alojadas en los entornos de la nube pública, privada e híbrida. Además, da visibilidad de todo el tráfico a la organización, permitiendo inspeccionar de forma exhaustiva el tráfico registrado en todos los puertos y protocolos.

28. Este tipo de soluciones, normalmente hacen uso de un cliente *software* instalado en el *endpoint* del usuario, que se conecta a la solución VPNaaS de manera automática en cuanto detecta que el *endpoint* tiene conexión a Internet, sin intervención del usuario. Para la conexión con los servicios y recursos del centro de datos de la organización, puede requerir de algún tipo de conector para adaptar los sistemas de la organización a la nube, dependiendo de la solución.

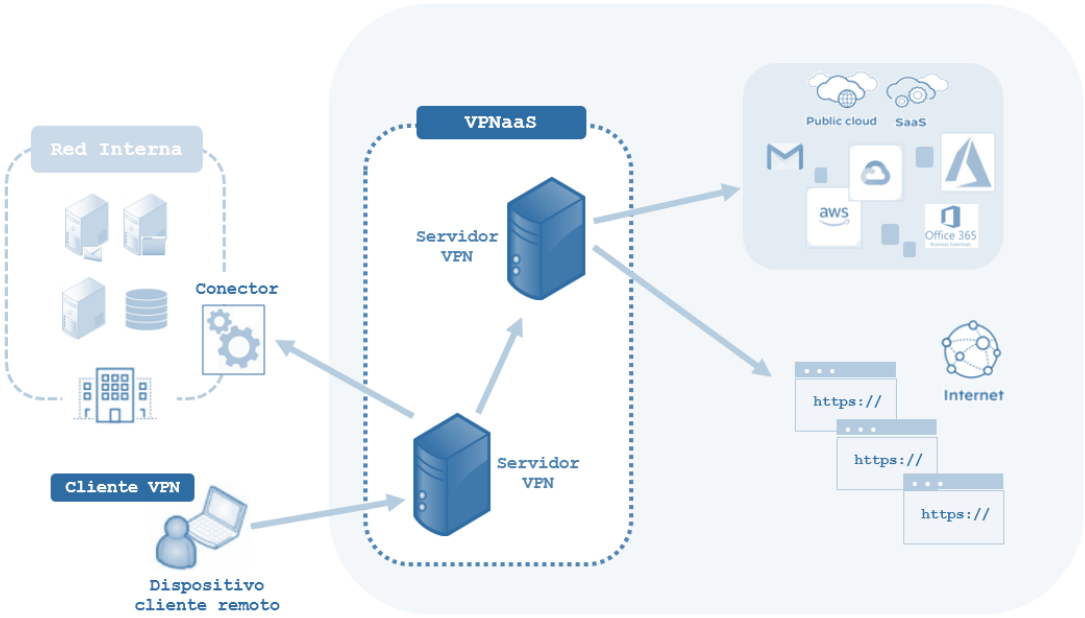


Figura 5. VPNaaS

Las VPNaaS utilizadas deberán estar incluidas en la familia Redes Privadas Virtuales IPsec o TLS **dentro del Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC).** Deberá tenerse en cuenta la categoría del ENS o el grado de clasificación para la cual está cualificado/aprobado el servicio y seguir su Procedimiento de Empleo Seguro (PES).

4.4 TECNOLOGÍAS VPN

29. Actualmente, el protocolo TCP/IP constituye la infraestructura tecnológica más extendida y desarrollada sobre la que circulan las comunicaciones electrónicas (datos, voz, multimedia…). Su expansión se ha debido principalmente al desarrollo exponencial de la red mundial, Internet.

30. TCP/IP está diseñado en una estructura de capas, fundamentada en el estándar de los protocolos de comunicaciones diseñado por la organización ISO, denominado OSI, *Open Systems Interconnection.* Cada una de las capas es responsable de llevar a cabo una tarea específica de la comunicación. Las cuatro (4) capas en las que se divide el estándar son las mostradas en la Figura 6.

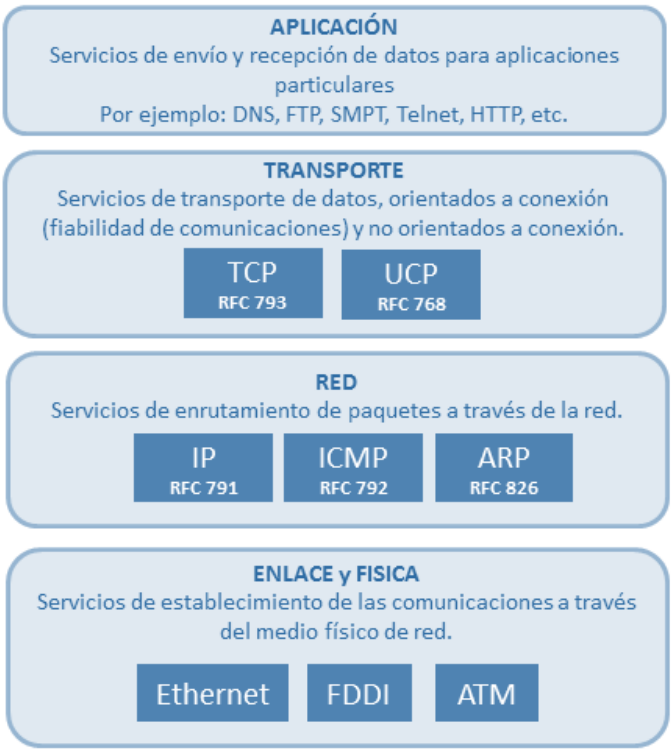


Figura 6. Niveles de la familia de protocolos TCP/IP[2]

31. Las principales vulnerabilidades de seguridad asociadas a los protocolos TCP/IP se engloban en tres (3) áreas concretas:

    a) **Confidencialidad**: Los protocolos no proporcionan mecanismos de cifrado de las cabeceras o datos, lo cual permite que una tercera entidad se sitúe en medio de la comunicación y pueda interceptar e inspeccionar los paquetes.

    b) **Autenticidad**: Al no proporcionar autenticación en las cabeceras o datos, es posible que una entidad genere paquetes simulando que provienen de otra entidad, y así suplantando a cualquier otro elemento de la red.

    c) **Integridad**: Debido a la falta de mecanismos de integridad, es posible que una entidad intercepte y modifique el tráfico intercambiado por otras entidades.

32. Las tecnologías VPN pretenden proporcionar mecanismos que imposibiliten la realización de los ataques mencionados, mediante el uso de protocolos de seguridad que proporcionen los servicios de confidencialidad, integridad y autenticidad.

33. En función de la capa o nivel en el que trabajan los protocolos de seguridad empleados por las tecnologías VPN, existirán VPN de nivel de aplicación, de nivel de transporte, de nivel de red y de nivel de enlace.

[2] **FDDI** hace referencia a Interfaz de Datos Distribuida por Fibra (en inglés*: Fiber Distributed Data Interface*). **ATM** hace referencia a Modo de Transferencia Asíncrona (en inglés: *Asyncronous Transfer Mode*).

4.4.1 VPN DE NIVEL DE APLICACIÓN

34. Las VPN de nivel de aplicación implementan mecanismos de seguridad para proteger las comunicaciones propias de cada aplicación *software* específica. Esta protección se puede conseguir mediante dos (2) vías: construir, dentro de la propia aplicación *software*, los protocolos VPN de nivel de aplicación; o hacer uso de programas externos, los cuales proporcionen los servicios de seguridad.

35. En el caso de aplicaciones comerciales, el *software* es propiedad del fabricante y no puede ser modificado. En el caso de que el *software* no proporcione la protección con el nivel de seguridad requerido por la organización, será necesario hacer uso de programas externos.

36. En el caso de que no sea factible emplear ninguna de las dos vías, deberán utilizarse VPN de capas inferiores, para proporcionar los servicios de seguridad a la comunicación.

37. **SSH** (*Secure Shell*) [2] es un protocolo de nivel de aplicación que permite acceder de manera remota a servidores y otros equipos de forma segura. Hace uso de un cliente SSH instalado en el equipo cliente. Este es por lo tanto un protocolo que puede ser usado por la aplicación *software* para establecer un túnel seguro de comunicación con el destino.

38. Las VPN basadas en túneles SSH requieren tiempo y recursos para su configuración y mantenimiento. Es necesario instalar y configurar el *software* SSH en cada cliente, así como configurar las aplicaciones *software* para utilizar el túnel SSH. Además, cada usuario deberá tener permisos para conectarse al servidor destino.

39. Este tipo de VPN cuentan con varias desventajas, ya que una configuración inadecuada puede dejar sin protección a información sensible del nivel de aplicación. Además, no provee protección para la información de capa de red (cabeceras IP).

40. Dada su complejidad y las desventajas mencionadas, normalmente las VPN basadas en túneles SSH **solo deben ser utilizadas por administradores IT** dentro de la red de la Organización.

4.4.2 VPN DE NIVEL DE TRANSPORTE

41. Las VPN de nivel de transporte implementan mecanismos de seguridad para proteger las comunicaciones de cualquier tipo de aplicación. Esto permite establecer comunicaciones seguras sin necesidad de realizar ninguna modificación en el *software* de aplicación.

42. El protocolo de seguridad más empleado por las VPN de nivel de transporte es **TLS**[3].

[3] TLS (*Transport Layer Security*), está basado en la versión 3 de SSL (*Secure Socket Layer*). La última versión de TLS es TLS 1.3 y se encuentra definida en el estándar RFC 8446 [16].

43. Este tipo de VPN se emplea normalmente en escenarios de acceso remoto, donde un cliente necesita acceder a una o varias aplicaciones basadas en Web, ubicadas en la red interna de la organización. Son, por lo tanto, arquitecturas de cliente/servidor, donde ambos deben soportar TLS. Al ser aplicaciones basadas en Web, en muchos casos el cliente puede acceder a ellas desde su navegador web, sin necesidad de instalar ningún otro *software* cliente.

44. Además, TLS permite la **autenticación mutua del cliente y del servidor**. Sin embargo, la mayoría de las implementaciones solo hacen uso de la autenticación en un único sentido: la autenticación del servidor.

45. Existen varios tipos de implementación de VPN TLS. La más extendida es la que despliega un **portal web** en el servidor VPN. Los usuarios acceden a través del navegador al portal, el cual cuenta con los enlaces de acceso a las aplicaciones internas de la organización. Otra implementación es la que proporciona una extensión de la red interna, proporcionando acceso a todos los recursos de la red interna.

46. Una función muy extendida de las VPN TLS para las aplicaciones basadas en Web es la de ***proxy***. En este caso, las conexiones HTTPS establecidas por el cliente, no son con el servidor de la aplicación destino, sino con el *proxy* (servidor VPN). Este puede realizar la autenticación y autorización del cliente, en función de los mecanismos y listas de control de acceso que tenga configurados. Tras la autenticación y autorización, el *proxy* será el que establezca la conexión con el servidor destino, o con una aplicación concreta en función de los permisos del cliente.

47. El uso de la función *proxy* es beneficioso en el caso de que la organización necesite proteger las comunicaciones para un número considerable de aplicaciones basadas en Web. Además, el uso del proxy añade una capa más de seguridad a la comunicación.

48. Para las aplicaciones no basadas en Web, es necesario que, o bien el equipo cliente tenga instalado un *software* específico, o bien hacer uso de un servidor de terminales que disponga de este *software*. Los datos de la aplicación se encapsularán en un túnel HTTPS u otro protocolo.

49. La tecnología de VPN TLS se explica con mayor detalle en el anexo ANEXO A.

4.4.3 VPN DE NIVEL DE RED

50. Las VPN de nivel de Red implementan mecanismos de seguridad en la capa de red. Dado que es en este nivel donde se añade la información IP, las VPN de nivel de red pueden proteger tanto los datos como las cabeceras IP, lo que no hacen las VPN de nivel de aplicación y de nivel de transporte. Sin embargo, solo soportan comunicaciones IP, y cuentan con problemas de compatibilidad con la tecnología NAT.

51. Las VPN de nivel de red se basan principalmente en el estándar **IPsec**, que está compuesto por un conjunto de protocolos y mecanismos de seguridad, que

trabajan de forma conjunta y admiten múltiples configuraciones, para proveer el nivel de protección requerido por la comunicación.

52. Las VPN IPsec se caracterizan por proporcionar acceso completo a la red remota, y ser complejas de configurar y administrar, debido a todas las opciones y funcionalidades ofrecidas por esta tecnología. Cuentan con dos (2) modos de funcionamiento: modo túnel y modo transporte.

53. La tecnología VPN IPsec se explica con mayor detalle en el anexo A.

54. Las VPN de nivel de Red implementan mecanismos de seguridad en la capa de red. Dado que es en este nivel donde se añade la información IP, las VPN de nivel de red pueden proteger tanto los datos como las cabeceras IP, algo que no hacen las VPN de nivel de aplicación y de nivel de transporte. Sin embargo, solo soportan comunicaciones IP. En caso de necesitar compatibilidad con tecnología NAT, se recomienda el uso de la tecnología WireGuard por encima de IPsec dado que esta última cuenta con problemas de compatibilidad con dicha tecnología.

55. Existen dos opciones principales para las VPN de nivel de red.

    a) El estándar **IPsec**, que está compuesto por un conjunto de protocolos y mecanismos de seguridad, que trabajan de forma conjunta y admiten múltiples configuraciones, para proveer el nivel de protección requerido por la comunicación.

    b) WireGuard, que está compuesto de un conjunto de protocolos y primitivas criptográficas modernas que proporcionan de un nivel de seguridad y rendimiento muy altos. Admite la configuración de VPNs de tipo sitio a sitio y de punto a sitio.

56. Las VPN IPsec se caracterizan por proporcionar acceso completo a la red remota, y ser complejas de configurar y administrar, debido a todas las opciones y funcionalidades ofrecidas por esta tecnología. Cuentan con dos (2) modos de funcionamiento: modo túnel y modo transporte.

57. La tecnología VPN IPsec se explica con mayor detalle en el ANEXO A.

58. WireGuard se caracteriza por facilitar la creación de túneles eliminando la complejidad de configuración estableciendo los protocolos de alta seguridad automáticamente. Delega la distribución de claves y direccionamiento IP a mecanismos externos.

59. La tecnología WireGuard se explica con mayor detalle en el ANEXO D.

4.4.4 VPN DE NIVEL DE ENLACE

60. Las VPN de nivel de enlace implementan mecanismos de seguridad en la capa de enlace. Al encontrarse esta capa un nivel por debajo de la capa de red, estas VPN pueden funcionar con cualquier otro protocolo de red, no solo IP.

61. Estas VPN se utilizan para proteger enlaces físicos, como pueden ser circuitos dedicados entre dos edificios, cuando existe un riesgo sobre accesos no autorizados a los componentes físicos del enlace.

62. En la actualidad, las VPN de nivel de enlace se basan en el estándar **MACsec, Media Access Control (MAC) Security,** definido en IEEE 802.1AE, que especifica un conjunto de protocolos que proporcionan medidas de seguridad para la protección de los datos en la capa de enlace (L2 OSI) de redes de área local (LAN) tipo Ethernet. La versión actual es la **IEEE 802.1AE-2018**. La tecnología MACsec se explica con mayor detalle en el anexo ANEXO C.

Dentro de las VPN de nivel de enlace, se recomienda el uso MACsec y **evitar protocolos vulnerables como PPTP, L2F o L2TP.**

4.4.5 COMPARATIVA DE VPN SEGÚN SU NIVEL DE OPERACIÓN

63. A continuación, se incluye una tabla comparativa que muestra las ventajas e inconvenientes de las distintas tecnologías de VPN y sus protocolos. Es importante indicar que estos aspectos, en la realidad varían mucho en función de las características de los diversos productos e implementaciones.

	Tecnología	Ventajas	Inconvenientes
APLICACIÓN	**En cada aplicación SW**	– Ofrece mucha granularidad para configurar la protección de las comunicaciones de las aplicaciones software.	– La protección es exclusiva para la aplicación software específica. – Normalmente no se pueden añadir a las aplicaciones comerciales, cuyo software es propiedad de los fabricantes. – Una configuración inadecuada podría dejar sin protección información sensible del nivel de aplicación. – No proporciona protección para la información de la capa de red (cabeceras IP).

	Tecnología	Ventajas	Inconvenientes
TRANSPORTE	**TLS**	– Provee mecanismos robustos de cifrado y autenticación de origen a través de protocolo TLS 1.2 y TLS 1.3. – Múltiples métodos de autenticación. – La función proxy añade una capa más de seguridad, al impedir la conexión directa entre cliente y servidor destino. – Control de acceso granular. – Compatibilidad NAT. – Capacidades de registros y auditoría. – Controles de seguridad en endpoints.	– No provee protección para la información de la capa de red (cabeceras IP). – No recomendada para aplicaciones no basadas en Web. – Las implementaciones típicas no autentican el cliente en el servidor, sólo el servidor en el cliente. – En caso de VPN tipo túnel requieren instalación de software cliente o de *plugins* en el navegador web.
RED	**IPsec**	– Protección para todo el tráfico IP independiente de la aplicación o protocolo que lo genera. – Apto para protocolos y aplicaciones obsoletas o tradicionales de cliente/servidor. – Soportado por casi todos los sistemas operativos. – Proporciona mecanismos robustos de cifrado y autenticación. – Puede usar una variedad de protocolos de autenticación.	– Sólo protege comunicaciones IP. – Requiere instalación de software cliente. – Complejo de configurar, operar y mantener. – Posibles problemas de compatibilidad con NAT. – No proporciona control de acceso granular a los recursos. – No proporciona controles de seguridad a los *endpoints* (aunque depende del software cliente del producto IPsec).
RED	**WireGuard**	– Mayor rendimiento que IPSec y VPNs basadas en TLS – Bajo consumo de recursos – Protección contra DoS y suplantación de identidad – Clientes multiplataforma – Código abierto y soporte nativo en el kernel de Linux – Fácil configuración – Permite configurar VPNs de tipo Sitio a Sitio y Punto a Sitio – Utiliza primitivas criptográficas modernas – Superficie de exposición reducida (pocas líneas de código comparado com otras soluciones)	– Solo opera en la capa 3 (OSI) – Solo gestiona el establecimiento del túnel. La gestión de direcciones IP, distribución de llaves, y otras operaciones deben ser realizadas por otros mecanismos – Nivel mínimo de logs. – Solo soporta UDP.

	Tecnología	Ventajas	Inconvenientes
ENLACE	**MACsec**	– Se puede utilizar con redes no IP. – Provee cifrado simétrico entre los *endpoint* y los *switches* o entre *switches* de una misma red local. – Establece mecanismos de verificación de integridad de datos.	– No aplicable a todos los casos de uso. – Sobrecarga adicional agregada por el encabezado MACsec lo que puede provocar una pérdida/demora inesperada de paquetes si la MTU (*Maximum Transmission Unit*) es demasiado baja. – Requiere dispositivos específicos que implementen MACsec.

Tabla 1. Comparativa de VPN según su nivel de operación

4.5 ARQUITECTURA DE VPN

64. Las decisiones a tomar en el diseño de la arquitectura de la VPN de la organización, se basan en dos (2) aspectos fundamentales:

- El modo de implementación VPN.
- La ubicación de los concentradores VPN, dentro de la infraestructura de red.

65. Las decisiones que se tomen sobre estos dos aspectos tendrán implicaciones para la organización, ya que afectarán a cuestiones como la funcionalidad, seguridad y rendimiento de su infraestructura.

4.5.1 MODO DE IMPLEMENTACIÓN

66. Para la implementación del concentrador VPN, se puede utilizar un equipo físico dedicado (*appliance*), o se puede hacer uso de otros dispositivos existentes en la infraestructura de la organización como, por ejemplo, servidores de propósito general, o equipos de comunicaciones (por ejemplo, enrutadores) en los que se añada una tarjeta para funciones criptográficas.

67. La elección del modo de implementación tiene implicaciones en los aspectos de seguridad, rendimiento, escalabilidad, operación y mantenimiento, capacidades de control y coste.

- **Seguridad**. La seguridad es el propósito principal de las VPN. El uso de un dispositivo físico dedicado se considera en general una opción más segura. Esto se debe a que la única función del dispositivo, es la de administrar las conexiones VPN. Mientras que, si el dispositivo realiza más funciones que las de VPN, la probabilidad de que existan vulnerabilidades que puedan ser explotadas por un atacante aumenta. La solución es proteger adecuadamente el dispositivo, pero es una tarea compleja y requiere de unos elevados conocimientos de seguridad.

- **Rendimiento**. La ejecución de las funciones VPN tiene un elevado consumo de recursos debido, principalmente, a las actividades de cifrado y descifrado de datos. En el caso de un dispositivo físico dedicado, este deberá dimensionarse adecuadamente. En el caso de utilizar un dispositivo existente en la red, puede producirse una carga excesiva y llegar a la situación de interrupción del servicio. También puede darse el caso de que el servicio VPN se vea afectado por picos de consumo de CPU provocados por alguna de las otras funciones del dispositivo. Una posible solución sería el uso de tarjetas criptográficas que realicen estas funciones.
- **Escalabilidad**. Se refiere a la capacidad de expandir la VPN para añadir más conexiones remotas, usuarios o equipos.

  - En el caso de los dispositivos físicos dedicados, la escalabilidad dependerá del equipo físico y sus características. En el peor de los casos, podría requerirse un nuevo equipo de mayor capacidad.
  - En el caso de utilizar otros dispositivos de la infraestructura, se podrán ampliar los recursos de estos (agregar procesadores, memoria, etc.) o trasladar la VPN a otro dispositivo con más recursos.

- **Operación y mantenimiento**. Aunque existen tareas comunes (por ejemplo, las actualizaciones de parches de seguridad), los dispositivos físicos dedicados requieren más actividades de mantenimiento. Hay que tener en cuenta que se añaden nuevos equipos a la infraestructura hardware de la organización. Además, son equipos muy específicos, que pueden incluso tener su propio sistema operativo, por lo que las tareas de operación se dificultan.
- **Capacidades de control**. En el caso de utilizar dispositivos de la infraestructura, se pierden capacidades de control relacionadas con el equipo físico o con el software de base (como el sistema operativo y otras utilidades). Por ejemplo, en caso de que sea necesario un reinicio para restaurar la operación correcta de la VPN, deberá planificarse teniendo en cuenta los requisitos de disponibilidad del resto de funciones del dispositivo. Tampoco podrán instalarse actualizaciones o componentes *software* adicionales, sin tener en cuenta cómo pueden afectar a dichas funciones.
- **Coste**. En general los dispositivos físicos dedicados son más costosos. Además del coste inicial de adquisición y despliegue de la solución, existen muchos factores que influyen en el coste final. Por ejemplo, la escalabilidad es un aspecto que tiene gran impacto en el coste, ya que, si la solución seleccionada no resulta escalable, el coste se elevará de forma muy acusada cuando la VPN supere su capacidad. Es por ello, que el coste debe calcularse a largo plazo para realizar una comparativa correcta entre las diversas opciones de implementación.

4.5.2 UBICACIÓN DE LOS CONCENTRADORES VPN

68. La situación de los concentradores VPN dentro de la arquitectura de red de la organización, es un asunto complejo, principalmente debido a la estrategia de defensa en capas que las organizaciones emplean para proteger sus redes y que, por lo tanto, requieren un conocimiento extenso y profundo de la red y de las políticas de seguridad.

69. A la hora de decidir la ubicación de los concentradores VPN, se deberán tener en cuenta varios aspectos. Entre ellos, los principales son las funcionalidades de análisis de tráfico, funcionalidades de mapeo direcciones IP y el tráfico no protegido:

- **Funcionalidades de análisis de tráfico**. Generalmente hay dispositivos dentro de la infraestructura, que realizan funciones de análisis de tráfico como parte de las medidas de seguridad de la red. Estos dispositivos, normalmente son IDS (*Intrusion Detection Systems*), IPS (*Intrusion Protection Systems*) y cortafuegos, y deben poder realizar estas funciones. Dado que el tráfico VPN es un tráfico cifrado, éste deberá ser descifrado por el concentrador VPN antes de que estos dispositivos procedan a realizar su análisis. Este es un factor que condiciona, por lo tanto, la ubicación de los concentradores VPN.

- **Funcionalidades de mapeo direcciones IP**. En caso de que sea necesario realizar NAT (*Network Address Translation*) en la red, hay que tener en cuenta que el dispositivo que lo realice modificará la dirección IP, lo cual significa modificar el paquete de datos. Si los mecanismos de integridad ya hayan sido aplicados por la VPN, esta modificación supone una ruptura de la integridad del paquete. Esta es una cuestión que, en caso de que la tecnología VPN seleccionada no tenga sus propios métodos para solucionarla, implica diseñar la arquitectura para que el NAT sea aplicado previamente a los mecanismos de integridad VPN.

- **Tráfico no protegido.** El tráfico no protegido, es aquel que discurre entre el concentrador VPN destino y el equipo destino de la comunicación, en VPN de acceso remoto. O también el que discurre entre el equipo origen y su concentrador VPN, en VPN *site to site.* Dado que este tráfico no está protegido por los mecanismos de seguridad VPN, el segmento de red por el que discurra, deberá contar con suficientes medidas de protección en caso necesario.

70. La opción recomendada para la ubicación del concentrador VPN es en una DMZ dedicada, aislado del resto de servidores de la DMZ. En esta arquitectura el concentrador VPN se encuentra protegido por el firewall y no expuesto a Internet. Por otro lado, también se controla el tráfico que va desde el concentrador hacia la red interna. Esta arquitectura se muestra en la siguiente Figura.

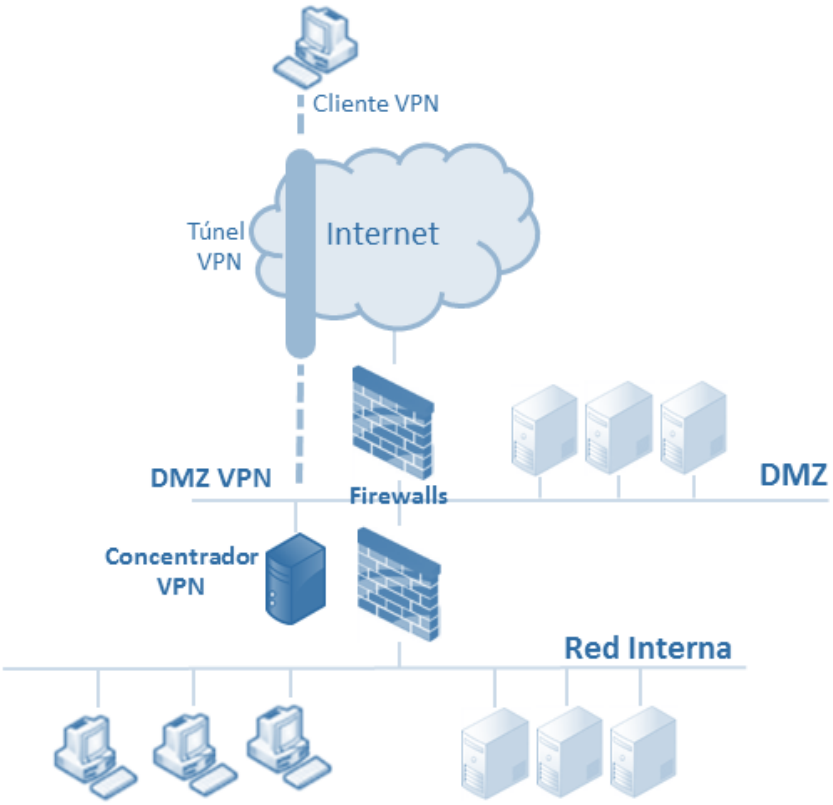


Figura 7. Arquitectura VPN en DMZ dedicada

71. Para finalizar, otro aspecto que hay que considerar en el diseño de la arquitectura de la VPN, es el de disponibilidad y redundancia. En el diseño de la VPN deben tenerse en cuenta aspectos de disponibilidad y redundancia para todos los dispositivos que formen parte de la infraestructura VPN. Fallos en algún dispositivo o tareas de mantenimiento programado no deben interrumpir el servicio. Esto es especialmente importante en los casos en los que los dispositivos funcionen en línea (*inline*), ya que la caída del equipo podría causar la interrupción del tráfico de red del segmento en el que se encuentre.

5. REQUISITOS GENERALES DEL SISTEMA VPN

72. La VPN representa una infraestructura formada por elementos *hardware* y/o so*f*tware, cuyo objetivo final es proporcionar servicios de seguridad a las comunicaciones.

73. Desde el punto de vista organizativo, es fundamental que la tecnología VPN se incluya en las políticas, procesos y procedimientos de la organización. Así, deberán formar parte de la normativa de seguridad de la organización, al menos, las siguientes políticas:

- **Política de VPN.** En ella se describirán las reglas que gobiernan el uso de la tecnología VPN en la organización. Se incluirán aspectos relativos a: datos a proteger y los mecanismos empleados para su protección; mecanismos de

autenticación y parámetros criptográficos; mecanismos de filtrado y selección de tráfico; roles y responsabilidades relativas a los componentes de la infraestructura VPN; controles de seguridad mínimos en los componentes; requisitos de las cuentas de los administradores (por ejemplo, autenticación de doble factor, cambios periódicos de contraseñas, condiciones de eliminación de cuentas, etc.); tipos de protección a aplicar entre concentradores VPN y servidores de gestión (si existen); límites al tiempo que puede estar abierta una sesión e imponer un tiempo máximo para cerrar sesiones inactivas, etc.

- **Política de uso aceptable de la VPN.** Esta política deberá incluir aspectos relacionados con el uso apropiado e inapropiado de la VPN y las medidas disciplinarias correspondientes (por ejemplo, prohibir el uso personal o el uso por parte de otros individuos). Se indicará lo que se puede hacer a través del acceso VPN, qué aplicaciones se pueden usar, qué datos son accesibles y en qué condiciones estos datos pueden almacenarse en el equipo cliente. Se incluirán los requisitos de autenticación de usuario para el acceso a VPN (por ejemplo, autenticación de doble factor, o seguridad de las contraseñas), requisitos sobre el equipo cliente (si deben ser equipos corporativos normalizados o los niveles de parcheado de sistema operativo y del antivirus), requisitos específicos de la conexión (por ejemplo, no conectarse a la VPN a la vez que a otras redes), etc.

- También deberán existir los **procedimientos** necesarios relativos a la VPN. Estos podrán integrarse en otros procedimientos similares ya existentes en la organización. Al menos existirán los siguientes procedimientos:

    - Alta, baja y modificación de elementos en la VPN (usuarios, equipos, servicios o aplicaciones, etc.). Incluyendo auditorías periódicas de la lista de usuarios autorizados, y la baja de aquellos que ya no sean necesarios.

    - Operación y mantenimiento de la infraestructura VPN. Acorde con los planes generales de operación y mantenimiento de la infraestructura hardware de la organización.

    - Planes de recuperación y *backup* de la infraestructura VPN. Acorde con los planes generales de recuperación y *backup* de la infraestructura de la organización.

    - Gestión de eventos y registros de log. Acorde con la política general de gestión de eventos de la organización. Se incluirán aspectos como la información a registrar, cuánto tiempo debe conservarse, cada cuanto tiempo debe revisarse, envío de copias de los eventos a servidores centralizados de gestión, etc.

    - Gestión y respuesta a incidentes de la VPN. Acorde con la política general de gestión de incidentes de la organización. Se analizará cómo los componentes de la infraestructura VPN pueden verse afectados por los incidentes, para documentar las actividades que den respuesta a estos incidentes de forma efectiva y eficiente.

- Auditorías periódicas de la infraestructura VPN. Acorde con la política general de auditorías de la organización. Se incluirán aspectos como la periodicidad y el tipo de auditorías a realizar sobre cada componente.

74. Se deberá también establecer un **Proceso formal de Autorización** de acceso a la VPN para nuevos usuarios, equipos o servicios.

75. Estas medidas establecen que el sistema VPN deberá ser configurado adecuadamente antes de entrar en explotación. Para ello, deben seguirse los principios de **mínima funcionalidad** y **seguridad por defecto**. Algunos aspectos a tener en cuenta son los siguientes:

- Se deshabilitarán todas las características y funciones del servidor VPN, que no sean necesarias para alcanzar los objetivos definidos en la fase de diseño, tanto características funcionales, como de operación, administración, o auditoría.
- El acceso a los componentes de la infraestructura VPN estará limitado al mínimo número de técnicos necesarios. Se deberán considerar, además, controles de seguridad adicionales. Por ejemplo, permitir acceso sólo desde unas direcciones IP específicas.
- La distribución de las cuentas de administración deberá proporcionar una adecuada segregación de funciones. Por ejemplo, diferentes cuentas para revisión de logs del sistema, y para modificación de la configuración del sistema.
- La configuración de seguridad deberá incluir un perfil especial para auditoría de uso del equipo.
- Los usuarios y equipos cliente, sólo tendrán acceso a la VPN en caso de necesidad justificada, y se requerirá del correspondiente proceso de aprobación.

76. Se deberá desarrollar y documentar un procedimiento de gestión de la configuración adecuado. Este procedimiento deberá tener en cuenta, entre otras cosas, las necesidades de aprobar y documentar los cambios en la configuración de seguridad, de realizar pruebas previas al despliegue de cualquier cambio, y las necesidades de copias de seguridad de configuraciones de seguridad previas.

77. Con respecto a las medidas de protección física:

- Los equipos se instalarán en áreas separadas específicas para su función. El acceso a dichas áreas será controlado y existirán medios que eviten el acceso por puntos diferentes al control.
- Se restringirá el acceso a las áreas, de forma que toda persona deberá estar autorizada y pasará por el control de acceso para verificar su identificación y autorización, dejando el correspondiente registro.
- Se registrará toda entrada y salida de equipamiento.

- Los locales deben estar adecuadamente acondicionados (suministro eléctrico, climatización, etc.) y protegidos frente a amenazas (incendios, cortes de suministro, inundaciones).
- En función de los requisitos de disponibilidad del sistema VPN, deberá existir un sistema VPN de respaldo en instalaciones alternativas con las mismas garantías de seguridad, para poder ser empleado en caso de que las instalaciones habituales no estén disponibles.

78. Se deberán también implantar medidas relacionadas con la concienciación y formación del personal, en concreto:

- Se deberá concienciar regularmente al personal acerca de su papel y responsabilidades en el uso de la VPN. En particular hay que refrescar regularmente al menos, la normativa relativa al uso aceptable de la VPN y los procedimientos de reporte de incidencias.
- Se deberá formar regularmente al personal acerca de las técnicas que requieran para el desempeño de sus funciones. Se impartirá la formación necesaria, por ejemplo, para poder llevar a cabo la instalación, configuración, administración, operación y mantenimiento de la VPN y para la gestión de incidentes en la VPN.

6. PROCESO DE PLANIFICACIÓN Y DESPLIEGUE DE VPN

79. La implantación de una tecnología VPN en la organización, deberá seguir un proceso ordenado de planificación y despliegue en fases. Esto permitirá que cualquier problema potencial pueda ser identificado de forma temprana en el proceso, minimizando así su impacto y consecuencias.

80. Las fases a seguir son: identificación de necesidades y requisitos; diseño de la solución VPN; selección del producto VPN; pruebas de la solución VPN; implantación y despliegue; operación y mantenimiento.

6.1 IDENTIFICACIÓN DE NECESIDADES Y REQUISITOS

81. La primera fase del proceso es la de identificar la necesidad de comunicaciones remotas, y recopilar los requisitos asociados. Se recomienda tener en cuenta futuras necesidades, es decir, deberán considerarse también las comunicaciones que serán necesarias en un futuro próximo.

82. Se identificarán y recopilarán los requisitos asociados a la comunicación. Por un lado, todos los posibles orígenes y destinos, sus particularidades y las características de las redes por las que discurra el tráfico. Por otro lado, los requisitos técnicos necesarios, como rendimiento, número de conexiones simultáneas, disponibilidad del servicio, etc.

- **Origen y destino de la comunicación**. Determinar si se requiere una conexión desde un equipo a una red completa, o sólo a unos recursos determinados. O

se trata de una conexión desde varios equipos, a un recurso concreto. O de una conexión entre dos redes.

- **Características de la red y de sus dispositivos**. Es necesario considerar las características de la red física y si se trata de segmentos cableados o inalámbricos. También se deben identificar los equipos de red participantes en la comunicación, y analizar sus características de capacidad, grado de modernidad, posibilidades de actualización, rendimiento, etc. Asimismo, otras características particulares de la red deben revisarse y tenerse en cuenta, como son el uso de NAT, direcciones IP dinámicas, filtrado de paquetes, etc.

83. También será necesario recopilar cualquier otro requisito relacionado con la infraestructura, el personal técnico y las organizaciones externas que puedan participar en la comunicación.

- **Capacidad del equipo de administradores IT.** Dado que son los administradores los que deberán desplegar la solución de conexión que se implante finalmente, y realizar su posterior operación y mantenimiento, la capacidad de este equipo debe tenerse en cuenta.
- **Infraestructura existente en la organización.** Debe analizarse si la organización dispone ya de otras soluciones de conexión, que puedan ampliarse o modificarse para las nuevas necesidades.
- **Requisitos externos a la organización.** Si en la comunicación van a intervenir participantes externos, éstos pueden disponer de infraestructura específica con la cual, la solución de conexión debe ser compatible.

6.2 DISEÑO DE LA VPN

84. Tras haber recopilado las necesidades y requisitos sobre las comunicaciones, se deberán analizar los requisitos de seguridad de la información a la que se quiere acceder, y que será transmitida. La valoración de la información la determina el responsable de la misma teniendo en cuenta su naturaleza y la normativa aplicable:

a) Se determinarán los escenarios de uso de la VPN. En el apartado 4.2, se detallan los tres (3) escenarios más frecuentes de uso de VPN: VPN de sitio a sitio, VPN de acceso remoto y VPN de equipo a equipo.

b) Se definirá **el modo de implementación**. Para ello además de tener en cuenta los factores indicados en el apartado 4., se aplicarán los requisitos del apartado 5.

c) Se diseñará la arquitectura de red y la ubicación de los concentradores VPN, teniendo en cuenta los factores indicados en el apartado 4.2. Se deberán definir también las políticas de *firewalls* adecuadas para la arquitectura definida, y cualquier otra configuración de red que aplique. Se deberá garantizar que todo el tráfico esperado se encauce a través de la VPN y no se permita el *Split tunneling*.

d) La ***suite* criptográfica** seleccionada atenderá a los requisitos establecidos en el ENS y en la normativa de Sistemas Clasificados, sobre uso de algoritmos autorizados por el CCN y las longitudes de clave mínimas (ver guía CCN-STIC-807). La suite criptográfica estará formada por:

   - Algoritmos de Confidencialidad (cifrado).
   - Algoritmos de Integridad y Autenticidad.
   - Algoritmos de Acuerdo de clave.

e) Se diseñarán los **Mecanismos de Autenticación** atendiendo a los requisitos establecidos.

f) Se diseñarán los **controles de seguridad a aplicar en los equipos remotos (*endpoints*)**, en caso de que se vayan a realizar controles sobre estos equipos, y de qué forma se llevarán a cabo dichos controles. Es decir, cómo se realizará el chequeo del equipo (a través de *software* cliente VPN, o a través de descarga de controles de contenido activos), y qué se chequeará del equipo (por ejemplo, parcheado de seguridad del sistema operativo, estado de actualización del antivirus, etc.).

g) Se diseñarán las **reglas de control de acceso**. Se determinará a qué recursos particulares pueden acceder los usuarios, en función de características como su identificación, tipo de equipo desde el que se realiza el acceso, tipo de recurso al que se accede, grupo al que pertenece el usuario, etc.

h) Se definirá la **configuración del sistema VPN**, teniendo en cuenta las características y parámetros específicos de la tecnología seleccionada, y siguiendo los principios de mínima funcionalidad y seguridad por defecto especificados en las medidas de seguridad del ENS y de la normativa de Sistemas Clasificados.

i) Se definirán el resto de medidas de seguridad que puedan ser de aplicación al sistema VPN diseñado, teniendo en cuenta los requisitos generales del ENS o de la normativa de Sistemas Clasificados que sean de aplicación (ver apartado 5). Por ejemplo, las medidas de protección de la infraestructura del sistema VPN (acondicionamiento del local, control de acceso a las áreas de equipamiento, acondicionamiento y protección del local, etc.), o la estrategia de alta disponibilidad (tipo de respaldo de los equipos VPN, modo de funcionamiento y tipo de replicación entre los equipos).

j) Se diseñarán las **políticas, la normativa y los procedimientos de seguridad** relativos a la VPN acordes con el resto de las Políticas y procedimientos de la organización (ver apartado 5.).

k) Se diseñarán los **planes de formación y concienciación** para el personal relacionado con el sistema VPN: responsables, usuarios, técnicos, etc.

6.3 SELECCIÓN DEL PRODUCTO VPN

85. Una vez diseñada la solución VPN, se deberá seleccionar el producto VPN más apropiado. Como ya se indicó anteriormente, dicho producto deberá estar incluido en el listado de Productos Cualificados del CPSTIC si el sistema se encuentra bajo el alcance del ENS o en el listado de Productos Aprobados si el sistema va a manejar información clasificada. En ambos casos deberá tenerse en cuenta la categoría del ENS/nivel de clasificación para el cual el producto está cualificado/aprobado.

86. De esta forma, deberán seguirse los siguientes criterios:

    a) Sistema clasificado: se seleccionarán productos aprobados para un nivel de clasificación mayor o igual que el del sistema.

    b) Sistema bajo el alcance del ENS: deberán utilizarse productos cualificados para una categoría mayor o igual que el nivel de seguridad requerido para las dimensiones de confidencialidad, integridad y autenticidad.

6.4 PRUEBAS DE LA SOLUCIÓN VPN

87. Antes de la puesta en producción de la solución VPN, ésta deberá probarse en un entorno de pruebas apropiado. El objetivo es detectar posibles problemas, malfuncionamiento o brechas de seguridad, que puedan ser resueltas antes de que la solución sea desplegada en el entorno de producción.

88. El entorno de pruebas deberá ser representativo del entorno de producción, dentro de lo posible. En algunos casos, esto sólo podrá conseguirse utilizando el propio entorno de producción y desplegando la solución en una parte acotada y controlada de éste. En estos casos se deberán tomar las precauciones necesarias, como realizar las pruebas en un tramo horario que minimice el impacto de algún fallo en las comunicaciones. También deberán realizarse copias de seguridad antes de realizar ningún cambio, para poder restaurar el entorno al estado anterior en caso necesario.

89. Para llevar a cabo las pruebas de forma correcta, se emplearán todas las herramientas de pruebas adecuadas para cada objetivo: herramientas de monitorización de servidores, de análisis de tráfico, análisis de logs, etc.

90. Deberá elaborarse un plan de pruebas adecuado, que permita verificar al menos los siguientes aspectos.

    a) **Interoperabilidad de componentes**. Todos los componentes de la solución VPN deberán funcionar juntos de forma correcta. Este aspecto será particularmente importante cuando los componentes provengan de fabricantes distintos.

    b) **Conectividad**. Las conexiones entre el origen y el destino, se deben establecer correctamente a través de la VPN.

    c) **Configuración de Seguridad**. La solución VPN debe cumplir los requisitos de seguridad especificados. Esto significa comprobar que los mecanismos de

protección establecidos, realizan su función correctamente para cada tipo de tráfico. En concreto, es importante verificar que los mecanismos de autenticación son robustos, ya que el fallo de autenticación deja inoperativa la VPN.

d) **Rendimiento**. La solución VPN debe cumplir los requisitos especificados sobre disponibilidad y rendimiento. En condiciones de tráfico normal y en condiciones pico. Deberá verificarse el rendimiento de todos los componentes en la comunicación y comprobar que no se generan cuellos de botella.

e) **Compatibilidad**. La solución VPN tendrá que ser compatible con el hardware y software de los dispositivos donde se vaya a instalar.

f) Es recomendable también realizar la **búsqueda y análisis de vulnerabilidades** de la solución VPN y de todos sus componentes, para detectar posibles vulnerabilidades que supongan brechas de seguridad de la solución.

91. Una vez finalicen las pruebas, los errores, incidencias y vulnerabilidades detectadas deberán ser registrados y reportados para su corrección. Las pruebas deberán repetirse las veces necesarias, hasta verificar que los errores reportados han sido corregidos adecuadamente.

6.5 IMPLANTACIÓN Y DESPLIEGUE

92. Una vez que se hayan completado las pruebas, y que todos los errores y problemas detectados hayan sido resueltos, se procederá a la implantación y despliegue de la solución VPN en la organización.

93. Es prudente utilizar una estrategia de despliegue gradual. La infraestructura de red, aplicaciones y usuarios deben ser introducidos poco a poco en la nueva solución VPN. De esa forma, los administradores pueden evaluar el impacto de la implantación y resolver problemas antes de que el despliegue sea completo en la organización.

94. En esta fase se realizarán al menos, las siguientes actividades:

a) Instalación y configuración de los componentes VPN (*hardware* y *software*).

Se llevará a cabo la instalación de los componentes y el despliegue de la configuración de seguridad definida en la fase de diseño. Se configurarán los parámetros generales (direcciones IP, nombres de equipo, etc.) y los parámetros específicos de seguridad de la solución VPN, entre ellos la suite criptográfica definida.

Será necesario tener precaución con los valores por defecto de los parámetros de configuración. Debe revisarse cuidadosamente cada uno de ellos para verificar que el valor de cada parámetro es el correcto. También debe verificarse que, en ninguna circunstancia, el sistema vuelva a la configuración por defecto.

- Configuración y despliegue de los mecanismos de autenticación definidos en la fase de diseño.

- Configuración y despliegue de los controles de seguridad en los *endpoints*.
- Configuración y despliegue de la política de control de acceso.
- Implantación y despliegue de otras medidas de seguridad determinadas en la fase de diseño de la solución.

b) Documentar las políticas y procedimientos de seguridad de la VPN.

Durante la implantación y despliegue, será recomendable estar alerta a cualquier disminución del rendimiento de la red, ya que puede significar problemas causados por la implantación. Son problemas característicos de una implantación VPN, que algunos dispositivos o servicios puedan ver su funcionamiento afectado negativamente por el nuevo tráfico cifrado (IDS, cortafuegos, etc.). O que otros dispositivos puedan estar bloqueando el tráfico cifrado, porque no hayan sido configurados adecuadamente.

6.6 OPERACIÓN Y MANTENIMIENTO

95. Finalmente, una vez que la solución VPN se encuentre implantada, se inicia la fase de operación y mantenimiento. Esta fase se mantendrá indefinidamente, hasta que cambios significativos deban ser introducidos en la VPN, en cuyo caso deberá iniciarse de nuevo el proceso de planificación y despliegue.

96. Las actividades de operación y mantenimiento harán uso de los procedimientos definidos y documentados relativos a la VPN. Algunas de las actividades a desarrollar en esta fase son las siguientes:

- Operación diaria, que abarca tareas como añadir nuevas conexiones, nuevos equipos cliente y usuarios, etc.
- Monitorización de la disponibilidad y rendimiento de la infraestructura VPN. El objetivo es detectar problemas de rendimiento en los dispositivos de la infraestructura, para aumentar su capacidad en caso necesario y evitar así, fallos en las comunicaciones provocados por el desbordamiento de alguno de sus componentes.
- Gestión de incidencias. Cualquier incidencia que se detecte en el funcionamiento de la VPN, será reportada, analizada y corregida.
- Realización de pruebas periódicas sobre la infraestructura VPN para verificar que los requisitos de seguridad se siguen cumpliendo de forma eficiente y efectiva.
- Actualización y gestión de parches.
- Gestión de la configuración.
- Adaptación de los mecanismos de la VPN por cambios en la política de seguridad de la organización.

7. ASPECTOS CRIPTOLÓGICOS

97. Al margen de las consideraciones genéricas establecidas en los apartados anteriores, es necesario tener en cuenta las siguientes:

Todas las VPN que se establezcan en sistemas bajo el alcance del ENS deberán configurarse de tal forma que **solamente hagan uso de los algoritmos autorizados para el ENS.** Estos algoritmos están descritos en la CCN-STIC-807 [3]. Además, también deberán utilizarse los mecanismos y protocolos descritos en la citada guía.

Todos los productos con capacidad de establecer VPN que vayan a ser utilizados en sistemas clasificados deberán haber pasado una **evaluación criptológica** en la que se comprobará la fortaleza y correcta implementación los mecanismos y algoritmos utilizados, de acuerdo a lo establecido de la CCN-STIC-130 [19].

8. EJEMPLO DE PROCESO DE PLANIFICACIÓN Y DESPLIEGUE DE UNA VPN

98. A continuación, se describe un ejemplo de un proceso de planificación y despliegue de una VPN para una organización.

99. El supuesto consiste en que se requiere proporcionar un acceso seguro a los recursos internos de la organización, para múltiples usuarios desde localizaciones remotas. No todos los usuarios deberán poder acceder a los mismos recursos, dependerá del grupo al que pertenezcan. El acceso a día de hoy, se necesita para los equipos corporativos de los usuarios (portátiles), pero a medio plazo deberá poder realizarse desde ordenadores públicos (como hoteles o locutorios de internet).

100. El sistema está bajo el alcance del Esquema Nacional de Seguridad y se ha determinado que es de categoría ALTA, dado que el nivel asociado a su dimensión de Confidencialiad [C] es ALTO.

8.1 IDENTIFICACIÓN DE NECESIDADES Y REQUISITOS.

101. Los usuarios del departamento financiero de la organización, son los únicos que tendrán acceso a los recursos del departamento financiero y no tendrán acceso a otros recursos.

102. Del resto de usuarios de la organización, un número elevado de ellos deberá tener acceso a todos los recursos de la red interna (menos a los del departamento financiero).

103. Los accesos desde equipos no corporativos, sólo estarán permitidos si estos disponen de un sistema operativo permitido, con un nivel de parches de seguridad determinado, y si el antivirus está actualizado y en ejecución.

104. Los accesos desde equipos no corporativos sólo se permitirán al correo electrónico, al servicio de calendario y al directorio corporativo de empleados.

105. Se requiere que las conexiones tengan suficiente capacidad (múltiples conexiones simultáneas), rendimiento (*throughput*) y disponibilidad (deberán estar disponibles las 24 horas).

106. La infraestructura de la organización no tiene capacidad para absorber nuevos servicios.

107. Los recursos de la red interna incluidos los del departamento financiero, no están basados en Web en su mayor parte. Tan sólo están basadas en Web las aplicaciones estándar, como correo electrónico, servicios de calendario y directorios corporativos.

108. El número de recursos IT destinados al soporte y mantenimiento de la infraestructura *hardware* y *software* de la organización es limitado y no tienen capacidad para absorber muchas más tareas.

8.2 DISEÑO DE LA VPN

109. La organización evalúa el nivel de seguridad requerido en las dimensiones de seguridad de la información y de los servicios a los que se accederá a través de la VPN.

110. Se definen los siguientes aspectos del diseño de la VPN:

a) Escenario de conexión. Se trata de una VPN de acceso remoto, ya que cada usuario individual se encontrará en una ubicación distinta desde la que debe conectarse a la red interna de la organización, a través de Internet.

b) Tecnología. Para este escenario, la organización evalúa las tecnologías VPN existentes. Decide que la más apropiada es la VPN TLS, ya que:

- No requiere despliegue de software cliente. Esto, por un lado, evita el consumo de recursos IT para *su* instalación y mantenimiento. Por otro lado, permite el acceso desde equipos no corporativos (públicos) en los que no se puede instalar ningún *software* cliente.
- Permite una elevada granularidad en el control de acceso a los recursos (por usuario, por grupo, por tipo de recurso, etc.).
- No requiere modificar las aplicaciones para las que se necesita el acceso remoto, que son bastante variadas.

La VPN TLS será tipo Túnel para los accesos a la totalidad de los recursos de la organización, y para los accesos a los recursos del departamento financiero (que no están basados en Web). Será tipo Portal para el acceso restringido desde los equipos no corporativos, a los servicios de correo electrónico, calendario y directorio de empleados, que son servicios basados en Web.

El protocolo seleccionado será TLS 1.2/1.3.

c) Modo de implementación. Los requisitos de capacidad, rendimiento y disponibilidad son elevados, y dado que la infraestructura actual de la organización no tiene capacidad suficiente, se decide que los concentradores VPN serán dispositivos físicos dedicados (*appliances*).

d) Arquitectura. Los concentradores VPN se situarán en la DMZ. Se colocará un firewall con capacidades de IDS (*Intrusion Detection System*) entre los concentradores VPN y la red interna, para proporcionar protección no sólo en el *front-end*, sino también en el *back-end*.

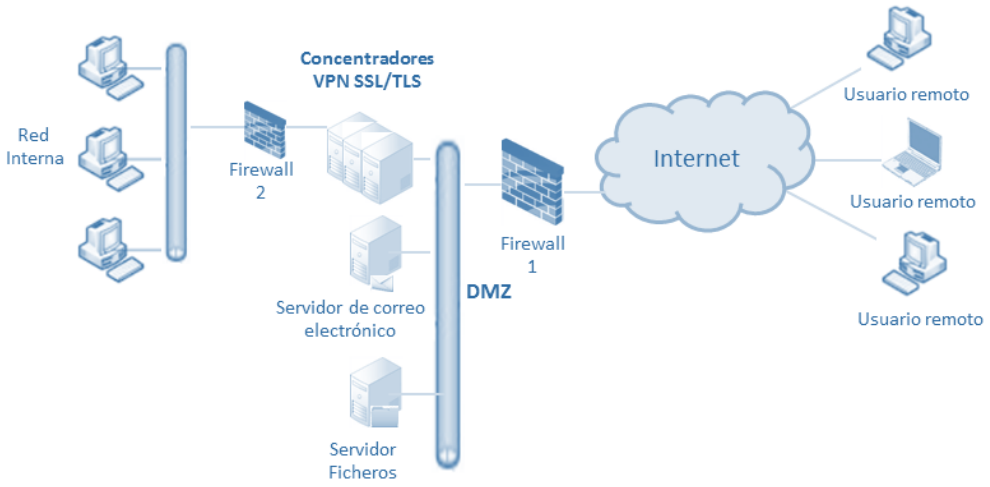


Figura 8. Arquitectura de la VPN TLS diseñada para la organización.

e) *Suite* Criptográfica. Se emplearán algoritmos y fortalezas de clave autorizadas, según determina la guía CCN-STIC-807 [3]. La suite criptográfica seleccionada podría ser, por ejemplo, la siguiente:

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384, donde ECDHE se utiliza para acuerdo de claves, AES-256 en modo GMC para cifrado, y HMAC-SHA384 para autenticación de origen.

f) Mecanismos de Autenticación. La autenticación de cada usuario será por doble factor: contraseña con nivel de resistencia medio y dispositivo físico (*token*). La autenticación del servidor VPN se realizará instalando un certificado emitido por una Entidad de certificación (CA) de confianza de la organización.

g) Se creara una política de control de acceso. Se agruparán los recursos de la red en, por ejemplo, los 3 grupos:

- Recursos_G: Todos los recursos de la organización menos los del departamento financiero.
- Recursos_F: Recursos del departamento financiero.
- Recursos_NC: Recursos a los que podrán acceder los equipos no corporativos.

Se agruparán los usuarios de la siguiente forma:

- Usuarios_G: Usuarios que pueden acceder a todos los recursos de la organización (Recursos_G), menos a los del departamento financiero (Recursos_F).
- Usuarios_F: Usuarios que solo pueden acceder a los recursos financieros (Recursos_F).

Se agruparán los dos (2) tipos de acceso que se puede realizar:

- Desde equipos corporativos: a todos los recursos, en función del grupo al que pertenezca el usuario.
- Desde equipos no corporativos: sólo a un grupo reducido de recursos (Recursos_NC) y siempre que cumplan las condiciones establecidas para el equipo.

Se elabora la tabla de control de acceso:

Usuarios	Tipos de Acceso	Recursos	Tipo de VPN TLS
Usuarios_G	Corporativo	Recursos_G	Túnel
Usuarios_F	Corporativo	Recursos_F	Túnel
Usuarios_G	No corporativo	Recursos_NC	Portal

Tabla 2. Comparativa de VPN según Nivel de operación.

h) Política de seguridad de los equipos remotos (*endpoints*). Antes de que el usuario pueda conectarse, la VPN realizará un chequeo del equipo. Para ello se efectuará la descarga y ejecución en el equipo, de controles de contenido activos. A través de estos controles o *applets*, se verificarán las claves de registro para identificar si el equipo es o no corporativo.

En caso de que el equipo no sea corporativo, se chequeará si la versión de sistema operativo está dentro de las permitidas, si dispone de los parches de seguridad determinados, y el estado de actualización y ejecución del antivirus.

i) Se diseñará la configuración de seguridad de los equipos VPN. Esta atenderá a los principios de mínima funcionalidad y de seguridad por defecto y tendrá en cuenta los aspectos indicados en el apartado 5. Por ejemplo, el acceso administrativo a los concentradores VPN sólo se podrá realizar desde unas direcciones IP determinadas.

j) Diseño del portal VPN para acceso a los Recursos_NC. Se definirá una personalización para el portal VPN (gráficos con el logo de la organización, sólo se desplegarán las opciones para las que el usuario tenga autorización de acceso, etc.).

k) Se definirán las Políticas y Procedimientos relativos a la VPN, consistentes con los de la organización. Algunos de ellos:

- *Backup* de los ficheros de configuración una vez a la semana.
- Monitorización de los concentradores VPN integrada en el sistema de monitorización general de la infraestructura.
- Modificación de la política de los equipos corporativos para permitir la descarga y ejecución de los controles de contenido activos para permitir la comprobación de equipos.
- Estrategia de alta disponibilidad basada en varios concentradores VPN en modo balanceo de carga. Configuración en espejo en los

dispositivos, de forma que cambios en la configuración de uno de ellos, sea automáticamente replicada en los demás.

l) Se definirán los planes de formación y concienciación a los usuarios generales, usuarios del departamento y técnicos del departamento IT, sobre el uso y responsabilidades en el nuevo sistema VPN.

m) Se instalarán los concentradores VPN en el CPD (Centro de Proceso de Datos) de la organización.

8.3 SELECCIÓN DEL PRODUCTO VPN

111. La organización llevará a cabo un proceso de selección y adquisición del producto VPN más apropiado, capaz de proporcionar todos requisitos y características definidos en el Diseño.

112. Dado que el sistema en el que se va a desplegar la VPN está bajo el alcance de ENS y su categoría es ALTA (nivel ALTO en la dimensión de Confidencialidad [C]), el producto seleccionado debe ser un producto cualificado para categoría ALTA. Para ello, se debe consultar el Catálogo de Productos y Servicios de Seguridad TIC (CPSTIC) en su publicación en modalidad guía (CCN-STIC-105) o en su modalidad web.

8.4 PRUEBAS DE LA SOLUCIÓN VPN

113. Se realizarán pruebas en un entorno de laboratorio, que será una réplica reducida del entorno de producción. Deberá disponer de *firewalls* y servidores con la misma configuración que los de producción. Se elaborará y ejecutará el plan de pruebas para evaluar todas las características definidas en el diseño (conectividad, control de acceso, autenticación, seguridad de los equipos remotos, etc.). Se realizarán pruebas con una muestra representativa de equipos clientes y se cubrirán todos los escenarios posibles (conexión desde equipos corporativos o públicos con distintas configuraciones, y para diversos tipos de usuarios).

8.5 IMPLANTACIÓN Y DESPLIEGUE

114. Se realizarán un despliegue en fases, utilizando un proyecto piloto, que pueda contribuir a la experiencia de usuario y ayudar a resolver cualquier problema con la conectividad o la funcionalidad. Una vez se dé la conformidad al piloto, se realizará el despliegue gradual en toda la organización.

ANEXO A. VPN TLS

115. Las VPN SSL/TLS[4] surgieron para simplificar la complejidad de otras soluciones VPN, como IPSec, y proporcionar un acceso remoto y seguro a ciertas aplicaciones existentes dentro de una organización, sobre todo aplicaciones basadas en Web, o que pueden ser accedidas a través de un interfaz Web.

116. El uso de SSL 3.0 (SSLv3) no está recomendado, tal y como se indica en la RFC 7568 - *Deprecating Secure Sockets Layer Version 3.0,* de 2015 [4]. Esta RFC considera SSLv3 como un protocolo inseguro dada la larga serie de ataques que ha sufrido, tanto a sus mecanismos de acuerdo de claves, como a los de cifrado.

117. SSLv3 fue reemplazado por TLS 1.0, 1.1, 1.2 y, finalmente, la última versión actual TLS 1.3. **TLS 1.3** representa un cambio significativo y tiene por objetivo abordar las amenazas que han surgido a lo largo del tiempo desde la especificación de TLS 1.2. **A día de hoy, TLS 1.3 es la versión de TLS considerada más segura**. Sin embargo, no es compatible con versiones anteriores, por lo que el uso de TLS 1.3 puede requerir un tiempo de adaptación para los sistemas y aplicaciones

> Deberán utilizarse versiones del protocolo **TLS 1.2 o superior**. Siempre que sea posible, se recomienda utilizar TLS 1.3.

118. Las principales características proporcionadas por el uso del protocolo TLS son las siguientes:

    a) Protección de la **confidencialidad** mediante el uso de algoritmos de cifrado simétrico. Las claves para este cifrado se generan a partir de un secreto pre-compartido (*pre_master_secret*) que se establece entre cliente y servidor en las primeras fases del protocolo, utilizando métodos de intercambio de claves (*Key Exchange*).

    b) Protección de la **integridad y autenticidad de origen** mediante el uso de funciones HMAC (*Hash-based Message Authentication Code*).

    c) **Autenticación** mediante el uso de certificados de clave pública X.509 [1].

    d) **Protección anti-reenvíos**, mediante números de secuencia añadidos al mensaje.

    e) ***Perfect Forward Secrecy*** (secreto hacia adelante), asegurando que, si la clave se descubre en un momento dado, no podrá ser usada para descifrar ninguno de los datos trasmitidos anteriormente.

    f) **Control** sobre lo ocurrido en la sesión a través de un sistema de alertas avanzado, que notificará al usuario inmediatamente en el caso de que algún error o incidencia ocurra.

[4] Aunque el protocolo empleado para la VPN sea TLS, estas se siguen conociendo como VPN SSL.

A.1 MODOS DE FUNCIONAMIENTO

119. Una **VPN TLS**[5] proporciona un canal de acceso seguro a los recursos de una organización. Está formada por varios *Gateways* o Servidores VPN a los que los usuarios se conectan, a través de navegadores web (*Web browsers*), o a través de un *software* específico instalado en el equipo del usuario (cliente VPN). Todo el tráfico entre el navegador o cliente, y el servidor VPN, estará protegido y cifrado a través del protocolo TLS.

120. Las ventajas de las VPN basadas en TLS es que permiten más fácilmente el envío de tráfico a través de *firewalls*, *proxies* y dispositivos NAT. Adicionalmente, algunos tipos de VPN SSL no requieren de un cliente VPN, sino que emplean el navegador web para acceder a las aplicaciones corporativas.

121. Se contemplan dos (2) casos de uso:

    a) **VPN TLS Portal.** El usuario remoto se conecta mediante una conexión TLS a un "Portal Web". A partir de este Portal se accede de forma segura a un conjunto limitado de aplicaciones y servicios de la red interna de la organización, para los que el usuario tenga autorización. El acceso a este portal se realiza a través del navegador web del equipo.

    Este portal normalmente realiza funciones de *proxy.* Esto indica que no se establece la conexión directa entre el cliente y las aplicaciones internas. Es el proxy quien establece ambas conexiones, por un lado, con el cliente (recibe las peticiones de información) y por otro lado con las aplicaciones, solicitando la información y enviándosela posteriormente al cliente.

    Las aplicaciones y servicios accesibles desde el portal, deben ser *Web-based* o poder ser accedidos mediante interfaz Web. En otro caso, será necesario que el proxy TLS disponga de funciones de "traducción de protocolo" y ser capaz de convertir información de un protocolo a otro.

    b) **VPN TLS Túnel.** Permite a un usuario remoto acceder a todos los recursos de la red interna de la organización, incluyendo aquellos que no estén basados en Web. En este caso es necesario instalar un cliente VPN en el equipo del usuario. Este proporciona un túnel de capa 3 a través del cual, los usuarios pueden acceder a la red interna de la organización.

    Este tipo de VPN normalmente permite dividir el tráfico (s*plit tunneling*), de forma que sólo el tráfico especificado y que necesite ser protegido, circulará a través de la VPN. El resto del tráfico no será redirigido a la VPN.

122. Las VPN TLS proporcionan diversas funcionalidades y servicios de seguridad. Estos elementos pueden variar en función de las características de cada producto VPN. A continuación, se indican los más comunes.

5

Característica	Definición
Autenticación	Cada producto VPN TLS puede soportar varios métodos de autenticación, desde método integrados hasta el uso de servidores externos de autenticación. La autenticación del cliente puede utilizar métodos basados en contraseñas, tarjetas inteligentes o *tokens*. Uno de los más extendidos es el uso de certificados digitales x.509 [1].
Control de Acceso	Las funciones de control de acceso son uno de los objetivos principales de las VPN TLS. Se hace uso de diversas políticas de control de acceso para proporcionar el acceso a los servicios, en función de múltiples parámetros.
Confidencialidad e Integridad	Servicios proporcionados por los protocolos TLS mediante técnicas de cifrado.
Controles de seguridad de los equipos remotos (*endpoints*)	Los productos VPN TLS pueden proporcionar capacidades para verificar el cumplimiento de las políticas de seguridad de la organización, por parte de los equipos remotos
Operación y Gestión	Los productos VPN TLS disponen de funcionalidades para facilitar la operación y gestión de la infraestructura VPN. Por ejemplo: eventos, *logs*, informes…
Alta disponibilidad y escalabilidad	Dichos productos pueden proporcionar mecanismos de protección frente a fallos de componentes de la VPN, de forma que el servicio no se vea interrumpido. Esto puede ser proporcionado a través de métodos de balanceo de carga.

Tabla 3. Características de las VPN TLS

A.2 FUNCIONAMIENTO DE TLS: *HANDSHAKE & RECORD PROTOCOLS*

123. TLS se compone de cuatro (4) protocolos. Los dos principales son el protocolo **Handshake** y el protocolo **Record**. Los otros dos protocolos son: *Change Cipher Spec y Alert*. *ChangeCipherSpec* realmente solo está compuesto de un mensaje, y se utiliza para indicar el cambio en la estrategia de cifrado, tal y como se indica más adelante. El protocolo *Alert*, envía mensajes de alerta que contienen la severidad (Warning o Fatal) y una descripción de la alerta. Los mensajes con severidad Fatal producen una finalización inmediata de la conexión TLS. Se pueden consultar los mensajes de alerta disponibles en TLS 1.2 en la sección 7.2 de la RFC 5246 [5].

A.2.1 *HANDSHAKE PROTOCOL*

124. Toda conexión TLS comienza con un *Handshake*, una negociación entre cliente y servidor en la que se establecen los detalles de cómo se va a realizar la comunicación.

125. Entre el cliente y el servidor durante el *Handshake* se realiza, principalmente, lo siguiente:

    a) Negociar y acordar los **algoritmos criptográficos** (*cipher suite* y algoritmos de firma), e intercambiar valores aleatorios (random).

    b) Intercambiar parámetros entre cliente y servidor, necesarios para obtener el secreto pre-compartido (**pre_master_secret**).

    c) Intercambiar **certificados** para permitir que cliente y servidor se autentiquen mutuamente.

    d) Generar el ***master_secret*** a partir del secreto pre-compartido (*pre_master_secret*) y de los valores *random* intercambiados. A partir del *master_secret*, posteriormente se derivará el material de claves.

    e) Proporcionar al *Record Protocol*, los parámetros de seguridad

126. Un *TLS Handshake* implica diversos pasos. Los pasos exactos varían dependiendo del método de Key Exchange usado, y de las *cipher suites* seleccionadas por cliente y servidor.

127. Lo primero que se realiza es el establecimiento de conexión por parte del protocolo de transporte, en este caso TCP. Una vez que se ha establecido la comunicación, comienza el *TLS Handshake*. A continuación, se indican los pasos que se realizan en el *handshake*.

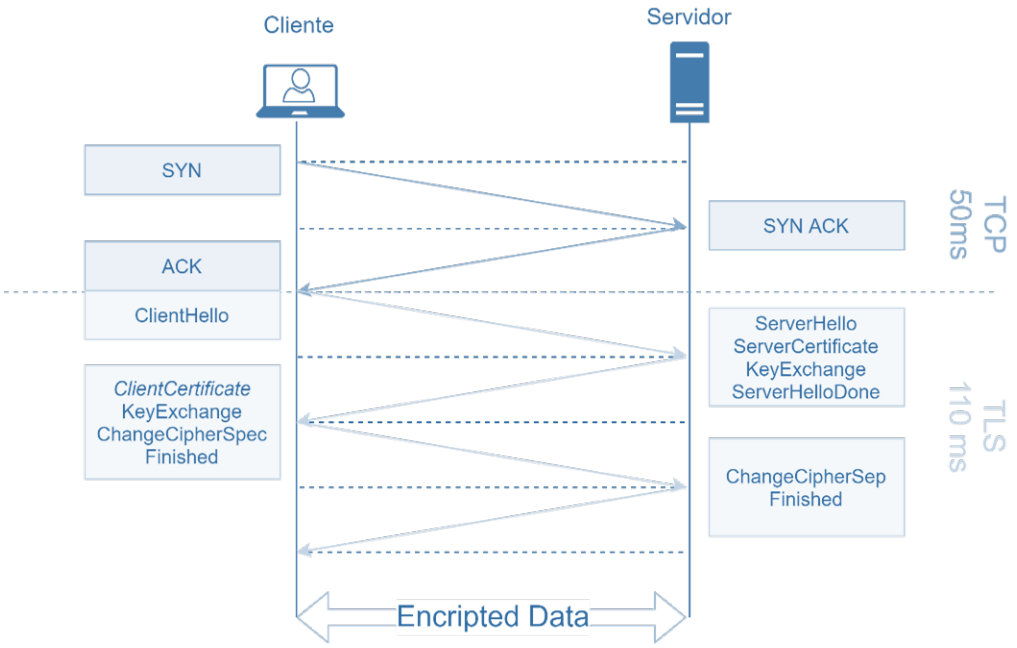


Figura 9. *TLS Handshake Protocol*

128. Tras el establecimiento de la conexión, el cliente le envía al servidor el mensaje *ClientHello* con una lista con las suites criptográficas (*cipher suites*) que ofrece, y más parámetros (versión TLS, valores aleatorios, etc.). El servidor selecciona de entre todas las suites criptográficas, la que acepta y la envía en el mensaje *ServerHello*. Aunque las suites criptográficas más robustas sean enviadas en

primer lugar, no tienen por qué ser las que acepte el servidor, aunque sean compatibles con las suyas. Si no tienen suites criptográficas en común, la conexión se aborta.

129. Para que el cliente realice la autenticación del servidor, este le envía su certificado a través del mensaje *ServerCertificate*. En ciertos casos[6], el servidor envía también el mensaje *Server KeyExchange*, con información para que el cliente pueda establecer el secreto pre-compartido (*pre_master_secret*).

130. En caso de que se requiera una autenticación mutua, el servidor enviará una petición de certificado al cliente, *CertificateRequest*, y este ha de enviar su certificado para su autenticación por parte del servidor. El envío se realiza mediante el uso del mensaje *ClientCertificate*.

131. Finalmente, el cliente envía al servidor los parámetros necesarios para crear el secreto pre-compartido, mediante el mensaje *Client KeyExchange*[7].

132. Una vez se cierra la negociación de los parámetros de seguridad de la conexión, se envía el mensaje *ChangeCipherSpec*. Este mensaje informará al otro participante de que deben empezar a utilizarse los parámetros de seguridad acordados durante la negociación y cambiar a un entorno cifrado. Todos los mensajes que siguen, llevarán protección a través de las operaciones criptográficas realizadas con los algoritmos y claves de la suite criptográfica negociada y acordada.

133. Se finaliza el intercambio con un mensaje *Finished*, el cual indica el fin del TLS Handshake, y el inicio de una conexión cifrada con los parámetros establecidos.

134. El proceso de negociación es **completamente seguro** y está protegido de cualquier escucha o alteración por parte de un atacante. Esto se garantiza a través de los mensajes *Finished* que se envían tras el mensaje de *ChangeCipherSpec*, y que proveen protección de integridad a todos los mensajes intercambiados en la negociación.

135. En **TLS 1.3** se rediseña el *Handshake* de manera significativa, para ser más consistente y eficiente:

    a) Se eliminan mensajes superfluos como el *ChangeCipherSpec*.

    b) Todos los mensajes posteriores al *ServerHello* van **cifrados**.

    c) **No se usa compresión**, poniendo a cero la lista de algoritmos de compresión.

    d) Se añade la **negociación de la versión de TLS**, ya que el cliente envía una lista de las versiones soportadas en la extensión *supported_versions*, a partir de la cual, el servidor selecciona la versión TLS que prefiera.

[6] Esto ocurre cuando el método de *Key Exchange* seleccionado en la suite criptográfica es DH (*Diffie-Hellman*) o ECDH (*Elliptic Curve Diffie-Hellman*). En estos casos, el cliente necesita los parámetros *Diffie-Hellman* que debe enviar el servidor, para generar el secreto compartido.

[7] En caso de que el método de *Key Exchange* seleccionado sea DH o ECDH, serán los parámetros *Diffie-Hellman*. En caso de que el método sea RSA será el secreto cifrado con la clave pública RSA del servidor.

e) TLS 1.3 implementa un mecanismo de **protección frente a ataques *downgrade*** para detectar si el servidor está seleccionando una versión inferior a TLS 1.3, o si, por el contrario, se trata de un ataque *downgrade*.

f) Se añade un **modo "*zero rount-trip" time (0-RTT)*** que permite enviar algunos datos de aplicación tempranos (*early data*) durante la primera ronda, agilizando así el Handshake.

A.2.2 RECORD PROTOCOL

136. *TLS Record Protocol* es el encargado de recoger los mensajes a enviar, y transmitirlos de forma segura. Para ello, utiliza los parámetros de seguridad (*Security Parameters*) proporcionados por el *Handshake*, y deriva el material de claves que necesita para la transmisión.

137. Estos parámetros de seguridad son los siguientes:

a) Algoritmos para el cifrado y HMAC negociados y acordados en los mensajes *Hello* del Handshake.

b) Método de compresión negociado y acordado en los mensajes *Hello* del *Handshake*.

c) Valores *random* intercambiados en los mensajes *Hello* del Handshake (*client.random*, *server.random*).

d) Master_secret derivado del Handkshake.

138. Para la derivación de material de claves, *Record Protocol* necesita cuatro (4) claves:

a) 2 claves que usará el cliente TLS en el envío de datos al servidor: una clave de cifrado (*client_write_key*) y otra clave para el cálculo del valor MAC (*client_write_MAC_key*).

b) 2 claves que usará el servidor TLS en el envío de datos al cliente: una clave de cifrado (*server_write_key)* y otra clave para el cálculo del valor MAC (*server_write_MAC_key*).

139. El tamaño de cada clave depende de los algoritmos negociados. Por ejemplo, si la cipher suite es TLS_DHE_RSA_WITH_AES_128_CBC_SHA256, significa que las claves de cifrado deben ser de 128 bits (16 bytes) y las claves MAC deben ser 256 bits (32 bytes).

140. Un típico flujo para el envío de datos mediante *Record Protocol* es el siguiente:

a) El *Record Protocol* recibe el mensaje de la capa de aplicación a ser transmitido.

b) El mensaje es dividido en bloques (*payload*), de máximo 2^{14} bytes, o 16 KB.

c) Cada bloque se comprime usando el método de compresión negociado en el Handshake.

d) Se calcula y se añade el MAC a cada paquete. Se hace uso de la función *hash* negociada en el *Handshake* y la clave MAC derivada.

e) Se cifran los datos de cada paquete mediante el algoritmo de cifrado negociado en el *Handshake* y la clave de cifrado derivada.

f) Una vez se han completado estos pasos, la información cifrada se pasa a la capa de transporte TCP. En el caso contrario, se realizan los pasos a la inversa.

141. A continuación, se muestra la estructura de un paquete del protocolo *TLS Record*.

Byte	+0	+1	+2	+3
0	Content type			
1..4	Version		Lenght	
5..n	Payload			
n..m	MAC			
m..p	Padding (Solo cuando se usa cifrado por bloques)			

Figura 10. Estructura Paquete TLS Record

A.3 *CIPHER SUITES* Y OTROS PARÁMETROS CRIPTOGRÁFICOS

A.3.1 TLS 1.2

142. En la fase de Negociación de TLS (*Handshake*), se acuerdan los parámetros de seguridad de la conexión. Entre ellos, lo que se denomina la suite criptográfica o **cipher suite**. Esta *cipher suite* está compuesta por los algoritmos y funciones criptográficas, junto con sus parámetros (longitud de clave, modo de operación, etc.) que se van a utilizar para proteger la conexión.

143. De forma general, una *cipher suite* se representa de la siguiente manera:

TLS_KeyExchange_Auth_WITH_Cipher_KeyLength_Mode_HashFunction

144. La primera parte corresponde a los métodos de intercambio de clave (*KeyExchange*) y autenticación (*Auth*). La parte intermedia corresponde al algoritmo de cifrado (*Cipher*), su longitud de clave (*KeyLength*) y su modo de operación (*Mode*). La última parte es la función hash (*HashFunction*) que se utilizará para el cálculo del HMAC durante el envío de mensajes, y para la derivación del material de claves en la función PRF.

A.3.1.1 KEY EXCHANGE

145. TLS 1.2 utiliza varios métodos de *Key Exchange*. Principalmente: claves pre-compartidas (PSK), algoritmos de clave pública (RSA) y métodos *Diffie-Hellman* (DH o ECDH).

No se recomienda el uso de claves pre-compartidas (PSK), por dos (2) motivos principales: cualquier parte que sepa la PSK podría autenticarse correctamente, y, además, estas claves son vulnerables a ataques de diccionario.

146. Para los métodos *Key Exchange*, se deben usar aquellos que proporcionen FS (***Forward Secrecy***). Esta característica, impide que se descifre el contenido de la comunicación anterior si se compromete la clave actual de la sesión. Los algoritmos DH o ECDH estáticos, y RSA como método de Key Exchange no proporcionan FS.

147. Los únicos métodos Key Exchange que proporcionan FS son DHE y ECDHE, es decir, DH y ECDH Ephemeral.

Se recomienda el uso de los métodos de ***Key Exchange DHE* o *ECDHE***, ya que proporcionan ***Forward Secrecy* (FS).**

Se recomienda que la implementación de TLS 1.2 soporte el uso de **curvas elípticas (EC)**.

148. En el caso de **DHE**, el uso de los Grupos *Diffie-Hellman* en TLS se describe en la RFC 7919 [6]. Esta RFC añade una modificación en la que se define una lista de los grupos DH seleccionados para su uso en TLS. Además, se tiene la extensión *Supported_Groups* en la que el cliente envía los grupos DH soportados. Esto permite que el servidor pueda escoger un grupo soportado tanto por el cliente como por el servidor.

Grupo	Longitud (bits) de los parámetros (p)	Fortaleza (bits)	Uso permitido
ffdhe2048	2048	103	No permitido
ffdhe3072	3072	125	Hasta 2022
ffdhe4096	4096	150	Posterior a 2025
ffdhe6144	6144	175	Posterior a 2025
ffdhe8192	8192	192	Posterior a 2025

Tabla 4. Grupos DH y fortaleza (RFC 7919 Apéndice A)

Se recomienda que la implementación de TLS 1.2 soporte el uso de la extensión ***Supported_Groups*.**
Además, no se debe usar el grupo **ffdhe2048**, ya que proporciona una fortaleza inferior a 128 bits.

8.5.1.1 AUTENTICACIÓN Y FIRMA

149. Con respecto a la autenticación y firma, no se recomienda el uso de suites que no proporcionan autenticación (por ejemplo, *TLS_DHE_**anon**_WITH*), y tampoco se recomienda el uso de claves pre-compartidas (PSK), por los motivos previamente indicados.

150. El algoritmo de clave pública indicado en la *cipher suite*, determina el tipo de clave pública del certificado del servidor, y para qué se utilizará esta clave.

151. Se hace uso de la extensión ***signature_algorithms*** en el mensaje *ClientHello,* para indicar los algoritmos de firma soportados. Si no envía esta extensión, el servidor seleccionará el algoritmo de clave pública de la *cipher suite* y, por defecto, la función hash SHA-1.

Se recomienda utilizar **autenticación a través de certificados de clave pública X.509v3 del tipo RSA o ECDSA.**

En TLS 1.2, se recomienda el uso de la extensión ***signature_algorithms*** para indicar los algoritmos de firma soportados. En ella deberán incluirse, además del algoritmo de clave pública (RSA o ECDSA), funciones *hash* iguales o superiores a **SHA-256.**

152. Respecto a la longitud de la clave pública RSA y ECDSA, a continuación, se resumen los diferentes tamaños de claves según el nivel de seguridad que proporcionan.

Fortaleza (bits)	Longitud de Clave RSA	Longitud de Clave ECC
80	1024	160
112	2048	224
128	3072	256
192	7680	384
256	15360	512

Tabla 5. Comparación de Niveles de Seguridad y Longitudes de Claves

No se deben utilizar claves con una **fortaleza inferior a 128 bits.** Esto supone utilizar claves RSA de, al menos, 3072 bits, y claves ECC de, al menos, 256 bits.

8.5.1.2 CIFRADO

153. En TLS, la parte central de la *cipher suite* negociada indica el algoritmo de cifrado simétrico (*Cipher*), su longitud de clave (*KeyLength*) y su modo de operación (*Mode*).

154. Aunque algunas suites de TLS 1.2 hace uso de TDEA (3DES), **se recomienda el uso de AES**, al haberse demostrado que es un algoritmo mucho más robusto y eficiente. Con respecto al modo de operación de AES, TLS 1.2 soporta los modos CBC, GCM y CCM.

155. AES en modo *Cipher Block Chaining (AES_CBC)* es el modo más tradicional donde, antes de ser cifrado, a cada bloque de texto se le aplica una operación XOR con el bloque previo ya cifrado. Además, para hacer cada mensaje único se debe usar un vector de inicialización en el primer bloque.

156. AES en modo Galois Counter (AES-GCM) y AES en modo Counter y CBC MAC (AES-CCM) son nuevos modos de operación **AEAD** (*Authenticated Encryption with*

Additional Data)[8] que se introducen en TLS 1.2. Este tipo de algoritmos proporcionan, además de la confidencialidad, también autenticidad de origen e integridad sin necesidad de hacer uso de algoritmos adicionales.

En TLS 1.2, se recomienda el uso del algoritmo de **cifrado AES en los modos AEAD**, como son AES_GCM y AES_CCM.

8.5.1.3 *CIPHER SUITES* RECOMENDADAS

Las *cipher suites* recomendadas en TLS1.2 son*:*

- *TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_ECDSA_WITH_AES_128_CCM*
- *TLS_ECDHE_ECDSA_WITH_AES_256_CCM*
- *TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256*
- *TLS_ECDHE_RSA _WITH_AES_128_GCM_SHA256*
- *TLS_ECDHE_RSA _WITH_AES_256_GCM_SHA384*
- *TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256*

Otras cipher suites permitidas son:

- *TLS_DHE_RSA_WITH_AES_128_GCM_SHA256*
- *TLS_DHE_RSA_WITH_AES_256_GCM_SHA384*
- *TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256*

8.5.1.4 INTEGRIDAD Y AUTENTICIDAD DE MENSAJES

157. En TLS 1.2, la parte final de la *cipher suite* negociada indica la función *hash* (*HashFunction*) que se utilizará para:

    a) El cálculo de los valores MAC que *Record Protocol* añadirá a los paquetes enviados entre el cliente y servidor TLS, para verificar la integridad y autenticidad de origen.

    b) La función PRF (*pseudorandom function*) que se usará para generar el material de clave.

158. Un código de autenticación de mensaje o MAC (*Message Authentication Code*), es un cálculo del *checksum* de un mensaje, utilizando para ello una función segura y una Secret Key. Cuando dicha función es una función hash, se denomina HMAC (*Keyed-Hash Message Authentication Code*). Un MAC proporciona al mensaje: **integridad**, ya que una variación en el mensaje producirá un MAC distinto y **autenticidad de origen**, ya que solo el origen auténtico dispondrá de la clave correcta.

[8] Existen varias RFCs que definen el uso de estos algoritmos en TLS 1.2: RFC 5288 (*AES Galois Counter Mode (GCM) Cipher Suites for TLS*) [13], RFC 6655 (*AES-CCM Cipher Suites for TLS*) [14], RFC 7251 - *AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS*) [15].

159. En TLS 1.2 se soportan las siguientes funciones para la integridad y autenticidad de mensajes: *hmac_md5, hmac_sha1, hmac_sha256, hmac_sha384* y *hmac_sha512.*

160. Es importante notar que MD5 y SHA1 se consideran funciones hash inseguras y sujetas a colisiones[9]. La guía CCN-STIC-807 no permite el uso de MD5 y únicamente admite el uso de SHA1 de forma temporal cuando se emplea en HMAC.

> En TLS 1.2, se recomienda el uso de *cipher suites* con funciones hash de la familia **SHA-2 o superior**. Solo se permite el uso de **SHA-1** con HMAC. No se debe usar MD5.

A.3.2 TLS 1.3

161. TLS 1.3 introduce varios cambios relacionados con la criptografía:

    a) Se eliminan los algoritmos simétricos considerados obsoletos y únicamente se utilizan algoritmos **AEAD** (*Authenticated Encryption with Associated Data*).

    b) Se elimina el uso de la función *hash SHA-1.*

    c) Se elimina el uso de los métodos de *Key Exchange* estáticos como RSA y DH o ECDH. Todos los mecanismos de *Key Exchange* empleados proporcionarán ***Forward Secrecy***. Además, no se recomienda el uso del grupo ***ffdhe2048***, ya que proporciona una fortaleza inferior a 128 bits.

    d) Con respecto a los **algoritmos de clave pública** para firma, se elimina el uso de DSA y se utiliza la implementación de RSA *Probabilistic Signature Scheme* (RSASSA-PSS).

    e) Los algoritmos de curva elíptica (EC) pasan a formar parte de la especificación base de TLS 1.3. Se añaden también nuevos algoritmos de curva elíptica para firma como EdDSA (*Edwards-Curve Digital Signature Algorithm*), definido en la RFC 8032.

    f) Se rediseña el cálculo del material de claves, pasando a utilizar primitivas **HKDF** (*HMAC-based Extract-and-Expand Key Derivation Functions*).

162. Por otro lado, en TLS 1.3, el concepto de *cipher s*uite cambia. Se separan los mecanismos de *Key Exchange* y autenticación, del algoritmo de protección AEAD y la función *Hash*.

163. Las **cipher suites** se siguen negociando en el *Handshake* (mensajes *ClientHello*, *ServerHello*) y tienen el siguiente formato: **TLS_AEAD_HASH**, donde:

    a) AEAD es el algoritmo AEAD usado para el cifrado y la integridad.

    b) HASH es la función *hash* usada para la derivación de claves mediante la función HKDF.

[9] Una colisión se produce cuando distintos mensajes producen el mismo valor hash.

En TLS 1.3, se recomienda hacer uso de las siguientes *cipher suites:*

- *TLS_AES_128_GCM_SHA256*
- *TLS_AES_256_GCM_SHA384*
- *TLS_CHACHA20_POLY1305_SHA256*
- *TLS_AES_128_CCM_SHA256*
- *TLS_AES_128_CCM_8_SHA256*

ANEXO B. IPSEC

165. IPsec[10] es un estándar abierto para comunicaciones VPN que opera a nivel de capa de red, proporciona seguridad a la comunicación y es transparente para el nivel de capa de aplicación. Típicamente es utilizado en las configuraciones VPN de acceso remoto y *site-to-site*.

166. Los principales componentes de IPsec son:

    a) Los protocolos de seguridad **AH**[11] (*Authentication Header*) y **ESP**[12] (*Encapsulating Security Payload*). AH provee protección de integridad y autenticación de origen, junto con protección anti-reenvío de manera opcional. ESP ofrece los mismos servicios junto con confidencialidad.

    b) Protocolo **IKE**[13] (*Internet Key Exchange*). Se utiliza para la autenticación mutua de origen y destino; definición de los parámetros de seguridad de la conexión (*Asociaciones de Seguridad,* SA); intercambio de claves de sesión; y para gestionar, actualizar y finalizar el canal de comunicación. La versión actual del protocolo es la IKEv2.

    c) Protocolo **IPComp** [7] para la compresión de los datos antes de su cifrado.

167. Las VPN IPsec proporcionan diversas funcionalidades y servicios de seguridad. Estos elementos pueden variar en función de las características de cada producto VPN. En la siguiente tabla se indican los más comunes.

Característica	Definición
Autenticación	Los productos VPN IPsec disponen de diferentes métodos de autenticación. Se puede realizar a través de claves pre-compartidas o a través de certificados. Siempre que sea posible, **se recomienda hacer uso de certificados para la autenticación**.
Confidencialidad e Integridad	La confidencialidad es proporcionada por el protocolo IPsec mediante técnicas de cifrado. La integridad es proporcionada gracias a los servicios de IPsec de autenticación de datos (HMAC).
Protección anti-reenvíos	El protocolo IPsec proporciona mecanismos de protección frente a ataques de reenvío. Esto lo consigue mediante la asignación de un número de secuencia único a cada paquete, para detectar paquetes duplicados.

[10] Definido en la RFC 4301 - *Security Architecture for the Internet Protocol* [12]
[11] Definido en la RFC 4302 – *IP Authentication Header (AHv3)* [8]
[12] Definido en la RFC 4303 – *IP Encapsulating Security Payload (ESPv3)* [9]
[13] Definido en la RFC 7296 – *Internet Key Exchange Protocol Version 2 (IKEv2)* [10]

Característica	Definición
Transparencia	El protocolo IPsec trabaja por debajo de la capa de transporte, por lo que es transparente a los usuarios y a las aplicaciones. Esto permite que no se necesite realizar ningún cambio al software cuando se implemente en el router o firewall.
Perfect Forward Secrecy	Los productos VPN IPsec cuentan con la capacidad PFS, que aumenta la seguridad en las comunicaciones. Esto lo realiza creando una clave única para cada negociación.

Tabla 6. Características de las VPN IPsec.

B.1 MODOS DE FUNCIONAMIENTO

168. IPsec cuenta con dos (2) modos de funcionamiento: modo túnel y modo transporte.

B.1.1 MODO TRANSPORTE

169. El modo transporte se utiliza, típicamente, en escenarios de VPN de equipo a equipo, en los que no intervienen elementos intermediarios (servidores VPN), y los dos equipos pueden intercambiar tráfico IPsec de forma nativa.

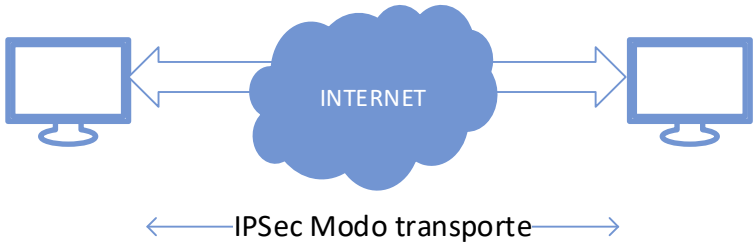


Figura 11. IPsec modo transporte

170. Para la construcción del paquete IPsec en modo transporte, se añade una cabecera IPsec al paquete IP, pero sigue manteniéndose la cabecera original, por lo que no se oculta dicha información.

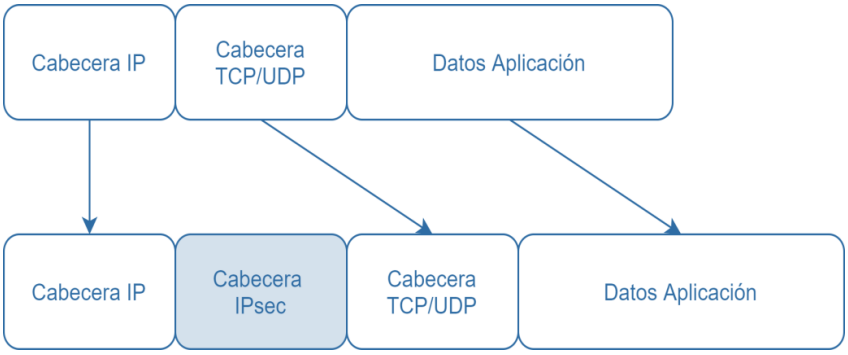


Figura 12. Construcción del paquete IPsec en modo transporte.

B.1.2 MODO TÚNEL

171. El modo túnel se utiliza, típicamente, en los escenarios de VPN *site-to-site*, cuando la conexión se establece entre los dos servidores VPN. En este caso, la protección es transparente a los equipos finales, y depende de los dispositivos de red enrutar los paquetes de estos equipos hacia los servidores VPN para procesarlos a través del túnel.

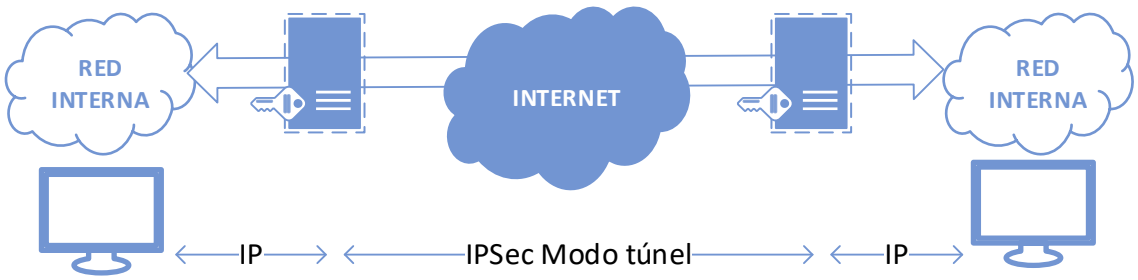


Figura 13. IPsec modo túnel

172. En el modo túnel, todo el paquete IP original se convierte en *payload* de un nuevo paquete IP de mayor longitud. En este caso se añade una nueva cabecera IP, lo que permite ocultar la información de red de ambas entidades y proteger la totalidad del paquete original.

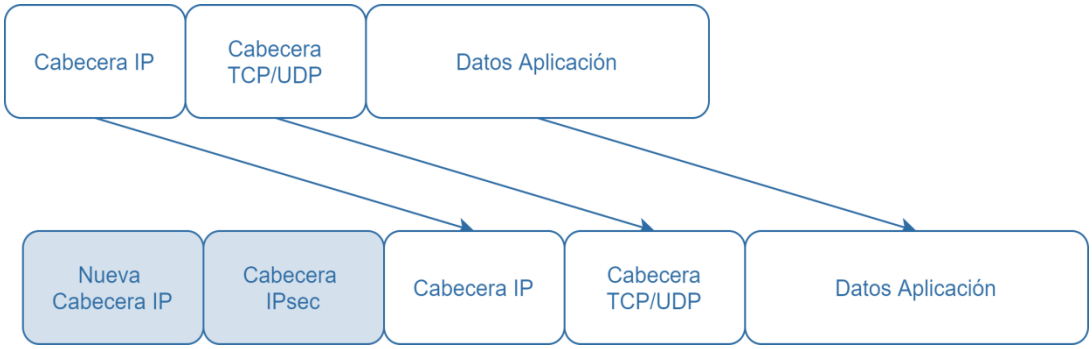


Figura 14. Construcción del paquete IPsec en modo túnel.

El **modo túnel** ofrece una mayor seguridad que el modo transporte. Por ello, **siempre que sea posible, se trabajará con esta configuración**. La elección del modo transporte solo está justificada en el caso de que el tamaño del paquete sea un problema debido a las restricciones impuestas por la red.

173. Una implementación de equipo Final (*End Point*) debe soportar ambos modos, mientras que una implementación de Pasarela (Servidor o *Gateway*) debe implementar el modo túnel, y podrá implementar el modo transporte de manera opcional. El uso de este último (transporte) solo se justifica en el caso de que actúe como *End Point* o provea seguridad entre nodos intermedios de un sistema.

B.2 ASOCIACIONES DE SEGURIDAD (SA)

174. Se denomina Asociación de Seguridad (*Security Association*, **SA**) al conjunto de parámetros de seguridad que se utilizarán en la conexión IPsec. Cada SA contiene los detalles de la conexión, el modo de funcionamiento (túnel o transporte), el protocolo empleado (AH, ESP o ambos), información de los algoritmos criptográficos empleados y un índice (SPI, *Security Parameter Index*) que identifica la conexión de forma unívoca. Cada conexión tiene dos SA asociadas, una en cada sentido, ya que los parámetros de la conexión de A hacia B, pueden ser diferentes a los de la conexión de B hacia A.

175. Un extremo IPsec puede tener múltiples SA con el mismo o distintos extremos, cada una de ellas con distinto SPI. Típicamente se emplean políticas de seguridad diferentes en base a la IP destino.

176. Las conexiones IPsec podrán soportar la gestión de SA y claves criptográficas de manera manual y automática. Las técnicas manuales son prácticas en entornos pequeños, en los que existe un único administrador de seguridad, y en entornos estáticos. En los casos restantes suelen presentar problemas de escalabilidad.

> Salvo en casos muy específicos, de entornos pequeños con un único administrador de seguridad, **no se debe realizar una gestión manual de las SA y del material criptográfico.** Esta gestión deberá realizarse mediante el uso de IKE.

B.3 PROTOCOLOS AH Y ESP

177. Los servicios de seguridad que provee IPsec, están basados en dos (2) protocolos diferentes, que son el núcleo de la tecnología IPsec.

    a) AH: *Authentication Header*, estandarizado en la RFC 4302 [8].

    b) ESP: *Encapsulating Security Payload*, estandarizado en la RFC 4303 [9].

178. Ambos se utilizan independientemente, o uno u otro, y en raras ocasiones se utilizan ambos a la vez.

B.3.1 PROTOCOLO AH

179. **AH** es un protocolo de seguridad de IPsec y provee los servicios de autenticación e integridad, protección anti-reenvíos y contra ataques de *spoofing*. No cifra el contenido del paquete y, por lo tanto, no aporta confidencialidad.

180. La **integridad** y **autenticación** de AH se proporcionan a través de algoritmos *hash* basados en claves compartidas. Un ejemplo de estos algoritmos es HMAC_SHA2. Se calcula un valor MAC (*Message Authentication Code)* sobre el mensaje, que implica una función hash criptográfica en combinación con una clave criptográfica secreta compartida por emisor y receptor (lo que proporciona autenticación).

181. Estos mecanismos de integridad y autenticación se aplican a todo el paquete, incluidos los campos cambiantes (aquellos que cambian al pasar entre los

diferentes enrutadores a medida que el paquete se transporta a su destino), como las direcciones IP, por lo que este protocolo suele presentar problemas de funcionamiento en entornos donde se utilice NAT (*Network Address Translation*).

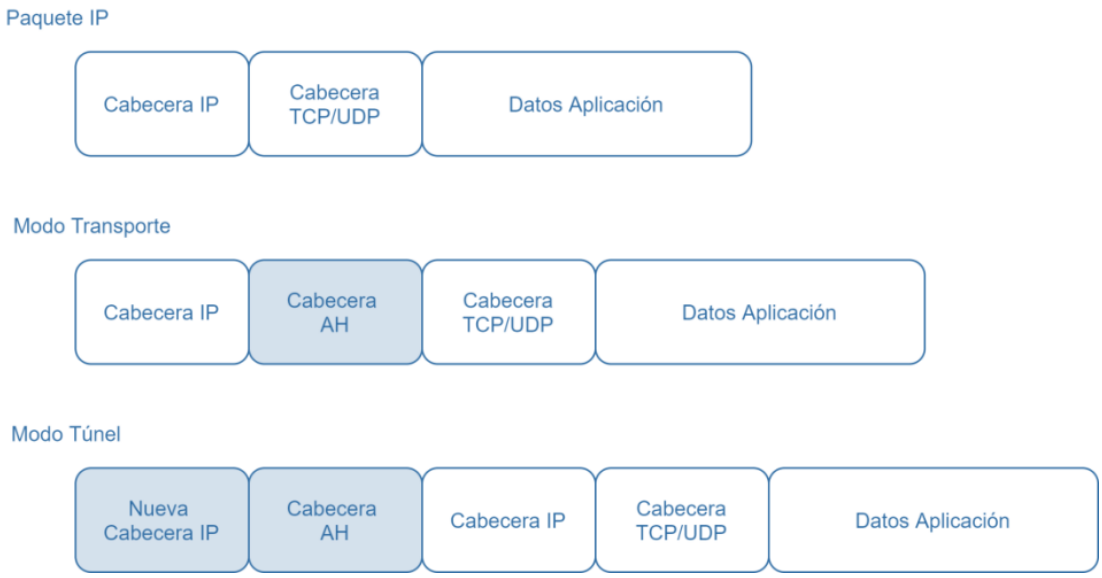


Figura 15. Construcción del paquete AH

AH es un protocolo opcional cuyo uso **no se recomienda**. En el caso de que no sea necesaria la protección de la confidencialidad se recomienda utilizar ESP con la opción de no cifrado.

B.3.2 PROTOCOLO ESP

182. **ESP** es otro de los protocolos de seguridad de IPsec y provee los servicios de confidencialidad (cifrado), autenticación e integridad y protección anti-reenvíos. Su uso junto con IKE proporciona seguridad extremo a extremo y no repudio. Inicialmente fue diseñado para proporcionar únicamente confidencialidad, ya que AH no cuenta con dicha capacidad. Las versiones actuales de ESP ya proveen integridad y autenticación.

Se recomienda el uso de ESP frente a AH. Este protocolo se puede configurar sin cifrado y sin control de la integridad, pero no es recomendable.

183. A diferencia de AH, en ESP solamente está autenticado el *payload*, por lo que cuando se trabaja en modo transporte no se autentica la cabecera IP del paquete.

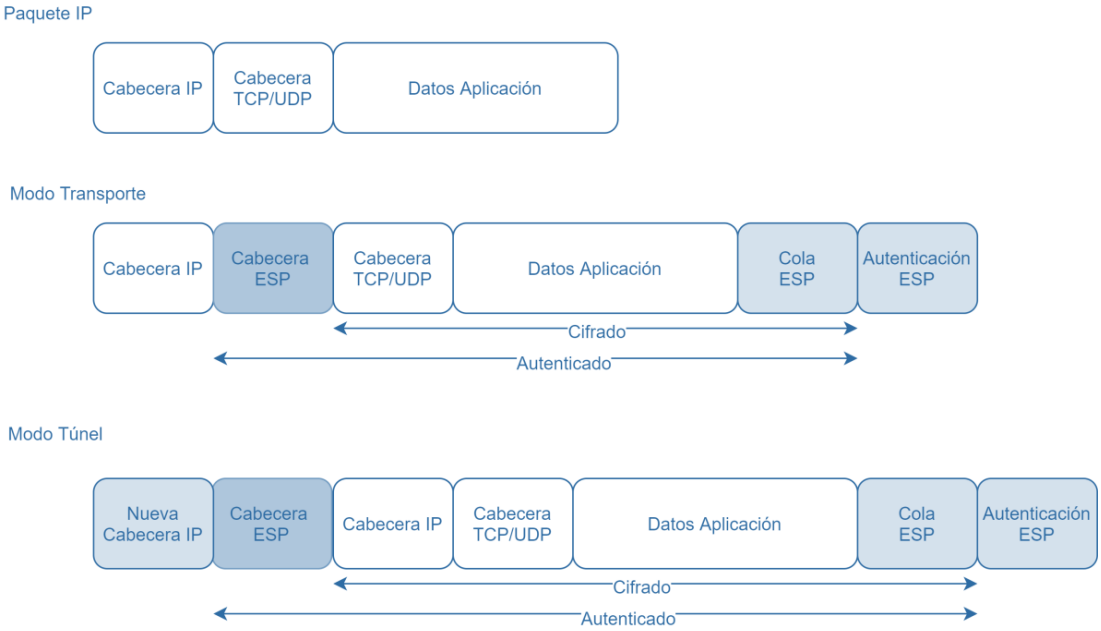


Figura 16. Construcción del paquete ESP.

184. La **confidencialidad** de ESP se proporciona mediante el uso de criptografía simétrica. Un ejemplo de estos algoritmos es AES-GCM.

185. Para aportar **protección de la integridad**, se realiza el cálculo de un valor ICV (*Integrity Check Value*) sobre el mensaje. En la mayor parte de los casos, IPsec utiliza para ello un código de autenticación protegido por clave (*keyed-hash message authentication code*, HMAC). Un ejemplo es HMAC-SHA-256.

186. Sin embargo, el uso de diferentes algoritmos de cifrado y protección de integridad requiere dos procesos criptográficos que harán uso de diferentes claves. En la práctica, existen algoritmos que combinan ambos procesos y cuyo uso incrementa sensiblemente las prestaciones. Estos algoritmos se denominan AEAD (*Authenticated Encryption with Associated Data).*

> Siempre que sea posible, se recomienda la utilización de algoritmos AEAD, como **AES-GCM**, dado que ofrece protección de la confidencialidad y de integridad en un único proceso.

B.4 PROTOCOLO IKE

187. El protocolo de establecimiento y mantenimiento de las SA utilizado por IPsec se denomina IKE (Internet Key Exchange). Este protocolo se encarga de la autenticación mutua entre los dos extremos, y de negociar, crear y mantener las Asociaciones de Seguridad (SA) de la conexión IPsec.

> Actualmente existen dos (2) versiones del protocolo IKE: IKEv1 e IKEv2. La primera se trata de una versión casi en desuso, y, por lo tanto, siempre que sea posible, **deberá utilizarse IKEv2** en lugar de IKEv1.

188. El protocolo **IKEv2** se define en la RFC 7296 - *Internet Key Exchange Protocol Version 2* (IKEv2) [10], la cual es una revisión de las anteriores RFC 5996 y RFC 4306.

189. Previo al establecimiento de la SA de la conexión IPsec (IPsec SA), se crea la IKE SA. Esta IKE SA establece los algoritmos criptográficos, claves secretas, mecanismos de autenticación, grupo *Diffie-Hellman*, y otros parámetros a usar para la protección de los mensajes intercambiados posteriormente en la negociación de las IPsec SA, y otros mensajes de control.

B.4.1 IKEV2: INTERCAMBIOS

190. Cada comunicación IKE entre origen y destino, está compuesta de un par de mensajes (petición / respuesta), al que se le denominará "intercambio". Existen (4) cuatro tipos de intercambios, los cuales se explican a continuación:

a) El primer intercambio ***IKE_SA_INIT*** negocia algoritmos criptográficos, intercambia *nonces* (números de un solo uso) y realiza un intercambio *Diffie-Hellman* (DH) a partir del cual se genera un secreto compartido. Todos los mensajes a partir de este intercambio estarán criptográficamente protegidos utilizando los algoritmos y claves negociados.

b) El segundo par de mensajes (***IKE_AUTH***) autentica los mensajes previos, intercambia identidades y certificados y establece la primera SA derivada (*Child SA)*. La confidencialidad y la integridad de este segundo par de mensajes está protegida con el material acordado en el primer intercambio.

La autenticación de los extremos en *IKE_AUTH* puede realizarse mediante claves pre-compartidas (*pre-shared-keys* o PSK), o mediante mecanismos de criptografía asimétrica (certificados digitales).

Para la **autenticación de extremos en IKEv2 se recomienda el uso de mecanismos de criptografía asimétrica**, **especialmente aquellos basados en uso de PKI**, en lugar de claves pre-compartidas (PSK), por dos motivos principales: cualquier parte que sepa la PSK podría autenticarse y conectarse a la VPN, y suelen ser vulnerables a ataques de diccionario.

Únicamente deberían utilizarse cuando sea posible asegurar que han sido generadas con la entropía suficiente para aportar la fortaleza deseada (Ej.: para sistemas del ENS categoría ALTA se exigen 128 bits) y es posible renovarlas en un período inferior a su "cripto período".

También existe una **opción de no autenticación**, aunque **no debe utilizarse**.

c) El tercer intercambio, ***CREATE_CHILD_SA***, se utiliza para crear, cuando sea necesario, nuevas SA (IKE o IPsec). Normalmente este intercambio se realizará cuando haya expirado el tiempo de vida de las SA y haya que crear

unas nuevas (*rekeying*). Este intercambio no podrá realizarse hasta que se haya completado el segundo.

d) El cuarto intercambio, ***INFORMATIONAL***, se utiliza para intercambiar mensajes de control con errores o cualquier tipo de notificación entre los participantes.

191. El protocolo IKE habitualmente escucha y recibe mensajes en el puerto UDP 500, aunque también pueden recibirse en el 4500 con un formato ligeramente diferente.

B.4.2 IKEV2: GENERACIÓN DE CLAVES

192. Para la generación de todo el material criptográfico que se utilizará en las IKE SA y en las IPsec SA, se hará uso de la derivación de claves. Para ello se intercambiarán claves efímeras mediante un algoritmo *Diffie-Hellman*, y se calculará el material criptográfico a partir de ellas, mediante una función pseudoaleatoria (PRF).

Para la generación de claves **deberán** emplearse grupos *Diffie-Hellman* que cuenten con una **fortaleza igual o superior a 128 bits**, es decir, grupos con longitud de módulo de, al menos 3072 bits, o grupos definidos por curvas elípticas sobre campos primos mayores o iguales a 224 bits.

193. Actualmente se encuentran definidos 32 grupos DH, aunque no todos se encuentran disponibles en las implementaciones de IKE. En la siguiente tabla se muestra un listado de los grupos permitidos para establecer VPN en las implementaciones actuales:

Grupo	Curva	Fortaleza (bits)	Uso permitido
15	*MODP 3072 bits*	128	Posterior a 2025
19	*256-bit random EC*[14]	128	Posterior a 2025
20	*384-bit random EC*[15]	192	Posterior a 2025
21	*512-bit random EC*[16]	256	Posterior a 2025
28	*Brainpool Elliptic Curve P256r1*	128	Posterior a 2025
29	*Brainpool Elliptic Curve P384r1*	192	Posterior a 2025
30	*Brainpool Elliptic Curve P512r1*	256	Posterior a 2025

Tabla 7. Curvas Elípticas y Fortaleza

[14] RFC 5903 basada en las curvas elípticas definidas por el NIST

[15] RFC 5903 basada en las curvas elípticas definidas por el NIST

[16] RFC 5903 basada en las curvas elípticas definidas por el NIST

En caso de seleccionar un grupo basado en curvas elípticas, siempre que sea posible, se recomienda el uso de **curvas *Brainpool*** (28, 29 o 30).

B.4.3 IKEV2: TIEMPO DE VIDA DE LAS SA

194. Para cada SA se podrá negociar un tiempo de vida que podrá estar basado en tiempo o en volumen de datos transmitidos, aunque se dará siempre prioridad a los criterios basados en tiempo. En IKEv2 no se podrá renegociar este tiempo una vez se haya establecido. Además, cada extremo de la SA podrá tener un tiempo de vida diferente, en este caso, el extremo que haya configurado ese tiempo de vida menor será el que solicite la renovación o cierre de la SA.

El tiempo de vida máximo recomendado para cada SA dependerá de las exigencias de cada aplicación, y será inversamente proporcional al grado de clasificación o sensibilidad de la información que se va a transmitir. A mayor frecuencia de renovación de claves mayor seguridad, aunque es necesario tener en cuenta posibles limitaciones impuestas por el tamaño de la red o el ancho de banda con el que se trabaja.

El tiempo de vida de las *Child SA* no deberá ser mayor que el de las IKE SA y, en general, se recomiendan valores inferiores a 4 horas para las Child SA, e inferiores a 24 horas para las IKE SA.

B.4.4 IKEV2: PERFECT FORWARD SECRECY (PFS)

195. La capacidad de *Perfect Forward Secrecy* impide que se descifre el contenido de la comunicación, aunque se comprometan las claves establecidas para las asociaciones de seguridad.

196. En el primer intercambio de IKE, se generan las claves para las asociaciones de seguridad IKE y *Child*. Si se negocian más *C*hild SA partiendo de las IKE SA existentes, el protocolo da la opción de realizar un nuevo intercambio *Diffie-Hellman*, lo que permite que se calculen nuevas claves para la sesión. De esta forma, aunque se comprometan las claves intercambiadas inicialmente, no es posible comprometer las claves posteriores.

Deberá activarse el PFS para IKEv2, y la renovación de claves cada cierto tiempo o cada cierto volumen de datos.

B.5 USO DE NAT CON IPSEC

197. Los elementos con capacidad de traducción de direcciones o **NAT** (*Network Access Translation*) no son compatibles con los protocolos de IPsec por defecto, ya que NAT realiza modificaciones en las cabeceras de los paquetes IP, y los protocolos de IPsec protegen los paquetes IP (incluidas las cabeceras) frente a modificaciones. Los motivos fundamentales son:

a) El uso del protocolo AH, como se ha explicado, autentica todo el paquete, incluidas las cabeceras.

b) Los *checksum* calculados en las cabeceras TCP y UDP dependen de las direcciones IP origen y destino. Los protocolos IPSec verifican el *checksum*, por lo que, si se han modificado las direcciones, el paquete sería descartado. Esto no aplicaría si se usa ESP en modo túnel o no se utiliza el *checksum* en UDP.

c) IKE negocia los detalles de la comunicación IPSec, incluyendo las direcciones, puertos a emplear, etc. Si se modifican estos valores negociados se invalidaría el paquete.

198. La RFC 3715 - *IPsec-Network Address Translation (NAT) Compatibility Requirements* [11], describe con mayor detalle las incompatibilidades entre IPsec y NAT.

199. **NAT-T**, conocido como NAT Transversal (RFC 3947), es un estándar diseñado para solucionar la problemática existente entre IPSec y los entornos de NAT. Este estándar se basa en encapsular los paquetes IPSec en paquetes UDP, de forma que las modificaciones realizadas por los entornos de NAT lo hagan sobre direcciones existentes en las cabeceras del paquete exterior UDP.

200. NAT-T emplea por defecto el puerto 4500 para la encapsulación en paquetes UDP, algo que deberá tenerse en cuenta en la configuración de los firewalls.

En el caso de que sea necesario emplear NAT en las comunicaciones, **deberá activarse la opción de NAT Transversal.**

ANEXO C. MACSEC

201. **MACsec, Media Access Control (MAC) Security,** es un estándar definido en IEEE 802.1AE, que especifica un conjunto de protocolos que proporcionan medidas de seguridad para la protección de los datos en la capa de enlace (L2 OSI) de redes de área local (LAN) tipo Ethernet. La primera versión fue publicada en 2006. La versión actual es la **IEEE 802.1AE-2018**.

202. MACsec proporciona, principalmente, los siguientes servicios de seguridad:

    a) **Confidencialidad de datos**, mediante el uso del algoritmo de cifrado simétrico AES en modos AEAD (*Authenticated Encryption with Additional Data*), mayormente AES-GCM.

    b) **Protección de la integridad de los datos sin conexión,** gracias al uso de un código de verificación de integridad (ICV) exclusivo y único en cada paquete MACsec, y no relacionado con el resto de paquetes (*sin conexión*). Esto permite que cualquier cambio no autorizado sea detectado.

    c) **Autenticidad de datos en origen,** ya que con el uso del código de verificación ICV, se garantiza que el paquete MAC recibido ha sido enviado por quien se indica en el campo *Dirección MAC Origen* del paquete.

    d) **Protección anti-reenvíos (*anti-replay*)**, mediante números de secuencia añadidos al mensaje (campo PN, *Packet Number*).

    e) **Arquitectura segura *hop-by-hop***, gracias al cifrado y descifrado de la información en cada nodo MACsec por el que pasa el paquete.

    f) **Límite de retraso de recepción**, mediante el uso del parámetro *bounded time*, el cual suele tener, normalmente, un valor menor a 2 segundos. Este parámetro indica el tiempo límite para la recepción de un paquete desde su momento de envío. Sirve para descartar todos aquellos paquetes que tardan más del tiempo habitual en ser recibidos, indicando que han podido ser interceptados y modificados entre el origen y el destino.

203. MACsec permite proteger gran parte del tráfico interno, como LLDP, LACP, DHCP y ARP, junto con otros protocolos que no suelen protegerse. Tecnologías de capas superiores, como son IPsec y TLS, no pueden detectar ni prevenir ataques de capa de enlace, pero pueden complementarse con MACsec para conseguir una seguridad de red extremo a extremo.

C.1 FUNCIONAMIENTO

204. Dentro del funcionamiento global de MACsec, intervienen los protocolos IEEE 802.1X/EAP, EAPOL y MKA.

    a) **IEEE802.1X/EAP** se utiliza para la **autenticación**, la **generación y distribución de una clave maestra** MSK (*Master Session Key*). De esta clave maestra posteriormente se derivará la **CAK** (*Connectivity Association Key*). Las tramas que se intercambian para estas negociaciones, se encapsulan con el protocolo EAPOL.

b) **MKA** (*MACsec Key Agreement Protocol*) se utiliza, principalmente, para:

- Descubrir miembros de una CA (*Connectivity Association*).
- Confirmar la posesión mutua de una CAK y, por tanto, probar una autenticación anterior.
- Derivar otras claves a partir de la CAK: la clave ICK que será usada para la protección de la integridad y autenticidad de los paquetes MKA, y la clave KEK que será usada para el cifrado de la clave SAK (clave final de cifrado de datos).
- Acordar la *cipher suite* y derivar y distribuir de forma segura las claves SAK utilizadas por MACsec para el cifrado de los datos (MSDU).
- Asegurar que las tramas enviadas no tienen retardo, mediante el uso conjunto de los parámetros MI (*Member Identifier*) y MN (*Message Number*).

205. El funcionamiento tanto de MACsec como de 802.1X y MKA es complejo. Se recomienda consultar las especificaciones IEEE correspondientes para mayor detalle.

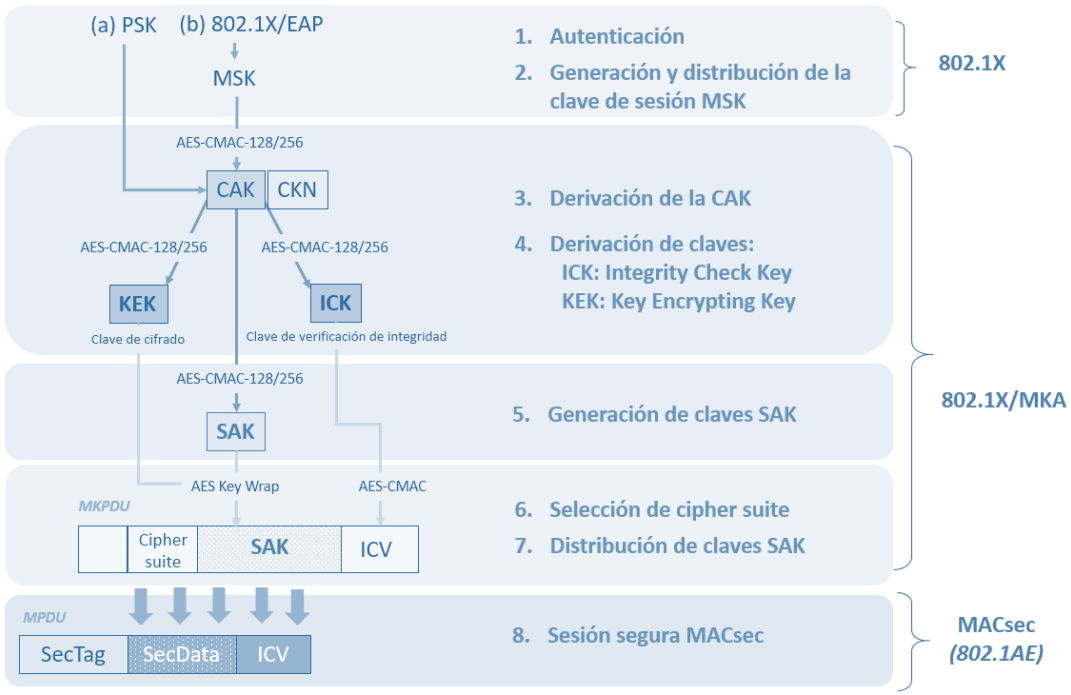


Figura 17. Diagrama de fases generales de MACsec

C.1.1 AUTENTICACIÓN Y DERIVACIÓN DE CLAVE CAK

206. El primer paso para el establecimiento de una sesión MACsec es la autenticación de los dispositivos que formarán parte de la CA, y la obtención de la **clave CAK** *(Secure Connectivity Association Key)*. Todos los dispositivos que forman parte de

una *Asociación de Conectividad Segura* (**CA**), comparten la clave CAK. De esta clave se derivará el material de claves.

207. Para ello se pueden utilizar, principalmente, dos (2) métodos: "Claves pre-compartidas" o IEEE 802.1X/EAP.

> **No se recomienda la autenticación con claves pre-compartidas**, por dos motivos principales: cualquier parte que sepa la clave podría autenticarse y, además, estas claves son vulnerables a ataques de diccionario. Además, añade complejidad a la instalación y al mantenimiento cuando el número de estaciones es elevado.
>
> Únicamente deberían utilizarse cuando sea posible asegurar que han sido generadas con la entropía suficiente para aportar la fortaleza deseada (Ej.: para sistemas del ENS categoría ALTA se exigen 128 bits) y que su distribución se realiza de manera segura no siendo posible su comprometimiento durante el transporte.

208. IEEE 802.1X define varios términos relacionados con la autenticación:

    a) **Suplicante**: dispositivo cliente que solicita el acceso a la red.

    b) **Autenticador**: dispositivo que permite o bloquea el acceso a la red (por ejemplo, un *switch*).

    c) **Servidor de Autenticación (AS)**: servidor que determina, a partir de las credenciales proporcionadas por el suplicante, si este está autorizado a acceder a los servicios proporcionados por el autenticador. Otra de las funciones del AS es la de generar e intercambiar las claves criptográficas con el suplicante, y distribuirlas de forma segura al autenticador.

209. Para el proceso de autenticación y autorización de acceso a la red, el estándar IEEE 802.1X define el protocolo **EAPoL** (*EAP over LAN*), que es la encapsulación de EAP (*Extensible Authentication Protocol*) sobre redes LAN.

210. El proceso de autenticación y autorización, se desarrolla de la siguiente forma:

    a) El suplicante inicia el proceso de autenticación enviando un *EAPoL Start* al Autenticador. Este le responde solicitándole la identidad, a través de una trama *EAP Request / Identity*. El suplicante responde con *EAP Response*, indicando cuál es su identidad y ratificando con ello su solicitud de autenticación.

    b) A partir de entonces, el Autenticador hace de intermediario entre el Suplicante, con el que se comunica con mensajes EAP, y el Servidor de Autenticación (AS), con el que se comunica con mensajes en función del protocolo de autenticación, por ejemplo, RADIUS. El AS y el suplicante, en primer lugar, acordarán cuál es el mecanismo de autenticación (método EAP). En función del mecanismo empleado, el suplicante proporcionará las credenciales correspondientes al AS y este las verificará (intercambio de mensajes *EAP Request* y *Response*, trasladadas por el Autenticador). Si todo

el proceso es correcto, el Autenticador finalizará con un mensaje *EAP Success* y permitirá al suplicante el acceso a la red.

c) Una vez autenticado el solicitante y permitido su acceso a la red, el servidor de autenticación y el solicitante acuerdan una clave maestra MSK (*Master Session Key*). Para ello, se utiliza también EAP. Este material criptográfico puede ser derivado de mutuo acuerdo entre el solicitante y el AS, o puede ser generado por el AS y distribuido al solicitante. El AS posteriormente deberá distribuirlo por un canal seguro al autenticador.

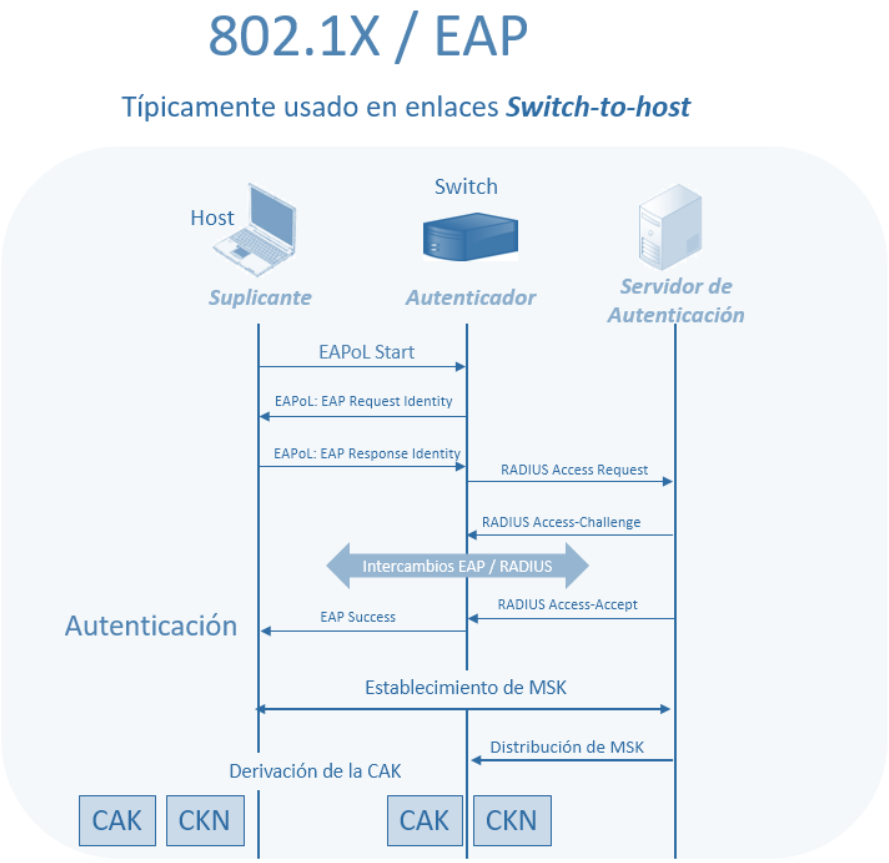


Figura 18. Diagrama de Autenticación y generación de CAK mediante 802.1X/EAP

211. A partir de la MSK se deriva la clave **CAK** (*Connectivity Association Key*). Esta es una **clave de larga vida** a partir de la cual se deriva el material criptográfico para MKA y MACsec. Todos los dispositivos que comparten dicha clave CAK forman parte de una *Asociación de Conectividad Segura* (**CA**).

212. La función de derivación KDF (*Key Derivation Function*), utilizada para generar la clave CAK, hace uso de la función pseudoaleatoria **AES-CMAC-128 o AES-CMAC-256,** dependiendo de si la clave que se desea obtener es de longitud 128 o 256 bits.

En caso de que se utilice la autenticación con **claves pre-compartidas**, se recomienda utilizar un identificador de la clave (CKN) de longitud, al menos, 32 bytes.

En caso de que se utilice la autenticación 802.1X se deberá utilizar una implementación que cumpla el estándar IEEE802.1X (sección 6.2.2 *Using EAP for CAK key derivation*).

213. Dado que los métodos EAP deben ser capaces de generar y distribuir el material de claves criptográficas y esto representa un proceso complejo y especialmente crítico desde el punto de vista de la seguridad, deberán utilizarse tecnologías maduras. Esto limita mucho las posibilidades de elección entre los métodos EAP[17]. Actualmente, solo se recomiendan los métodos basados en TLS.

Se recomienda la autenticación **IEEE 802.1X/EAP** con el método de autenticación **EAP – TLS** (RFC 5216), empleando una versión de **TLS 1.2 o superior**.

C.1.2 DERIVACIÓN DE CLAVES ICK Y KEK

214. Dentro de la jerarquía de claves MKA, la clave raíz de la jerarquía es CAK.

215. MKA no utiliza la clave CAK directamente, sino que deriva de ella otras claves que irán ligadas al identificador de la CAK (CKN) y cuyo uso, por lo tanto, estará restringido a las entidades que utilizan esa CAK (participantes de la misma CA):

    a) **Clave ICK**: *Integrity Check Key*. Clave usada para el cálculo del ICV (*Integrity Check Value*) empleado para verificar la integridad de los paquetes MKA (MKPDUs, *MKA Data Units*) y para verificar la autenticación previa realizada entre los pares. Esto último es posible porque el ICV demuestra que el nodo que envía el mensaje cuenta con la clave CAK.

    b) **Clave KEK**: *Key Encrypting Key*. A través de paquetes MKA (MKPDUs) se enviará la clave final de cifrado (SAK). El envío de esta clave está a su vez protegido con un cifrado *AES Key Wrap* usando la clave KEK.

216. La función de derivación KDF (*Key Derivation Function*), utilizada para la generación de la clave KEK, hace uso de la función pseudoaleatoria **AES-CMAC-128 o AES-CMAC-256** dependiendo de si la clave que se desea obtener es de longitud 128 o 256 bits.

[17] Los métodos EAP actualmente existentes, salvo aquellos que son propiedad de fabricantes, se encuentran en el Registro de IANA: *Extensible Authentication Protocol Registry: http://www.iana.org/assignments/eap-numbers/eap-numbers.xhtml#eap-numbers-4.*

Se recomienda que la implementación del protocolo MKA genere las claves **ICK y KEK,** mediante la derivación de la CAK haciendo uso de la función KDF. Para ello, la implementación deberá cumplir el estándar IEEE 802.1X-2010/2020 (sección 9.3.3 *Derived keys*).

217. SAK es la *Clave de Asociación Segura*, que será una clave asociada a cada asociación de seguridad (SA) y empleada para el cifrado de todos los paquetes que se transmitan en esa SA. En el proceso de generación y distribución de la clave de cifrado SAK interviene un ***Key Server***, que es uno de los participantes de la CA que desempeñará este rol.

218. El Key Server, o servidor de claves, es elegido de manera dinámica entre todos los participantes de la CA. Su principal función es la generación, a partir de la clave CAK, de las claves SAKs asociadas a las SAs, junto con la distribución de manera segura de estas a los miembros correspondientes. La elección del servidor se realiza de la siguiente manera:

    a) Cada estación o nodo MACsec envía un mensaje *heartbeat* en broadcast, el cual contiene:

        a. Prioridad del *Key Server*.

        b. Información anti-reenvío (lista de nodos *vivos*[18]).

    b) Una vez que las estaciones estén de acuerdo en la lista de nodos *vivos*, el nodo que tenga mayor prioridad será el elegido *Key Server*.

    c) Si el nodo abandona la lista de nodos *vivos*, se deberá escoger un nuevo *Key Server*.

219. La función de derivación KDF (*Key Derivation Function*), utilizada para la generación de la clave SAK en el Key Server, hace uso de la función pseudoaleatoria **AES-CMAC-128** en caso de que la clave CAK sea de 128 bits, o **AES-CMAC-256**, si la clave CAK es de 256 bits.

Se recomienda que la implementación del protocolo MKA genere las claves SAKs mediante derivación de la CAK. Para ello, la implementación deberá cumplir el estándar IEEE 802.1X-2010/2020 (sección 9.8.1 *SAK generation*).

220. A cada clave SAK se le asigna un identificador (**KI**) de 128 bits, compuesto por el identificador del *key server* (**MI,** *Member Identifier*) de 96 bits, junto con un número de 32 bits (**KN,** *Key Number*) asignado a la clave SAK por el Key Server. Este KN se asigna de forma secuencial empezando en 1.

221. El *Key Server* selecciona la *cipher suite* y la anuncia con cada clave SAK. Se distribuye el código identificativo de la *cipher suite* (8 octetos). También se

[18] La expresión *nodos vivos* hace referencia a la lista de nodos que se encuentran activos y conectados con dicha estación en ese instante.

distribuye un valor que es el "*Confidentiality Offset*", que puede ser 0, 30 o 50. Este valor significa que los primeros 0, 30 o 50 octetos del paquete MAC (MSDU) no van cifrados, solo llevan protección de integridad y aparecerán en el paquete MACsec (MPDU) inmediatamente después de campo SecTAG en el orden y composición que iban en MSDU. Los restantes octetos sí irán cifrados[19].

222. Las cipher suites posibles son cuatro: *GCM-AES-128, GCM-AES-256, GCM-AES-XPN-128 y GCM-AES-XPN-256* y se detallan en el apartado 3.

223. El *Key Server* distribuye la clave SAK cifrada con ***AES Key Wrap***[20] **usando la clave KEK.** Todos los participantes que dispongan de la CAK de la que se ha derivado la KEK, podrán descifrar el paquete. En el paquete MKA (MKPDU), el *Key Server* también incluye la *cipher sui*te seleccionada para esa SAK y un número que el Key Server asignará a esa SAK (KN, *Key Number*). Este KN se utilizará, junto con otros parámetros, para componer el identificador de la clave SAK (KI, *Key Identifier*).

> Se recomienda que la implementación MKA utilice la función **AES Key Wrap** para la distribución de claves SAK entre nodos MACsec. Para ello, la implementación deberá cumplir el estándar IEEE 802.1X-2010/2020 (sección 9.8.2 *Use of AES Key Wrap*).

224. El Key Server distribuirá las claves SAK en los paquetes MKPDU a todos los nodos de la red, hasta que dichos nodos respondan al mensaje confirmando la instalación de la clave SAK.

225. Las claves SAK se regeneran si se da alguno de los siguientes casos:

    a) Se supera el límite de usos de la clave. Dependiendo de la *cipher suite* usada, se permite un mayor o menor número de usos con una misma clave.

    b) Se añade un nuevo nodo o se elimina un nodo de la CA.

    c) Se modifica la *cipher suite* a usar.

    d) Se ha añadido un tiempo límite para la regeneración de las claves SAK.

226. En cualquiera de estos casos, el *Key Server* es el encargado de volver a generar una nueva clave SAK, tal y como se indica en el apartado 2.5.2, y de distribuirla a todos los miembros de la CA.

> Se recomienda que la implementación del protocolo MKA especifique que el *Key Server* regenere la clave SAK cada vez que se añada o elimine un nuevo miembro a la CA. Para ello, la implementación deberá cumplir el estándar IEEE 802.1X-2010/2020 (sección 9.8 *SAK generation, distribution, and selection*).

[19] La opción de *Confidentiality offset* se especificó en la 802.1AE-2006 para facilitar la implementación temprana de MACsec en sistemas que necesitaban examinar los octetos iniciales de las tramas de IPv4 o IPv6 y que, por lo tanto, debían ir sin cifrar.

[20] AES Key Wrap según la definición de IETF RFC 3394

227. Como se ha indicado con anterioridad, MKA proporciona un transporte seguro de información multipunto a multipunto entre los miembros de una misma CA. La clave CAK, que debe ser conocida por todos los miembros de la CA, se utiliza para autenticar cada paquete trasmitido (MKPDU), ya que la posesión de esa CAK demuestra que el transmisor es un miembro autenticado de la CA.

228. Cada miembro emisor incluye en el paquete MKPDU:

    a) El nombre de la CAK (CKN).

    b) Su SCI, *Secure Channel Identifier*, compuesto por la dirección MAC y el puerto.

    c) Su MI: *Member Identifier*, número aleatorio de 96 bit que escoge cada miembro cuando comienza su participación en el protocolo.

    d) Su MN: *Message Number*, número de 32 bits secuencial (iniciándose en 1) asignado a los paquetes MKPDU emitidos por un transmisor. Se incrementa con cada MKPDU transmitido.

    e) Un valor ICV (*Integrity Check Value*) calculado a partir de la clave ICK (derivada, a su vez, de la clave CAK tal y como se indica en el apartado 2.4).

229. Al incluir el identificador de la CAK usada (CKN), el receptor podrá verificar el ICV usando la CAK correcta. Esta verificación demuestra que el emisor poseía la CAK y, por lo tanto, se puede autenticar el paquete MKPDU.

230. Por otro lado, el uso de los valores MI y MN en conjunto, permite proteger las transmisiones de retardos o de ataques *replay*.

231. Una vez los nodos o estaciones MACsec han instalado correctamente la clave SAK, todo el tráfico transmitido estará cifrado con las *cipher suites* elegidas por el *Key Server*, utilizando las claves SAK correspondientes a cada SA. Estas claves SAK se van renovando, según se vaya superando el límite de paquetes enviados con dicha clave.

232. En la sesión segura, solo se permitirá el paso del tráfico cifrado MACsec, con la excepción del tráfico de control, como las tramas EAPoL.

233. La sesión segura utiliza un identificador único SCI (*Secure Channel Identifier*). Durante la sesión establecida solo se aceptan aquellos paquetes que contengan el identificador SCI de esa sesión.

234. La sesión segura también proporciona **protección anti-reenvíos (*anti-replay*)** utilizando el PN (*packet number*) y dos parámetros: *replayProtection* y *replayWindow*. El primero indica si está o no activa la protección anti-reenvío. El segundo indica la ventana de paquetes que podrán llegar desordenados y ser admitidos. Por ejemplo, si el *replayWindow* es 300 quiere decir que si recibe un paquete con PN=5, el siguiente paquete que admitirá podrá tener un PN entre 6 y 306. La protección anti-reenvío, consiste en un *replayWindow* cero, que es el valor por defecto indicado en el estándar IEEE 802.1AE.

Se recomienda que la implementación del protocolo MACsec disponga de la **protección anti-reenvío**. Para ello, la implementación deberá cumplir el estándar IEEE 802.1X-2010/2020 (sección 10.7.8 *Frame verification controls*).

C.1.3 CIPHER SUITES Y PARÁMETROS CRIPTOGRÁFICOS

235. El protocolo MACsec utiliza un algoritmo para el cifrado de los paquetes y para la protección de integridad, a través de lo que se denomina la suite criptográfica o ***cipher suite***. Esta *cipher suite* está compuesta por los algoritmos y funciones criptográficas, junto con sus parámetros (longitud de clave, modo de operación, etc.) que se van a utilizar para proteger la conexión.

236. De forma general, la *cipher suite* se representa de la siguiente manera:

Mode-Cipher-KeyLength

237. Los diferentes valores de la *cipher suite* corresponden al algoritmo de cifrado (*Cipher*), su longitud de clave (*KeyLength*) y su modo de operación (*Mode*).

238. En la versión actual del estándar MACsec[21], se encuentran aceptadas las siguientes cuatro (4) *cipher suites*, las cuales se emplean tanto para el cifrado como para la protección de la integridad.

Cipher Suite	Obligatoria / Opcional
GCM-AES-128	Obligatoria
GCM-AES-256	Opcional
GCM-AES-XPN-128	Opcional
GCM-AES-XPN-256	Opcional

Tabla 8. *Cipher suite* aceptadas

239. Como se puede observar en la tabla, la *cipher suite GCM-AES-128* es **obligatoria** y el resto son opcionales. En caso de emplear una *cipher suite* distinta a las indicadas en la tabla, deberán cumplirse una serie de requisitos indicados en el apartado 14.4.1 del estándar IEEE 802.1AE-2018.

Se recomienda que la implementación del protocolo MACsec utilice las *cipher suites* indicadas en la tabla anterior (Tabla 1). Para ello, la implementación deberá cumplir el estándar IEEE 802.1AE-2018 (sección 14.4 *Cipher Suite conformance*).

[21] Estándar IEEE 802.1AE-2018.

240. Indicar que, como se puede observar en las *cipher suites* de MACsec, la mínima longitud de clave AES es **128 bits.** Esto representa una **fortaleza suficiente para el ENS**.

241. Respecto al modo de operación de AES, actualmente MACsec solo soporta el modo **GCM**. *Galois Counter Mode*[22] es un modo de operación para cifradores de bloque. La operación que realiza es lo que se llama un AE "***Autheticated Encryption***" ya que proporciona autenticidad y confidencialidad.

242. Las *cipher suites* indicadas en la tabla como *GCM-AES-XPN-128/256* hacen uso de la característica ***MACsec Extended Packet Numbering (XPN)***, que se describe a continuación.

243. Como en otros modos de operación de cifradores de bloque, se requiere el uso de un Vector de Inicialización (IV) que deberá ser único para cada paquete cifrado con una clave (SAK, en este caso). Para componer el IV, se utiliza el parámetro **PN**[23] (*Packet Number*) de **32 bits**. Esto indica que el límite de usos de una misma clave SAK será de 2^{32}, lo cual puede ser un problema en enlaces de alta velocidad (40 Gb/s), ya que el PN se agota a los pocos segundos y es necesario volver a generar las claves SAK.

244. Con el uso de **XPN (*Extended* PN)**, se extiende la longitud del PN de cada paquete MACsec hasta 64 bits, lo cual requeriría varios años para que se agote el PN, asegurando que la regeneración de claves SAK no se produzca con tanta frecuencia en enlaces de alta velocidad.

245. Es importante indicar que el uso de XPN está diseñado solo para dispositivos que cuenten con un rendimiento igual o superior a 40 Gb/s.

246. La *cipher suite* y la clave SAK, se utilizan para el cifrado y para la protección de integridad.

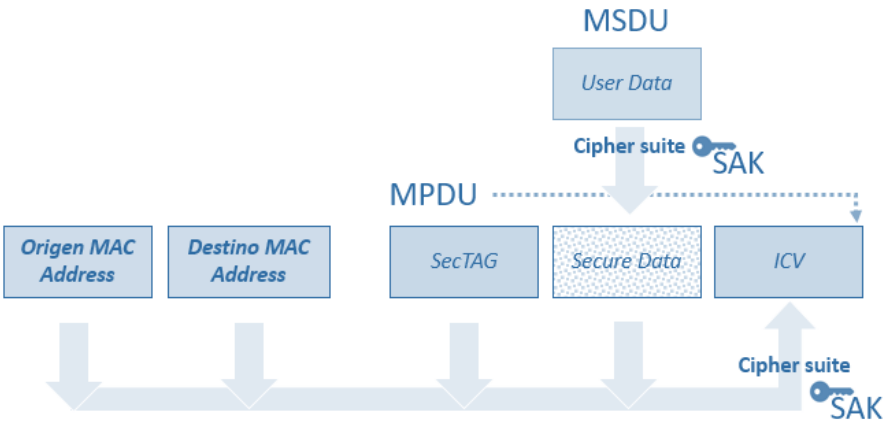


Figura 19. Cifrado y cálculo del ICV MACsec

[22] Se puede consultar más información sobre el funcionamiento del modo GCM en la ISO 17792 (Authenticated Encryption Modes), o en la publicación especial NIST SP 800-38D: *Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.*

[23] PN (*Packet Number*): Es un número de 32 o 64 bits (en este último caso es *Extended Packet Number, XPN*) que se va incrementando y que es único para cada trama MACsec transmitida con una misma clave SAK.

247. MACsec utiliza dos (2) cifrados:

(a) El cifrado de la clave SAK para su envío seguro. Esto lo hace el *Key Server* con el protocolo MKA, y utiliza para ello la función *AES Key Wrap* (ver apartado 2.5.3).

(b) El cifrado de los datos (MSDU) utilizando la clave de cifrado SAK. Para este cifrado se utiliza una de las *cipher suites* indicadas.

248. Es importante indicar que, tal y como se especifica en el estándar IEEE 802.1AE-2018 (sección 14.2 *Cipher Suite capabilities*) **en MACsec el uso del cifrado es opcional**.

> Se debe configurar el uso del cifrado en MACsec.

249. Para proporcionar integridad al paquete MACsec, se realiza el cálculo del valor **ICV** (*Integrity Check Value*) el cual es posteriormente añadido al paquete MACsec. **Esta función del cálculo del ICV sí es obligatoria.**

250. El cálculo del ICV protege la integridad de las direcciones MAC origen y destino, los datos (cifrados, en caso de que se esté aplicando la protección de confidencialidad) y la etiqueta SecTAG.

> Se recomienda que la implementación del protocolo MACsec proporcione integridad al paquete transmitido (MPDU) mediante el cálculo del parámetro **ICV** (*Integrity Check Value*) derivado de la clave SAK. Para ello, la implementación deberá cumplir el estándar IEEE 802.1AE-2018 (sección 14.1 *Cipher Suite use*).

251. El cifrado y el cálculo del ICV utilizan la función ***Protect***, mientras que su descifrado y verificación utilizan la función ***Validate***. Se puede consultar más información sobre la operación de estas funciones en la sección 14. *Cipher Suites*, del estándar IEEE 802.1AE.

C.2 USOS DE MACSEC

C.2.1 MACSEC SOBRE LAN

252. El principal caso de uso de MACsec es securizar las redes LAN. Para hacerlo hay dos (2) arquitecturas diferentes dependiendo del enlace a proteger, tal y como se muestra en la siguiente imagen.



Figura 20. MACsec sobre LAN

Arquitectura Switch-to-Host

253. Los enlaces MACsec de tipo ***switch-to-host***, o también denominados *downlink*, establecen una conexión protegida entre un dispositivo de red (*switch*) y un dispositivo final (*endpoint*).

254. En este tipo de enlace se hace uso de **EAP/802.1X**, tal y como se explica en el apartado 2.3 b), para realizar la autenticación de los dispositivos, y posteriormente hacen uso de MKA para la creación y distribución de claves. El paquete es cifrado en el envío, y descifrado en la recepción.

Arquitectura *Switch-to-Switch*

255. Los enlaces de tipo switch-to-switch de MACsec, o también conocidos como uplink, establecen una conexión segura entre dos dispositivos de red (switch).

256. La conexión uplink puede ser establecida de manera manual o dinámica. Para la realización manual se requiere una configuración previa por parte de un administrador en cada dispositivo de red, indicando los parámetros necesarios a usar durante la conexión. En este caso, se haría uso de la opción de claves pre-compartidas para el establecimiento de la clave CAK.

257. En el modo dinámico se hace uso de 802.1X/EAP para la autenticación, de manera que un switch se convierte en el suplicante NDAC[24] y el otro en el servidor de autenticación, encargado de autenticar y de distribuir las claves al suplicante, para que este, posteriormente, se convierta en el autenticador frente a los dispositivos finales.

> En arquitecturas ***switch-to-switch***, se recomienda hacer uso del modo **dinámico** para el establecimiento de la conexión.

MACSEC SOBRE VXLAN

258. VXLAN (*Virtual Extensible LAN*) es un protocolo que se basa principalmente en encapsular el tráfico de capa de enlace (concretamente, tráfico Ethernet) de una red de área local, y transportarlo sobre una red IP (encapsulado MAC-in-UDP) hasta otra LAN física diferente, consiguiendo así que los *hosts* de ambas redes se puedan comunicar de igual manera que si se encontrasen en la misma red de área local[25].

259. MACsec es compatible con VXLAN y otras tecnologías de encapsulación similares.

260. Un ejemplo de aplicación sería un usuario que cuenta con una red LAN privada virtual en la nube. En este caso, se puede hacer uso de MACsec para cifrar todo el tráfico interno entre sus máquinas virtuales. Esto consigue que el proveedor de

[24] Un suplicante NDAC es un *switch* que actúa como suplicante y se autentica frente al servidor de autenticación, de manera previa a convertirse en un autenticador de usuarios, *hosts*.

[25] VXLAN inicialmente surgió para resolver el problema generado en centros de proceso de datos con miles de máquinas virtuales ya que, en caso necesidad de agrupar estas máquinas en VLANs, el número de VLANs que se pueden generar es limitado. Con VXLAN se proveen los mismos servicios que una red VLAN convencional, pero aumentando la extensibilidad y la flexibilidad limitadas de este tipo de redes.

servicios de nube sea incapaz de ver las comunicaciones entre las máquinas virtuales asegurando así, la confidencialidad de la información del usuario.

261. El túnel MACsec se establece entre las máquinas virtuales, en la VXLAN proporcionada por el proveedor de servicios en la nube, a través de las interfaces MACsec. En la siguiente imagen se observa como hay dos (2) VXLANs diferentes y solo se hace uso de MACsec sobre VXLAN1, que conecta las máquinas virtuales HA1, HA2 y HA3.

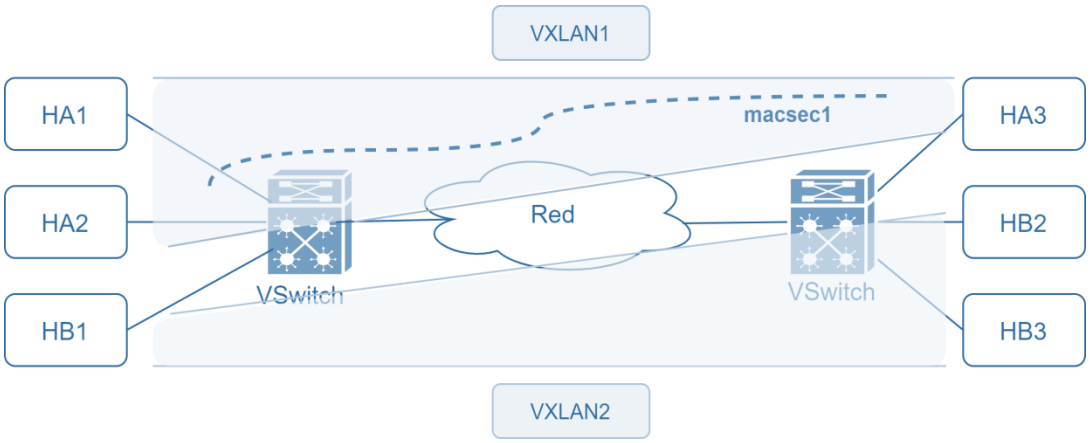


Figura 21. MACsec sobre VXLAN

C.2.2 MACSEC SOBRE WAN

262. Otro gran uso de MACsec se da sobre redes WAN. Actualmente, una organización no está compuesta de una sola red LAN, sino que cuenta con diversos proveedores de servicios, infraestructuras *cloud*, etc. El uso de WAN MACsec ofrece una conexión segura entre los diferentes sitios remotos de la organización.

263. WAN MACsec se basa en los estándares MACsec y utiliza características útiles para acoplarlo al uso en una WAN, como son:

    a) Configuración del parámetro *Anti-Replay Window*, que indica el tiempo, en segundos, en el cual está permitido el reenvío de paquetes.

    b) Configuración del parámetro *EAPoL Destination Address*, que permite modificar la dirección MAC destino del paquete MKA. Normalmente, MKA usa la dirección *multicast* EAPoL para que los paquetes lleguen a varios destinos. Como EAPoL es un protocolo usado por varios mecanismos de autenticación, pueden darse situaciones en las que dispositivos de red, cojan el paquete, lo intenten procesar y lo descarten, provocando un fallo en el establecimiento de la sesión MKA. Para evitar estas situaciones se permite configurar el parámetro *EAPoL Destiantion Address*.

264. El uso de MACsec en redes WAN ha ido creciendo durante los últimos años, debido a la seguridad que proporciona y a la velocidad que presenta frente a la tecnología IPsec.

265. En la siguiente imagen se muestra un ejemplo del funcionamiento de WAN MACsec *site-to-site*:

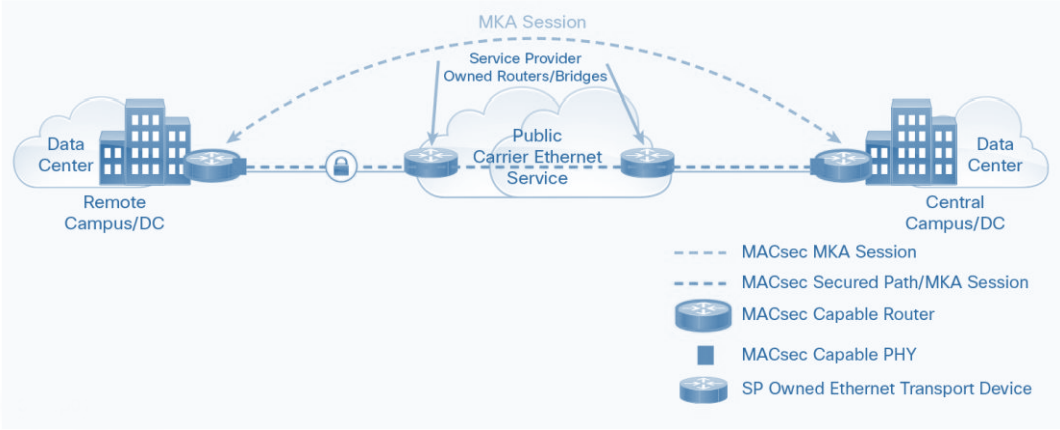


Figura 22. WAN MACsec ejemplo *site-to-site* [26]

[26] Imagen obtenida de: *https://www.cisco.com/c/dam/en/us/td/docs/solutions/Enterprise/Security/MACsec/WP-High-Speed-WAN-Encrypt-MACsec.pdf*

ANEXO D. WIREGUARD[27]

266. WireGuard es un túnel de red seguro que opera en la capa de red y que se implementa como un kernel de interfaz virtual de red para Linux. Su objetivo es remplazar tanto IPSec como soluciones VPN basadas en TLS siendo más seguro, rápido y fácil de usar que las anteriores.

267. Utiliza primitivas criptográficas modernas. Gracias a esta combinación de primitivas criptográficas extremadamente rápidas el rendimiento de WireGuard es muy elevado, y supera así a otras tecnologías como las basadas en TLS o IPsec.

268. WireGuard tiene una superficie de exposición mínima dado que ha sido implementado en una cantidad de lineas de código muy pequeña (aproximadamente 4000 lineas), dicha cantidad de lineas de código es de ordenes de magnitud menor comparado con otros productos VPN.

269. Las principales características son:

    a) Multiplataforma (Windows, Linux, MacOS, FreeBSD, Android, iOS).

    b) Se encuentra incluido en el kernel de Linux desde la versión 5.6.

    c) Código fuente simple y abierto.

    d) Bajo consumo de recursos.

    e) Gestión mínima de llaves. Una clave publica/privada por cliente.

    f) Intercambio de claves autenticado (Protocolo AKE).

    g) Evita la suplantación de identidad mediante llaves comprometidas.

    h) Tiene protección contra ataques de denegación de servicio y de reinyección de paquetes.

    i) Solo opera en la capa de red (Capa 3 OSI).

    j) No mantiene estado de clientes ni responde a paquetes no autenticados.

    k) Gestión transparente de la creación de sesiones utilizando un novedoso mecanismo de máquina de estado de temporizador.

[27] Información principal e imágenes obtenidas del technical whitepaper “WireGuard: Next Generation Kernel Network Tunnel”. https://www.wireguard.com/papers/wireguard.pdf

270. Protocolos y primitivas:

a) Uso de NoiseIK para el intercambio de llaves en una única comunicación de ida y vuelta (Basado en framework Noise[28]).

b) Curve 25519[29] para intercambio de llaves ECDH.

c) ChaCha20[30] para cifrado, autenticada con Poly1305[31] (Construccion AEAD RFC7539[32]) para la encapsulación de paquetes UDP.

d) BLAKE2s[33] para cálculos de hash (RFC7693[34]).

e) SipHash24[35] para tablas de hash de las llaves.

f) HKDF[36] para expansión del resultado del intercambio de llaves ECDH[37] (RFC5869[38]).

g) Modo opcional de Pre-shared key simétrica de 256 bits para añadir una capa de seguridad adicional de cifrado simétrico.

[28] Noise: Framework para protocolos criptográficos basados en el establecimiento de claves mediante el protocolo Diffie-Hellman. Su autor es Trevor Perrin.

[29] Curve 25519: Función de Curva Eliptica para Diffie-Hellman. https://cr.yp.to/ecdh/curve25519-20060209.pdf

[30] ChaCha20: Variante del algoritmo de cifrado de datos Salsa20/20. https://cr.yp.to/chacha/chacha-20080128.pdf

[31] Poly1305: Algoritmo de autenticación de mensajes. https://cr.yp.to/mac/poly1305-20050329.pdf

[32] RFC7539: ChaCha20 and Poly1305 for IETF Protocols. https://www.rfc-editor.org/rfc/rfc7539.txt

[33] BLAKE2: Función criptográfica hash. https://www.blake2.net/blake2.pdf

[34] RFC7693: The BLAKE2 Cryptographic Hash and Message Authentication Code (MAC). https://www.rfc-editor.org/rfc/rfc7693.txt

[35] SipHash24: Familia de funciones pseudo-aleatorias optimizadas cadenas cortas. https://cr.yp.to/siphash/siphash-20120918.pdf

[36] HKDF: Función de expansión de llaves basadas en HMAC. https://eprint.iacr.org/2010/264.pdf

[37] ECDH: Elliptic Curve Diffie-Hellman. https://www.rfc-editor.org/rfc/rfc6090.html#section-4

[38] RFC5869: HMAC-based Extract-and-Expand Key Derivation Function (HKDF).https://www.rfc-editor.org/rfc/rfc5869.txt

D.1 MODOS DE FUNCIONAMIENTO

271. WireGuard utiliza una interfaz virtual que puede ser administrada utilizando las herramientas estándar ip(8)[39] e ifconfig(8)[40].

272. Si bien durante el documento se utilizan las palabras cliente y servidor para identificar al remitente y destinatario de los paquetes de comunicación, en WireGuard no existe dicho concepto e identifica a ambos como peers.

273. Permite crear VPNs de tipo “sitio a sitio” y de tipo “punto a sitio”.

274. Su configuración es muy sencilla. Solo habrá que configurar la interfaz con una llave privada (utilizando de forma opcional una llave simétrica pre-compartida) y configurar las distintas llaves publicas que utilizarán las máquinas cliente para conectar. Las máquinas clientes intercambiaran las claves públicas con el servidor para iniciar la comunicación.

275. Los handshakes de conexión se realizan cada pocos minutos para proporcionar claves rotativas para garantizar la propiedad PFS[41]. Se realizan en función del tiempo en lugar del contenido de los paquetes de datos. Hay un mecanismo incorporado que garantiza que las claves y los handshakes más recientes estén actualizados y se renegocien cuando sea necesario. Utiliza una cola de paquetes separada por el host, lo que minimiza la pérdida de paquetes durante los handshakes y, al mismo tiempo, proporciona un rendimiento ininterrumpido para los clientes.

[39] Ip(8): Herramienta para mostrar y configurar enrutamiento, dispositivos de red, interfaces y tuneles. https://man7.org/linux/man-pages/man8/ip.8.html

[40] Ifconfig(8): Herramienta para configurar interfaces de red. https://man7.org/linux/man-pages/man8/ifconfig.8.html

[41] PFS: Perfect Forward Secrecy. La capacidad de Perfect Forward Secrecy impide que se descifre el contenido de la comunicación, aunque se comprometan las claves establecidas para las asociaciones de seguridad.

D.2 FUNCIONAMIENTO DE WIREGUARD: CRYPTOKEY ROUTING

276. El principio fundamental de una VPN segura es la asociación entre los clientes y la dirección IP que tienen permitido usar dichos clientes como dirección IP origen. En WireGuard los clientes son identificados estrictamente a través de su llave pública (32-byte Curve25519) y asociados a un conjunto de direcciones IP origen permitidas.

277. Para mantener esta asociación existe una tabla que asocia las llaves públicas de los clientes con las direcciones IP de origen permitidas (Cryptokey Routing table).

278. La interfaz del servidor tiene una llave privada y un puerto UDP en el que escucha, seguido de una lista de asociación entre direcciones IP origen y claves públicas

Configuration 1a

Interface Public Key	**Interface Private Key**	**Listening UDP Port**
HIgo...8ykw	yAnz..fBmk	41414
Peer Public Key	**Allowed Source IPs**	
xTIB...p8Dg	10.192.122.3/32, 10.192.124.0/24	
TrMv...WXX0	10.192.122.4/32, 192.168.0.0/16	
gN65..z6EA	10.10.10.230/32	

Figura 23. WireGuard: Tabla Cryptokey Routing

279. Cuando un paquete de salida está siendo transmitido a través de la interfaz de WireGuard hacia un cliente, la ip destino es utilizada para consultar la tabla anterior y determinar con que llave pública se debe realizar el cifrado de los paquetes.

280. En cambio, cuando la interfaz del servidor WireGuard recibe un paquete cifrado, tras descifrarlo y autenticarlo, solo se aceptará si su dirección IP origen coincide en la tabla con la llave pública utilizada en la sesión segura para descifrar el paquete.

D.3 FLUJOS DE COMUNICACIÓN

D.3.1 REALIZACIÓN DE HANDSHAKE

281. En la mayoría de casos el handshake se completa en una sola comunicación de ida y vuelta (1-RTT).

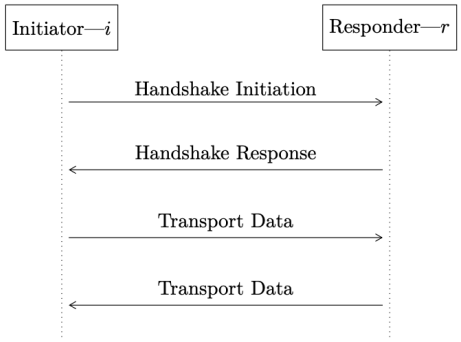


Figura 24. WireGuard: Handshake (1-RTT) en condiciones normales

282. Si una de las máquinas está sobrecargada, se añade un mensaje de respuesta de tipo cookie[42] al proceso de handshake para prevenir ante un ataque de denegación de servicio.

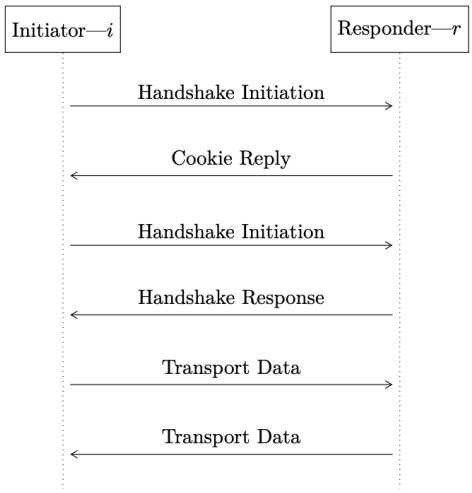


Figura 25. WireGuard: Repetición de handshake por alta carga de CPU

[42] Explicación de los tipos de mensajes en WireGuard en la sección "D.4.4. TIPOS DE MENSAJES"

D.3.2 ENVÍO DE INFORMACIÓN

283. Cuando un paquete es generado localmente (o reenviado) y está listo para ser transmitido pasa a la interfaz virtual de WireGuard (p.ej. wg0).

a) El paquete llega a la interfaz de WireGuard “wg0”.

b) La IP destino es inspeccionada y se comprueba en la tabla “Crypto Routing” si existe alguna llave pública asociada a dicha IP. Si no se encuentra se descarta el paquete y se informa al remitente con un mensaje estándar ICMP “no route to host”.

c) La llave de cifrado de envío simétrico y el nonce[43] de la sesión segura asociado al host de la llave pública son utilizados para cifrar el paquete utilizando ChaCha20Poly1305.

d) Una cabecera con distintos campos especiales del protocolo se añaden al inicio del paquete cifrado.

e) La cabecera y el paquete cifrado se mandan como un paquete UDP/IP al servidor configurado.

D.3.3 RECIBIR INFORMACIÓN

284. Cuando se recibe un paquete por el puerto e interfaz “wg0” configurados por Wireguard:

a) Un paquete UDP/IP que contiene una cabecera particular y el payload cifrado es recibido en el puerto correspondiente.

b) Usando la cabecera, WireGuard determina si el paquete está asociado con la sesión segura del cliente, comprueba la validez del contador del mensaje e intenta autenticarlo y descifrarlo utilizando la clave simétrica de recepción de la sesión segura. Si no puede determinar el cliente asociado o si la autenticación falla, el paquete se descarta.

c) Cuando el paquete ha sido correctamente autenticado, la dirección IP de salida del paquete UDP/IP recibido se utiliza para actualizar la información del cliente asociado.

d) Una vez el contenido del paquete ha sido descifrado, la interfaz tiene el contenido del paquete en texto claro. Si no es un paquete IP, es descarta. En caso contrario, WireGuard comprueba si la IP origen del paquete descifrado está en la lista de direcciones IP permitidas asociadas a la clave pública con la que el paquete ha sido descifrado. Si la IP no se encuentra entre las permitidas el paquete se descarta.

e) Si el paquete no ha sido descartado previamente, se inserta en la cola de paquetes recibidos de la interfaz wg0.

[43] Nonce: Es un valor arbitrario de un solo uso, utilizado en criptografía.

D.4 PROTOCOLO Y CRIPTOGRAFÍA

285. Para empezar a mandar paquetes cifrados y encapsulados, se realiza un handshake de una sola comunicación (1-RTT) usando el patrón IK del framework Noise. Se hace uso de una cookie para mitigar la posibilidad de ataques de denegación de servicio.

286. El handshake puede ser procesado de manera asíncrona:

    a) Cumple con los requisitos de seguridad de AKE (Authenticated Key Exchange).

    b) Evita la suplantación mediante llaves comprometidas.

    c) Evita los ataques de reinyección de mensajes.

    d) Provee de Perfect Forward Secrecy (PFS).

    e) Oculta la indentidad las llaves públicas.

    f) Es resistente a ataques de denegación de servicio.

D.4.1 EL SILENCIO COMO VIRTUD

287. Por diseño, WireGuard evita almacenar estados previos a la autenticación de los paquetes y no responde a los paquetes que no hayan sido autenticados, se evitan así diversos tipos de ataques. Debido a lo anterior, WireGuard es invisible para clientes ilegitimos y escáneres de red.

288. Para evitar ataques de reinyección de paquetes, se incluye un timestamp (12-bytes TAI64N[44]) o un número de 96 bits en el primer paquete del iniciador, cifrado y autenticado. El servidor mantiene el timestamp más reciente de peer y requiere que estos sean monotónicamente crecientes.

    a) No se deben reusar llaves privadas entre peers.

    b) En caso de compromiso de las llaves estas no pueden ser usadas para suplantar la identidad de un usuario debido al proceso de autenticación de las llaves de ambos peers mediante Diffie-Hellman. Una llave robada podría falsificar el mensaje de iniciación pero no completar el handshake. Esto provocaría a su vez la imposibilidad del usuario legítimo a continuar usando su llave, ayudando así a la detección de la suplantación.

[44] TAI64N: Una etiqueta que referencia a un nanosegundo del tiempo real (Tiempo atómico internacional). https://cr.yp.to/libtai/tai64.html

D.4.2 MODO OPCIONAL DE PRE-SHARED KEY SIMÉTRICAS

289. WireGuard se basa en que los pares intercambian las claves públicas estáticas entre si como identidades estáticas. El secreto de todos los datos enviados se basa en la seguridad de la función ECDH Curve25519.

290. WireGuard puede emplear opcionalmente un modo de cifrado en el que mediante una clave simétrica precompartida de 256 bits se consigue una capa de cifrado adicional. Si un atacante logra capturar suficiente tráfico y en un futuro, con ayuda de la computación cuántica, consiguiera romper el cifrado de Curve25519 la clave simétrica usada ya habrá sido modificada. A corto plazo, si esta clave simétrica es comprometida, el cifrado de Curve25519 proveería de protección suficiente.

D.4.3 MITIGACIÓN DE ATAQUES DE DENEGACIÓN DE SERVICIO Y COOKIES

291. Para evitar ataques de denegación de servicio por consumo exhaustivo de CPU el receptor puede optar por no procesar el handshake original y responder con un mensaje con una cookie que el iniciador deberá usar para reenviar el mensaje de handshake.

292. La cookie se calcula con la IP del iniciador más una valor secreto aleatorio que cambia cada dos minutos. El iniciador usará la cookie como clave MAC para crear un hash del paquete. El receptor, en condiciones de sobrecarga puede optar por no procesar este mensaje si la autenticación MAC no es válida. Al usar la IP de origen en este proceso se puede validar el propietario del paquete y limitar el número de paquetes recibidos.

D.4.4 TIPOS DE MENSAJES

293. Existen cuatro tipos de mensajes, cada uno prefijado mediante un byte.

a) **Iniciador del handshake:** El primer mensaje que manda el cliente al servidor para iniciar el proceso de handshake para establecer la sesión segura.

type := 0x1 (1 byte)	reserved := 0^3 (3 bytes)
sender := I_i (4 bytes)	
ephemeral (32 bytes)	
static ($\widehat{32}$ bytes)	
timestamp ($\widehat{12}$ bytes)	
mac1 (16 bytes)	mac2 (16 bytes)

Figura 26. WireGuard: Paquete iniciador de handshake

b) **Respuesta del handshake:** La respuesta que manda el servidor al mensaje iniciador para terminar el handshake, tras el cual se establece la sesión segura.

type := 0x2 (1 byte)	reserved := 0^3 (3 bytes)
sender := I_r (4 bytes)	receiver := I_i (4 bytes)
ephemeral (32 bytes)	
empty ($\widehat{0}$ bytes)	
mac1 (16 bytes)	mac2 (16 bytes)

Figura 27. WireGuard: Paquete de respuesta de handshake

c) **Mensaje con valor "Cookie":** Cuando cualquiera de los mensajes involucrados en el proceso de handshake (iniciador o respuesta) son rechazados, se envía un mensaje con un valor de cookie cifrado que debe ser usado al reenviar el mensaje que haya sido rechazado.

type := 0x3 (1 byte)	reserved := 0^3 (3 bytes)
receiver := $I_{m'}$ (4 bytes)	
nonce := ρ^{24} (24 bytes)	
cookie ($\widehat{16}$ bytes)	

Figura 28. WireGuard: Paquete con valor cookie

d) **Mensaje con datos:** Un paquete IP cifrado y encapsulado que usa la sesión segura negociada por el handshake.

type := 0x4 (1 byte)	reserved := 0^3 (3 bytes)
receiver := $I_{m'}$ (4 bytes)	
counter (8 bytes)	
packet ($\widehat{\|P\|}$ bytes)	

Figura 29. WireGuard: Paquetes de datos

D.5 RENDIMIENTO

294. Pruebas de rendimiento realizada junto a IPSec (Configurado de dos modos) y Open VPN, utilizando iperf3.

295. Comunicación realizada entre una maquina con Intel Core i7-3820QM con tarjeta de red Gibabit Intel 82579LM y una maquina con Intel Core i7-5200U con tarjeta de red Gibabit Intel I218LM.

Protocol	Configuration
WireGuard	256-bit ChaCha20, 128-bit Poly1305
IPsec #1	256-bit ChaCha20, 128-bit Poly1305
IPsec #2	256-bit AES, 128-bit GCM
OpenVPN	256-bit AES, HMAC-SHA2-256, UDP mode

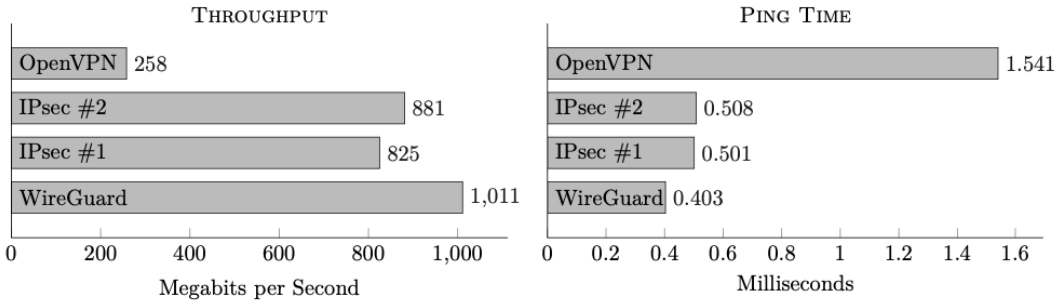


Figura 30. WireGuard: Comparativa de rendimiento con IPSec y OpenVPN

D.6 VERIFICACIONES FORMALES

296. WireGuard ha pasado por numerosas verificaciones formales que cubre aspectos de criptografía, protocolo e implementación. Entre las verificaciones formales se encuentran las siguientes:

   a) Symbolic Verification of Protocol using Tamarin[45].

   b) Computational Proof of Protocol in eCK Model[46].

   c) Computational Proof of Protocol in ACCE Model[47].

   d) Symbolic Verification of Protocol using ProVerif[48].

   e) Verified C Implementation of Curve25519 (HACL[49] & Fiat-Crypto[50]).

[45] Symbolic Verification of Protocol using Tamarin: https://www.wireguard.com/papers/wireguard-formal-verification.pdf

[46] Computational Proof of Protocol in eCK Model: https://www.wireguard.com/papers/dowling-paterson-computational-2018.pdf

[47] Computational Proof of Protocol in ACCE Model: https://www.wireguard.com/papers/lipp-computational-2018.pdf

[48] Symbolic Verification of Protocol using ProVerif: https://www.wireguard.com/papers/kobeissi-bhargavan-noise-explorer-2018.pdf

[49] Verified C Implementation of Curve25519 (HACL): https://www.wireguard.com/papers/zinzindohoue-bhargavan-protzenko-beurdouche-hacl-2017.pdf

[50] Verified C Implementation of Curve25519 (Fiat-Crypto): https://www.wireguard.com/papers/erbsen-philipoom-gross-sloan-chlipala-fiat-2019.pdf

ANEXO E. GLOSARIO DE TÉRMINOS

- **AH** (*Authentication Header*). Protocolo de seguridad empleado en IPsec, que provee integridad para los datos y cabeceras del paquete, pero no provee confidencialidad (cifrado) de datos.
- **Appliance.** Es un dispositivo físico dedicado específicamente a realizar una función concreta. Está diseñado y dimensionado para la ejecución de esa función específica. No es necesario instalarle ningún software, porque ya viene precargado con el software del fabricante para realizar esa función.
- **Autenticación.** Es el proceso de confirmar que algo (o alguien) es quien dice ser. A la parte que se identifica se le llama *probador*. A la parte que verifica la identidad se la llama *verificador*. Cuando los dos participantes en una comunicación se autentican entre sí, se llama autenticación mutua.
- **Autenticación de origen** *(data origin Authentication).* Propiedad que permite al receptor verificar que el mensaje no ha sido alterado en el tránsito (integridad de datos) y que ha sido originado del emisor legítimo (autenticidad).
- **Autenticidad.** Propiedad o característica consistente en que una entidad es quien dice ser o bien que garantiza la fuente de la que proceden los datos.
- **Cliente VPN**: equipo terminal perteneciente a un 'usuario remoto' desde el que se establece la VPN entre el mismo y un concentrador VPN.
- **Concentrador VPN**. También denominado servidor, terminador o *gateway* VPN, es el elemento de red encargado de la creación o terminación de una (o varias) VPN. Se ubica por lo tanto en el extremo de la comunicación y es el encargado de realizar la encapsulación / des encapsulación y cifrado / descifrado del tráfico a través de la VPN y de darle validez en la red local.
- **Confidencialidad**. Propiedad o característica consistente en que la información ni se pone a disposición, ni se revela a individuos, entidades o procesos no autorizados.
- **Disponibilidad**. Propiedad o característica de los activos consistente en que las entidades o procesos autorizados tienen acceso a los mismos cuando lo requieren.
- **Dominios de seguridad**. Conjunto de usuarios y sistemas sujetos a requisitos de seguridad comunes. Unos ejemplos de dominios de seguridad serían: Dominio de Uso Público, Dominio Difusión limitada, Dominio Confidencial.
- **DMZ** *(Demilitarized Zone).* Zona segura que se ubica entre la red interna de una organización y una red externa, generalmente Internet. Su objetivo es que las conexiones desde la red interna y la externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ solo se permitan a la red externa.
- **ESP** (*Encapsulating Security Payload*). Protocolo de seguridad empleado en IPsec que provee tanto integridad, como confidencialidad (cifrado) a los datos, pero no a las cabeceras.

- **GRE** (*Generic Routing Encapsulation*). Protocolo que permite encapsular una amplia variedad de tipos de protocolos diferentes dentro de túneles IP, creando una red punto a punto entre dos máquinas que estén comunicándose por este protocolo. Su uso principal es crear túneles VPN. Se define en la RFC 2784.
- **IKE** (*Internet Key Exchange*). Protocolo de seguridad empleado en IPsec para: (1) negociar la configuración de la conexión, (2) autenticación mutua de origen y destino, (3) definición de los parámetros de seguridad de la conexión, (4) intercambio de las claves de sesión y (5) gestionar, actualizar y finalizar el canal de comunicación.
- **L2TP** *(Layer 2 Tunneling Protocol).* Protocolo de nivel de enlace utilizado para soportar VPN. Inicialmente fue creado como sustituto de PPTP y L2F para corregir las deficiencias de estos protocolos, y establecerse como un estándar aprobado por el IETF (*Internet Engineering Task Force*). Está definido en la RFC 2661.
- **L2F** *(Layer 2 Forwarding).* Protocolo de nivel de enlace diseñado por Cisco, utilizado para soportar VPN. Está definido en la RFC 2341.
- **Integridad.** Propiedad o característica consistente en que el archivo de información no ha sido alterado de manera no autorizada.
- **MAC** (*Message Authentication Code*). Información utilizada para autenticar un mensaje, es decir, para confirmar que el mensaje provenía del remitente declarado (su autenticidad) y no ha sido cambiado en tránsito (su integridad).
- **MPPE** (*Microsoft Point-to-Point Encryption*). Versión Microsoft de un mecanismo de cifrado para utilizar en las implementaciones del protocolo PPTP para VPN.
- **MS-CHAP** (*Microsoft CHAP*). Versión *Microsoft* del protocolo CHAP (*Challenge-Handshake Authentication Protocol*). Se emplea como una opción de autenticación en las implementaciones Microsoft del protocolo PPTP para VPN.
- **NAT** (*Network Address Translation*). Es una función empleada por los dispositivos de red (normalmente por enrutadores), que consiste en la modificación en tiempo real de las direcciones IP de los paquetes. Está diseñada para simplificar y conservar direcciones IP. Permite que las redes IP privadas que usan direcciones IP no registradas puedan conectarse a Internet, traduciendo las direcciones privadas (no universalmente únicas) de la red interna, en direcciones legales antes de reenviar paquetes a otra red.
- **Nonces**. Es un valor arbitrario de un solo uso, utilizado en criptografía. Normalmente es un número aleatorio o pseudo-aleatorio que se utiliza en los protocolos de autenticación, para evitar el empleo de paquetes antiguos de la comunicación en ataques de reenvío (*replay attacks*). También se utilizan como vectores de inicialización (IV) en funciones hash criptográficas.
- **OSI** *(Open Systems Interconnection).* Modelo de referencia para los protocolos de la red de arquitectura en capas, creado en el año 1980 por la Organización Internacional de Normalización (ISO, *International Organization for Standardization*).

- **Payload**. Como parte de los paquetes en los que se divide un mensaje para ser enviado a través de un canal de comunicación, el *Payload* es la parte del paquete que representa los datos. Es decir, el *Payload* son únicamente los datos cuyo envío ha originado la comunicación, y no la información de cabeceras o metadatos que se añade al paquete para su envío a través de los canales de transmisión.
- **PPP** (*Point-to-Point Protocol*). Protocolo de nivel de enlace empleado para establecer una conexión directa entre dos nodos, sin necesidad de ningún dispositivo de red intermedio. Provee mecanismos de seguridad como autenticación, cifrado y compresión. Está definido en la RFC 1661.
- **PPTP** (*Point-to-Point Tunneling Protocol*). Protocolo de nivel de enlace utilizado para soportar VPN, sobre protocolo PPP. Utiliza un canal de control sobre TCP, y protocolo GRE para implementar el túnel en el que se encapsulan los datos. Está definido en la RFC 2637.
- **Rendimiento.** Medida o cuantificación de la velocidad con que se realiza una tarea o proceso en un dispositivo. No depende sólo del microprocesador, sino de la suma de sus componentes como la memoria, el bus, los diversos dispositivos, etc. y su software.
- **SSH** *(Secure Shell)*. Protocolo de nivel de aplicación que permite acceder de forma remota, a servidores y otros equipos de forma segura.
- **SSL/TLS** *(Secure Socket Layer/Transport Layer Security)*. Protocolo que proporcionan servicios de seguridad a las comunicaciones a través de Internet. Impide que ciertas actividades maliciosas tengan éxito, como escuchas (*eavesdroping*), manipulación (*tampering*) o falsificación de mensajes.
- **TCP/IP** *(Transmission Control Protocol/Internet Protocol).* Protocolos de red que respaldan a Internet y que hacen posible la transferencia datos entre redes.
- **Tunelización dividida** (*Split tunneling*). Concepto utilizado en redes de ordenadores mediante el cual, se permite a usuarios remotos el acceso simultáneo a redes en diferentes dominios de seguridad utilizando la misma o diferentes conexiones de red. Por ejemplo, acceso simultáneo a la red de área local de la organización a través de una VPN, y a Internet.
- **Usuarios Remotos**. Aquellos usuarios que por necesidades laborales requieren el acceso remoto a los recursos internos de la organización, empleando la infraestructura de un tercero como soporte de comunicaciones (generalmente Internet).
- **VPN de Acceso remoto**. Es la empleada para proteger las comunicaciones entre un equipo individual de usuario y la red interna de la organización. Normalmente se emplean para a los usuarios que trabajan desde casa o que están de viaje, y que requieren de un acceso a los recursos internos de la organización, a través de la infraestructura proporcionada por una red pública, como por ejemplo Internet.

- **VPN local**. Es la empleada para establecer un nivel adicional en las comunicaciones entre dos servidores situados incluso en la misma red local. Típicamente este escenario se presenta en redes con riesgos de seguridad, como la DMZ en la que se encuentran los distintos servidores expuestos en Internet.
- **VPN de sitio a sitio**. Es la empleada para proteger las comunicaciones entre dos redes de la organización (por ejemplo, una sede secundaria con la sede principal), a través de una red pública, como por ejemplo Internet, manteniendo la seguridad y enrutando las comunicaciones.

ANEXO F. REFERENCIAS

[1] RFC 5280 - Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Mayo 2008.

[2] RFC 4253 The Secure Shell (SSH) Transport Layer Protocol.

[3] Guía CCN-STIC-807 - Criptografía de empleo en el Esquema Nacional de Seguridad.

[4] RFC 7568 - Deprecating Secure Sockets Layer Version 3.0.

[5] RFC 5246 - The Transport Layer Security (TLS) Protocol Version 1.2.

[6] RFC 7919 - Negotiated Finite Field Diffie-Hellman Ephemeral Parameters for Transport Layer Security (TLS), Agosto 2016.

[7] RFC 3173 IP Payload Compression Protocol (IPComp).

[8] RFC 4302 - IP Authentication Header (AH).

[9] RFC 4303 - IP Encapsulating Security Payload (ESP).

[10] RFC 7296 - Internet Key Exchange Protocol Version 2 (IKEv2).

[11] RFC 3715 - IPsec-Network Address Translation (NAT) Compatibility Requirements.

[12] RFC 4301 - Security Architecture for the Internet Protocol.

[13] RFC 5288 - AES Galois Counter Mode (GCM) Cipher Suites for TLS.

[14] RFC 6655 - AES-CCM Cipher Suites for Transport Layer Security (TLS).

[15] RFC 7251 - AES-CCM Elliptic Curve Cryptography (ECC) Cipher Suites for TLS.

[16] RFC 8446 - The Transport Layer Security (TLS) Protocol Version 1.3, Agosto 2018.

[17] «Instrucciones de instalación de OpenVPN,» [En línea]. Available: https://openvpn.net/community-resources/how-to/.

[18] «Ethernet Bridging,» [En línea]. Available: https://openvpn.net/community-resources/ethernet-bridging/.

[19] CCN-STIC-130 Requisitos de Aprobación de Productos de Cifra para Manejar Información Nacional Clasificada..


PUBLICACIONES
Pd
DE DEFENSA


GOBIERNO
DE ESPAÑA
MINISTERIO
DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL
DE PUBLICACIONES
Y PATRIMONIO CULTURAL