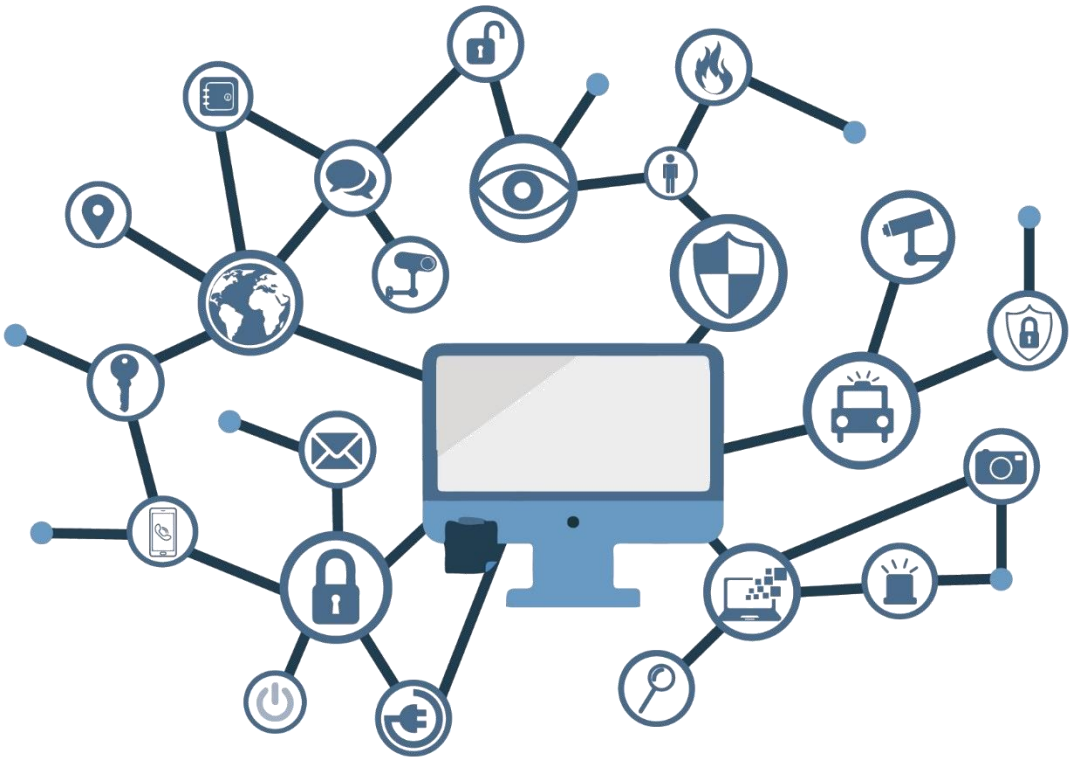
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC - Anexo D8.A: VPN IPSec



Junio 2021

MINISTERIO DE DEFENSA

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
2021.06.23 16:41:34 +02'00'

NIPO: 083-21-130-1

Fecha de Edición: Junio 2021

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

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Dispositivos/Herramientas para redes privadas virtuales (VPN[1])** para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación (CPSTIC), publicado por el CCN.
2. Estos requisitos representan las capacidades de seguridad mínimas que cualquier producto dentro de esta familia debe implementar para un determinado caso de uso, independientemente del fabricante y la tecnología, con el fin de proporcionar un nivel mínimo de confianza y considerarse objetivamente cualificado desde el punto de vista de la seguridad para ser empleado en los sistemas de información del sector público a las que sea de aplicación el Esquema Nacional de Seguridad (ENS). Estos requisitos aportan mecanismos enfocados a reducir vulnerabilidades y contrarrestar amenazas, fundamentalmente de carácter técnico, aunque también pueden ser de naturaleza física o procedimental.
3. Además, la aplicación de estos criterios permitirá:
   - Que se establezcan unas características mínimas de seguridad que sirvan de referencia a los **fabricantes** a la hora de desarrollar nuevos productos STIC.
   - Que los **organismos responsables de la adquisición** dispongan de evaluaciones completas, consistentes y técnicamente adecuadas, que permitan contrastar la eficacia y proporcionar información no sesgada acerca de los servicios de seguridad que ofrecen dichos productos.
   - Que los **usuarios finales** posean una guía que facilite el despliegue y garantice el uso apropiado del producto desde el punto de vista de la seguridad.
4. Por lo tanto, los productos catalogados dentro de la familia **Dispositivos/Herramientas para redes privadas virtuales** (**VPN**) conforme a la taxonomía definida por el Centro Criptológico Nacional, serán susceptibles de ser evaluados usando como referencia este documento.
5. En el caso de productos multipropósito, queda fuera del alcance de este documento cualquier otra funcionalidad de seguridad proporcionada, más allá de la especificada para esta familia en la sección siguiente. Dichos productos podrían optar a ser incluidos de manera adicional como Productos Cualificados en otra(s) familia(s) del CPSTIC si cumpliesen los RFS correspondientes.

[1] *Virtual Private Network*

2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS

2.1 FUNCIONALIDAD

6. Los productos asociados a esta familia están orientados a la protección de la confidencialidad e integridad de la información cuando atraviesa redes no confiables. Esto se consigue estableciendo canales protegidos criptográficamente -**túneles VPN (*Virtual Private Network*)-** entre los extremos de la comunicación que se quiere proteger -dispositivos VPN- y encaminando el tráfico de red entre ambos lados del túnel VPN.

7. Las formas más habituales en las que se utiliza esta familia de productos son las siguientes:

   - **VPN punto a punto.** Se usa habitualmente para conectar un sitio con uno o más sitios remotos, como por ejemplo para conectar la sede central de una organización con varias sucursales.

   - **VPN de acceso remoto.** Se usa habitualmente para conectar a través de Internet a usuarios remotos con la red de la organización para que puedan utilizar los recursos internos de la organización. También se puede usar para conectar pequeñas oficinas remotas o empleados trabajando desde casa, con la red de la organización.

8. Para ello, estos dispositivos proporcionan ciertas funciones básicas de seguridad:

   - Integridad de los datos enviados y recibidos a través de la VPN.
   - Confidencialidad de los datos enviados y recibidos a través de la VPN.
   - Autenticación de los dispositivos/usuarios que establecen la conexión de la VPN.
   - Control de acceso, restringiendo el acceso solo a usuarios/dispositivos autorizados y solo a los datos/redes a los que estén autorizados.

9. Algunos productos cliente o servidor de VPN implementan funcionalidades avanzadas de seguridad fuera de lo que se considera propiamente una VPN, como por ejemplo módulos de cortafuegos, o filtrado anti-malware. El presente documento no cubre estos aspectos. En caso de que se quisiese hacer uso de estas funcionalidades, el producto debería incluir en su certificación los RFS definidos para esas familias.

2.2 CASOS DE USO

10. Se contemplan dos casos de uso para esta familia de productos: las VPN punto a punto y las VPN de acceso remoto.

2.2.1. CASO DE USO 1 - VPN PUNTO A PUNTO

11. Las VPN punto a punto permiten interconectar de forma segura dos redes a través de una tercera red no confiable. Esta forma de uso requiere de dos dispositivos **servidores VPN** (también llamados VPN *gateways,* terminadores o concentradores de VPN), uno en cada sitio que se quiera conectar.
12. Ambos servidores, que en la mayoría de los casos serán dispositivos hardware, contarán con unas características de seguridad similares:
    - Autenticación de los VPN Gateway.
    - Control de acceso, restringiendo el acceso solo a personas/dispositivos autorizados y solo a los datos/redes a los que estén autorizados.
    - Cifrado de comunicaciones.
13. Un ejemplo de este caso de uso serían dos sedes de una misma organización conectadas a través de Internet, tal como se muestra en la figura. Tanto la sede central de la organización como cada una de las redes tendrían su dispositivo servidor VPN.

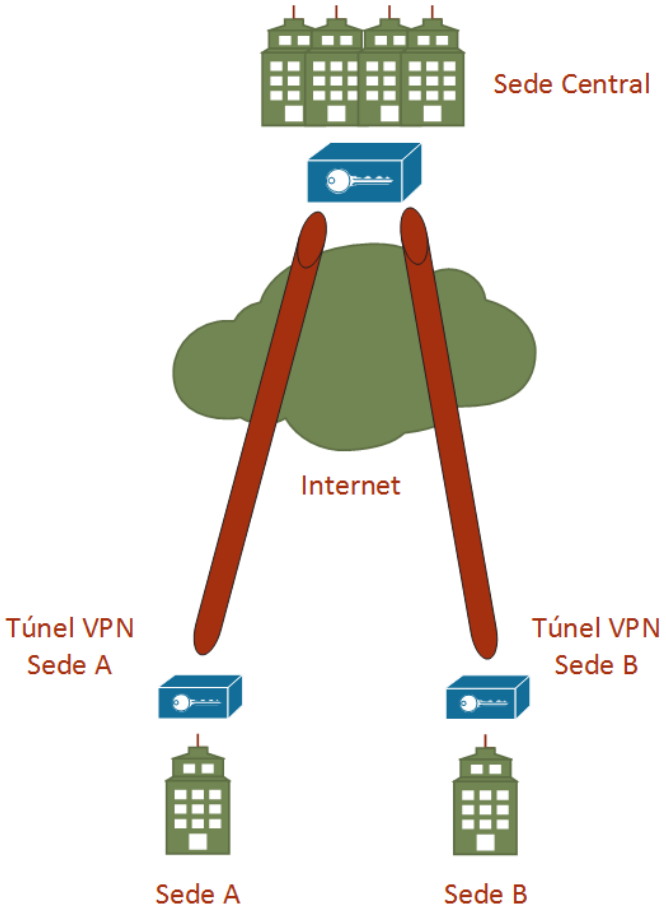


Figura 1 – Ejemplo de Caso de Uso 1: VPN Punto a Punto

2.2.2. CASO DE USO 2 – VPN DE ACCESO REMOTO

14. Las VPN de acceso remoto se usan habitualmente para conectar de forma segura a través de una red no confiable (por ejemplo, Internet) a usuarios remotos de una organización con la red de ésta, con la finalidad de que puedan utilizar sus recursos internos.

15. Esta configuración requiere de dos dispositivos, uno instalado en la red organización y otro en el lado del usuario remoto:

    - Dispositivo en la organización: Suele ser un dispositivo hardware, normalmente denominado concentrador de VPN o VPN *Gateway*, que conecta de forma segura la red de la organización con los clientes VPN.
    - Dispositivo en el usuario remoto: Suele ser un dispositivo software (p. ej. Empleados conectándose remotamente con un portátil mediante un software cliente VPN). Conecta de forma segura a los ordenadores o dispositivos cliente (p.ej. ordenadores o teléfonos inteligentes (*Smartphones)* de empleados que trabajan en ubicaciones remotas) con las redes de la organización.

16. Algunos ejemplos de funcionalidades de seguridad específicas de los clientes VPN son las siguientes:

    - Cifrado de la información.
    - Autenticación de los VPN Gateway y los productos cliente VPN.
    - Autenticación de los usuarios y/o sus dispositivos.
    - Control de acceso a recursos e información basado en roles de usuario o equipo móvil.
    - Funcionalidades de seguridad añadidas como, por ejemplo, controles para que el equipo móvil no esté conectado a la vez a la red de la organización (a través de la VPN) y a otras redes.

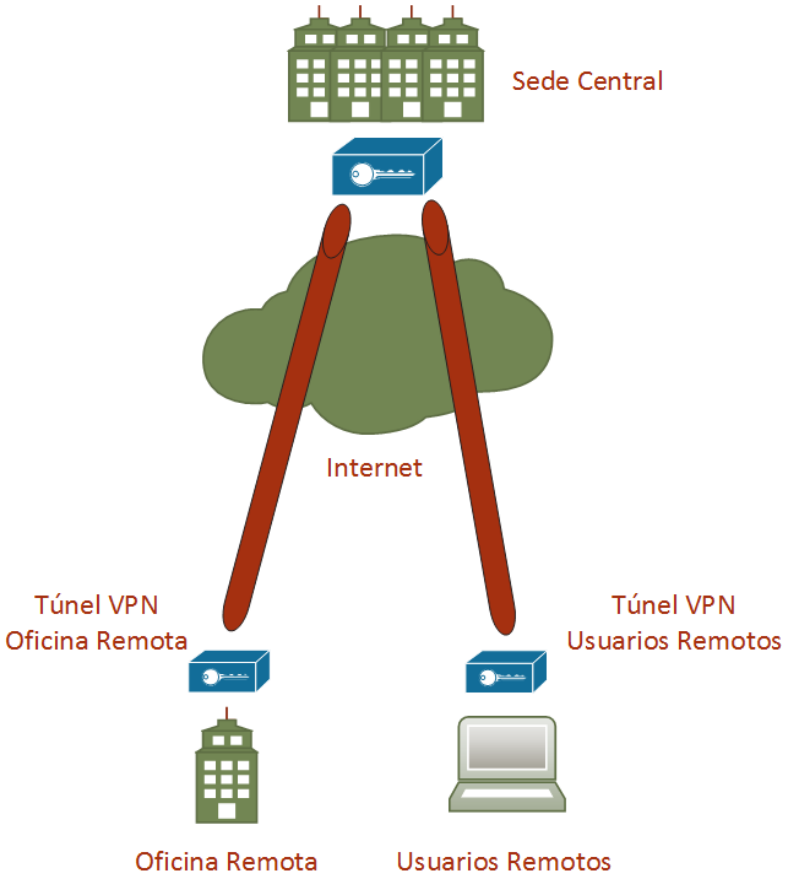


Figura 2 – Ejemplo de Caso de Uso 2: VPN de Acceso Remoto

2.3 ENTORNO DE USO

17. Por lo general, este tipo de dispositivos se encuentran en grandes o medianas empresas, así como en redes del sector público, como parte de una arquitectura de defensa en profundidad, en combinación con medidas complementarias en diferentes capas de protección.

18. Para la utilización en condiciones óptimas de seguridad de las VPN,es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Administración confiable**: El usuario administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Por ello se asume que dicha persona estará altamente capacitada y carecerá de cualquier intención dañina al administrar productos VPN.
    - **Protección de las credenciales**: Todas las credenciales, en especial la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.
    - **Política de seguridad de la información**: Una política de seguridad deberá recoger el conjunto de principios, organización y procedimientos impuestos

por una organización para hacer frente a sus necesidades de seguridad de la información, incluyendo el uso de las TIC.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

19. Típicamente los servidores VPN se presentan en formato **Equipo dedicado o (*Appliance*: hardware provisto de firmware dedicado)** con las funcionalidades necesarias para cumplir su finalidad y acotadas al servicio específico que presten. Los requisitos aplicables a estos productos se recogen en la sección 4 REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS) PARA SERVIDORES VPN.
20. Adicionalmente, los clientes VPN se suelen presentar en formato Software instalable en un equipo informático estándar (p.ej. en el ordenador portátil de un empleado).Los requisitos aplicables a estos productos se recogen en la sección 5 REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS) PARA CLIENTES VPN.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

21. El estándar *Common Criteria* (CC) proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TIC (Tecnologías de la Información y de las Comunicaciones).
22. En el ámbito de CC se elaboran unos perfiles de seguridad que definen, para un dominio o categoría de productos, un conjunto de objetivos y requisitos de seguridad, tanto funcionales como de evaluación, independientes de la implantación.
23. Los productos dentro de esta familia deberán estar certificados de acuerdo a la norma *Common Criteria*. Dicha certificación deberá evidenciar el problema de seguridad definido en el presente documento e incluir los requisitos fundamentales de seguridad recogidos en el apartado 4.
24. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será:
    - **El determinado por el perfil de protección** para aquellos SFR incluidos en los perfiles exigidos cuando los productos se encuentren certificados contra alguno de los perfiles anteriormente descritos.
    - **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra ningún perfil.
25. En caso de que alguno de los requisitos indicados en el apartado 4 no se encuentre recogido en la declaración de seguridad del producto, pero este sí implemente esa función de seguridad, se podrá llevar a cabo una **evaluación STIC complementaria**, cuyo objetivo será verificar el cumplimiento de esos requisitos.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

26. Los recursos que es necesario proteger mediante el uso de esta familia de productos, incluyen:

    - Información que atraviese el producto entre sus interfaces de red interna y externa en el caso de las *Gateways*, o entre el sistema cliente de la VPN y la red externa, en ambos sentidos.
    - Información que atraviese el túnel VPN.
    - Claves criptográficas utilizadas para proteger el canal de comunicaciones.
    - Información sobre la topología de las redes y sistemas conectados mediante el túnel VPN.
    - Datos de configuración del producto y de auditoría generados por éste.
    - Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

27. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente, atendiendo a los casos de uso expuestos en la sección 2.2 serían:

    - **Acceso no autorizado externo:** Un atacante desde la red externa (no confiable) consigue acceder/modificar/eliminar a información intercambiada a través del túnel VPN o utilizar el producto como mecanismo de acceso a la red interna.
    - **Acceso no autorizado interno:** Acceso desde una red interna (conectada por VPN) a recursos para los que no se cuenta con autorización de acceso y/o necesidad de conocer en otras redes internas (conectadas por la VPN).
    - **Divulgación de información:** Si la VPN permite obtener información sobre las redes y/o sistemas internos, esta información podría ser utilizada por un atacante.
    - **Propagación de virus y malware:** Propagación de virus y malware entre las distintas redes/sistemas conectados por la VPN.
    - **Conexión de equipos no autorizados:** En el caso de los clientes VPN, conexión de equipos no autorizados a las redes internas a través de un túnel VPN.
    - **Cifrado débil:** Utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.

- **Uso de canales de comunicación inseguros:** Mala implementación de protocolos estándar (p.ej. IPSec[2]) o utilización de protocolos no estandarizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones del dispositivo.

[2] *Internet Protocol Security*

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS) PARA SERVIDORES VPN

28. A continuación se recogen los requisitos que debe cumplir el dispositivo que actúe como Servidor VPN (también llamados terminadores VPN o VPN *Gateway*).

29. Este apartado debe utilizarse para dispositivos utilizados en los siguientes casos de uso:

    - VPN punto a punto.
    - VPN de acceso remoto.
        - Cuando se usa un dispositivo para conectar pequeñas oficinas con la red de la organización.

30. La información relativa a los requisitos para los programas software, que actúan como cliente en el caso de uso VPN de acceso remoto, no queda cubierta por este apartado.

4.1 PERFIL DE PROTECCIÓN COMMON CRITERIA

1. **REQ. 1** Los productos deberán estar certificados con uno de los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria:*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Devices[3]	2.2e	27/03/2020	CCDB
Collaborative Protection Profile for Network Devices[4]	2.1	24/09/2018	CCDB
Collaborative Protection Profile for Network Devices[5]	2.0 + Errata 20180314	14/03/2018	CCDB
Collaborative Protection Profile for Network Devices.6	1.0	27/02/2015	CCDB

Tabla 2. Perfiles de protección

2. **REQ.2.** En caso de que el producto no esté certificado contra ninguno de los perfiles anteriores, la declaración de seguridad deberá contener al menos los

[3] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.2E.pdf
[4] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.1.pdf
[5] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.0E.pdf
[6] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf

SFR (*Security Functional Requirements*) de *Collaborative Protection Profile for Network Devices V.2.2e* con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

3. **REQ. 2** Serán obligatorios los SFR FMT_MOF.1/AdminAct y FMT_MTD.1/AdminAct.

4.2 CONTROL DE LOS FLUJOS DE INFORMACIÓN

4. **REQ. 3** El producto dispondrá de al menos un interfaz de red para la conexión de red interna y otro diferente para la conexión con la red externa.
5. **REQ. 4** El producto permitirá establecer periodos de validez y ventanas de tiempo para los túneles. Si expiran, se cancelará la comunicación.
6. **REQ. 5** El producto deberá tener la capacidad de procesar e inspeccionar paquetes de los siguientes protocolos de red: IPv4[7], IPv6[8], TCP[9], UDP[10], de forma que se permita:
    a) Definir reglas de filtrado de paquetes en función de las direcciones origen y destino, puertos origen y destino o interfaz.
    b) Utilizar las siguientes operaciones básicas de filtrado: permitir, denegar y guardar en el registro de actividad (*logs*).
    c) Asignar reglas a interfaces de red del producto en el orden establecido por el administrador.
7. **REQ. 6** El producto deberá utilizar IPsec para establecer un canal de comunicaciones seguro entre él y las entidades autorizadas para las comunicaciones VPN. Este canal será lógicamente distinto de otros canales de comunicaciones y proveerá identificación segura extremo a extremo y protección de confidencialidad e integridad de la información.
8. **REQ. 7** El producto deberá utilizar IPsec, TLS[11], TLS/HTTPS para establecer un canal de comunicaciones seguro entre él y las entidades autorizadas que provean servicios adicionales al de VPN (servidor de auditoría, autenticación, etc.).

4.3 AUDITORÍA Y REGISTROS DE SEGURIDAD

9. **REQ. 8** La gestión de los registros sólo podrá ser realizada por un perfil de usuario privilegiado dedicado (p.ej.: rol de auditor), que será diferente del rol administrador.

[7] *Internet Protocol versión 4*
[8] *Internet Protocol versión 6*
[9] *Transmission Control Protocol*
[10] *User Datagram Protocol*
[11] *Transport Layer Security*

10. **REQ. 9** El dispositivo debe separar el rol auditor de cualquier otro rol en el sistema. El dispositivo no permitirá que una cuenta de usuario administrador pueda tener privilegios de auditor.

4.4 ADMINISTRACIÓN DEL PRODUCTO

11. **REQ. 10** La administración remota sólo podrá ser realizada a través de la interfaz conectada con la red interna o a través de interfaces de administración dedicados (estos interfaces no podrán estar conectados a redes externas).

4.5 PROTECCIÓN DEL DISPOSITIVO Y SUS SERVICIOS

12. **REQ. 11** En el caso en que el producto tenga componentes hardware, éste deberá:
    a) Implementar mecanismos que evidencien el intento de apertura *(tamper-evidence*) ante un intento de acceso no autorizado.
    b) Implementar encapsulado opaco que impida la observación directa o manipulación del módulo criptográfico.
    c) Distinguir lógicamente entre entrada de datos y de control, y salida de datos, control y estado.
    d) Control de integridad
13. **REQ. 12** El producto deberá implementar auto chequeos de arranque, donde se verifique la integridad del software o firmware, los mecanismos criptográficos y de funciones críticas, si procede.
14. **REQ. 13** El producto deberá implementar auto chequeos condicionales: Comprobación de los parámetros de seguridad sensibles (PSS) durante su establecimiento y entrada y salida. Verificación de la integridad y autenticidad del software o firmware durante su carga. Test periódico de los mecanismos criptográficos.
15. **REQ. 14** El producto deberá apagarse en caso de que se detectase un error en los chequeos anteriormente citados.
16. **REQ. 15** El producto permitirá a usuarios autorizados consultar la versión de software/firmware e iniciar actualizaciones de éstos.
17. **REQ. 16** El producto deberá tener la capacidad de verificar las actualizaciones del software/firmware utilizando firma digital con anterioridad a la instalación de estas actualizaciones. Solo permitirá la actualización en el caso de que la verificación de la firma haya sido correcta.

4.6 REQUISITOS CRIPTOGRÁFICOS

18. **REQ. 17** NOTA: Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán

encontrarse dentro de los acreditados por el CCN para su uso en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807.

19. **REQ. 18** Las claves utilizadas por los algoritmos criptográficos empleados por el producto deberán tener **una fortaleza de seguridad de 128 bits o superior**.
20. **REQ. 19** Generador de bits aleatorios. En caso de suministrar un servicio de generación de bits aleatorios (RBG[12]) determinísticos, el producto deberá:
    - Utilizar Hash_DRBG (any), HMAC_DRBG (any) o CTR_DRBG (AES).
21. **REQ. 20** Usar una **semilla** de al menos una fuente de entropía que acumule entropía de varias fuentes o disponer de una fuente de entropía estudiada, con un mínimo de bits de entropía al menos igual a la mayor fortaleza de seguridad de las claves y hashes que generará, de acuerdo a la ISO/IEC 18031:2011.
22. **REQ. 21** Algoritmos HASH. Las funciones resumen o HASH que utilice el producto deberán utilizar los algoritmos SHA-2[13] y SHA-3 de longitud mayor o igual a 256.
23. **REQ. 22** Firma digital. Para los servicios de verificación de firma digital, el producto deberá utilizar uno de los siguientes algoritmos:
    - *Digital Signature Algorithm* (DSA) con una longitud de clave de 3072 bits o superior.
    - *Elliptic Curve Digital Signature Algorithm* (ECDSA) con una longitud de clave de 256 o superior.
    - RSA con una longitud de clave de 3072 o superior.
24. **REQ. 23** Cifrado de datos y claves con AES[14]. El producto implementará cifrado de datos de acuerdo con el algoritmo AES los modos CBC[15], GCM[16], CTR[17] o CCM[18] y longitud de claves 128 bits o superior.
25. **REQ. 24** Autenticación de mensajes. Para los servicios de autenticación de mensajes, el producto podrá utilizar:
    - HMAC-SHA-2 o HMAC-SHA-1[19].
    - AES-XCBC-MAC-96, AES-XCBC-MAC-128.
    - CMAC-AES-96, CMAC-AES-128.
    - GMAC-AES-128.
26. **REQ. 25** El producto deberá implementar los siguientes métodos de borrado de claves:

[12] *Random Bit Generator*
[13] *Secure Hash Algorithm*
[14] *Advanced Encryption Standard*
[15] *Cipher Block Chaining*
[16] *Galois/Counter Mode*
[17] *Counter mode*
[18] *Counter with CBC-MAC*
[19] Solamente para el caso de autenticación de mensajes con HMAC se permitirá el uso de SHA-1.

a. Para memoria volátil, la destrucción podrá ser realizada utilizando los siguientes métodos:
   - Un patrón de sobrescritura de una pasada utilizando un patrón pseudoaleatorio generado por el RBG del producto o algún valor que no contenga ningún parámetro de seguridad crítico (PSC).
   - Destrucción de la referencia a la clave directamente seguida por una llamada al "recolector de basura" de la memoria.

b. Para memoria no volátil:
   - Que emplee un algoritmo de *wear-leveling*, la destrucción deberá consistir en alguno de los siguientes métodos:
     1. Una sola pasada de sobrescritura con un nuevo valor de clave de la misma longitud u otro valor que no contenga ningún PSC.
     2. Borrado de bloque.
   - Que no emplee un algoritmo *wear-leveling*, la destrucción deberá ejecutarse por:
     1. Una o más pasadas de sobrescritura que no contenga ningún CSP seguidos de una lectura de verificación.
     2. Borrado de bloque.

Si la lectura de verificación de los datos sobrescritos falla, el proceso deberá ser repetido de nuevo hasta alcanzar un número N (N>1) de intentos en el cual se devuelva un error.

27. **REQ. 26** Destrucción del material criptográfico. Todos los parámetros intermedios y claves criptográficas serán destruidas cuando finalice su uso, utilizando los métodos de borrado seguro establecidos.
28. **REQ. 27** Todos los procesos de ejecución de mecanismos criptográficos correrán de manera independiente.

4.7 REQUISITOS IPSEC

29. **REQ. 28** Este conjunto de requisitos IPSec especificados en este apartado son prioritarios sobre los requisitos de IPSec especificados en el *Network Devices cPP.*
30. **REQ. 29** El producto deberá implementar la arquitectura IPSEC de acuerdo a lo especificado en la RFC 4301, en modo túnel.
31. **REQ. 30** El producto deberá implementar el protocolo IKEv2 como se define en RFC 7296 con NAT transversal como opción.

32. **REQ. 31** El producto deberá asegurar que el protocolo IKE implementa autenticación extremo a extremo utilizando firma electrónica, con certificados X.509v3, claves previamente compartidas o EAP.
33. **REQ. 32** El producto deberá asegurar que la información cifrada IKEv2 utiliza AES en los modos CBC o GCM.
34. **REQ. 33** El producto deberá asegurar que los tiempos de vida de las asociaciones de seguridad (SA) de los protocolos IKE podrán ser configurados por un administrador en base al número de paquetes, volumen de tráfico y/o tiempo transcurrido.
35. **REQ. 34** El producto deberá asegurar que todos los protocolos IKE implementan al menos un grupo Diffie-Hellman de los siguientes:

Grupo	Nº IANA	RFC
3072-bit MODP GROUP	15	3526
4096-bit MODP GROUP	16	3526
256-bit random ECP GROUP	19	5903
384-bit random ECP GROUP	20	5903
512-bit random ECP GROUP	21	5903
Brainpool P256r1	28	6954
Brainpool P384r1	29	6954
Brainpool P512r1	30	6954

36. **REQ. 35** El producto deberá generar el valor secreto X utilizado en el intercambio de claves *Diffie-Hellman* ("x" en gx mod p) utilizando el RBG especificado y con una longitud de bits de al menos el doble de los "bits de seguridad" asociados con el grupo DH negociado.
37. **REQ. 36** El producto deberá implementar protocolo IPSEC ESP como se define en RFC 4303 utilizando AES junto con algún algoritmo para la autenticación de mensajes.
38. **REQ. 37** El producto deberá generar nonces para el intercambio en IKE. La probabilidad de repetir un nonce durante la vida de una determinada SA IPSec será menor o igual que $1/(2^{128})$.

5. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS) PARA CLIENTES VPN

39. Esta sección cubre los programas (software) utilizados como cliente VPN en las conexiones de acceso remoto, así como las que se utilizan habitualmente para la conexión de equipos móviles a la red de la organización (p. ej. Trabajadores remotos).
40. Este apartado debe utilizarse para dispositivos aplicados en el siguiente caso de uso:

- VPN de acceso remoto:
    - Cuando se utiliza un programa software para conectar a través de internet a usuarios remotos (por ejemplo, empleados trabajando desde casa) con la red de la organización.

41. La información relativa a los requisitos para los dispositivos Servidores VPN (también llamados terminadores VPN o VPN Gateway) no queda cubierta por este apartado.
42. A continuación se recogen los requisitos que debe cumplir el software cliente VPN, tanto generales debidos a funcionalidades comunes con otras tipologías de productos, como específicos para la familia de productos en la que se integra.

5.1 CONTROL DE LOS FLUJOS DE INFORMACIÓN

43. **REQ. 38** La creación, configuración, modificación o eliminación de túneles para la transmisión o recepción de información debe poder ser restringida a usuarios conciertos roles configurables.
44. **REQ. 39** El producto permitirá establecer periodos de validez y ventanas de tiempo para los canales. Si expiran, se cancelará la comunicación.
45. **REQ. 40** El producto deberá utilizar IPSec para establecer un canal de comunicaciones seguro entre él y las entidades IT autorizadas para las comunicaciones VPN. Este canal proveerá identificación segura extremo a extremo y protección de confidencialidad e integridad de la información.
46. **REQ. 41** El producto podrá iniciar la comunicación a través de dicho canal.

5.2 CONTROL DE INTEGRIDAD

47. **REQ. 42** El producto deberá implementar:

- Auto chequeos de arranque, donde se verifique la integridad del software o firmware, los mecanismos criptográficos y de funciones críticas, si procede.

- Auto chequeos condicionales: Comprobación de los parámetros de seguridad sensibles (PSS) durante su establecimiento y entrada y salida. Verificación de la integridad y autenticidad del software o firmware durante su carga. Test periódico de los mecanismos criptográficos.

48. **REQ. 43** El producto deberá cerrarse en caso de que se detectase un error en los chequeos anteriormente citados.
49. **REQ. 44** El producto permitirá a usuarios autorizados consultar la versión de software e iniciar actualizaciones de éstos.
50. **REQ. 45** El producto deberá tener la capacidad de verificar las actualizaciones del software utilizando firma digital con anterioridad a la instalación de estas actualizaciones. Solo permitirá la actualización en el caso de que la verificación de la firma haya sido correcta.

5.3 PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

51. **REQ. 46** El producto debe ser capaz de detectar intentos de acceso indiscriminado al servicio para evitar posibles denegaciones de servicio, a través de cualquier interfaz.
52. **REQ. 47** En caso de fallo de algún componente, el producto debe asegurar que no se incumplen las políticas de seguridad permitiendo flujos de información no autorizados.

5.4 REQUISITOS CRIPTOGRÁFICOS

53. **REQ. 48** NOTA: Todos los algoritmos de cifrado simétrico, asimétrico, protocolos de acuerdo de clave y funciones resumen que utilice el producto deberán encontrarse dentro de los acreditados por el CCN para su uso en el ENS. El listado de dichos algoritmos se encuentra recogido en la CCN-STIC-807.
54. **REQ. 49** Las claves utilizadas por los algoritmos criptográficos empleados por el producto deberán tener una fortaleza de seguridad de 128 bits o superior.
55. **REQ. 50** Generador de bits aleatorios. En caso de suministrar un servicio de generación de bits aleatorios (RBG) determinísticos, el producto deberá:
    - Utilizar Hash_DRBG (any), HMAC_DRBG (any) o CTR_DRBG (AES).
    - Usar una semilla de al menos una fuente de entropía que acumule entropía de varias fuentes o disponer de una fuente de entropía estudiada, con un mínimo de bits de entropía al menos igual a la mayor fortaleza de seguridad de las claves y hashes que generará, de acuerdo a la ISO/IEC 18031:2011.
56. **REQ. 51** Algoritmos HASH. Las funciones HASH que utilice el producto deberán utilizar los algoritmos SHA-2 y SHA-3 de longitud mayor o igual a 256.
57. **REQ. 52** Firma digital: Para los servicios de verificación de firma digital, el producto deberá utilizar uno de los siguientes algoritmos:

- *Digital Signature Algortim* (DSA) con una longitud de clave de 3072 bits o superior.
- *Elliptic Curve Digital Signature Algorithm* (ECDSA) con una longitud de clave de 256 o superior.
- RSA con una longitud de clave de 3072 o superior.

58. **REQ. 53** Autenticación de mensajes. Para los servicios de autenticación de mensajes, el producto podrá utilizar:
    - HMAC-SHA-1[20], HMAC-SHA-2.
    - AES-XCBC-MAC-96, AES-XCBC-MAC-128.
    - CMAC-AES-96, CMAC-AES-128.
    - GMAC-AES-128.
59. **REQ. 54** Cifrado de datos y claves con AES. El producto implementará cifrado de datos y claves de acuerdo con el algoritmo AES los modos CBC, GCM, CTR o CCM y longitud de claves 128 bits o superior.
60. **REQ. 55** El producto deberá implementar los siguientes métodos de borrado de claves:
    - Para memoria volátil, la destrucción podrá ser realizada utilizando los siguientes métodos:
        - Un patrón de sobrescritura de una pasada utilizando un patrón pseudoaleatorio generado por el RBG del producto, ceros, unos, un nuevo valor de clave o algún valor que no contenga ningún parámetro de seguridad crítico (PSC).
        - Destrucción de la referencia a la clave directamente seguida por una llamada al "recolector de basura" de la memoria.
    - Para memoria no volátil:
        - Que emplee un algoritmo de *wear-leveling*, la destrucción deberá consistir en alguno de los siguientes métodos:
            1. Un patrón de sobrescritura de una pasada consistente en ceros, unos, un nuevo valor de clave de la misma longitud o algún valor que no contenga ningún parámetro de seguridad crítico (PSC).
            2. Borrado de bloque.
        - Que no emplee un algoritmo *wear-leveling*, la destrucción deberá ejecutarse por:

[20] Solamente para el caso de autenticación de mensajes con HMAC se permitirá el uso de SHA-1.

3. Una o más pasadas de sobrescritura consistente en ceros seguidos de una lectura de verificación.
4. Una o varias pasadas de sobrescritura consistente en todos unos seguidos de una lectura de verificación, sobrescrito con un nuevo valor de una clave con la misma longitud seguido por una lectura de verificación.
5. Una o varias pasadas de sobrescritura consistente en algún valor que no contenga ningún CSP seguidos de una verificación de lectura, sobrescrito con un nuevo valor de una clave con la misma longitud seguido por una verificación de lectura.
6. Borrado de bloque.

Y si la lectura de verificación de los datos sobrescritos falla, el proceso deberá ser repetido de nuevo hasta un número mayor que cero de intentos en el cual se devuelva un error.

61. **REQ. 56** Destrucción del material criptográfico. Todos los parámetros intermedios y claves criptográficas serán destruidas cuando finalice su uso, utilizando los métodos de borrado seguro establecidos.
62. **REQ. 57** Protección de las claves y el material de cifra. El producto no deberá almacenar claves en memoria no volátil. Sólo podrá hacerlo cuando esté envuelta digitalmente o cifrada, o cuando reúna alguno de los siguientes criterios:
    - La clave no cifrada no es parte de la cadena de claves.
    - La clave no cifrada no permite acceso a los datos cifrados tras la utilización inicial.
    - La clave no cifrada se graba en un dispositivo externo de almacenamiento para usar como factor de autorización.
63. **REQ. 58** Los parámetros de seguridad críticos deberán ser almacenados cuando no se utilicen en un almacén de claves suministrado por la plataforma.
64. **REQ. 59** Todos los procesos de ejecución de mecanismos criptográficos correrán de manera independiente.

5.5 REQUISITOS IPSEC

65. **REQ. 60** El producto deberá implementar la arquitectura IPSEC de acuerdo a lo especificado en la RFC 4301, con los modos túnel y/o transporte.
66. **REQ. 61** El producto deberá implementar el protocolo IKEv2 como se define en RFC 7296 con NAT transversal como opción.

67. **REQ. 62** El producto deberá asegurar que el protocolo IKE implementa autenticación extremo a extremo utilizando firma electrónica, que utilice certificados X.509v3 o claves previamente compartidas.

68. **REQ. 63** El producto deberá asegurar que la información cifrada IKEv2 utiliza AES en los modos CBC o GCM.

69. **REQ. 64** El producto deberá asegurar que los tiempos de vida de las asociaciones de seguridad (SA) de los protocolos IKE podrán ser configurados por un administrador en base al número de paquetes, volumen de tráfico y/o tiempo transcurrido.

70. **REQ. 65** El producto deberá asegurar que todos los protocolos IKE implementan al menos un grupo *Diffie-Hellman* de los siguientes:

Grupo	Nº IANA	RFC
3072-bit MODP GROUP	15	3526
4096-bit MODP GROUP	16	3526
256-bit random ECP GROUP	19	5903
384-bit random ECP GROUP	20	5903
512-bit random ECP GROUP	21	5903
Brainpool P256r1	28	6954
Brainpool P384r1	29	6954
Brainpool P512r1	30	6954

71. **REQ. 66** El producto deberá generar el valor secreto X utilizado en el intercambio de claves *Diffie-Hellman* ("x" en g^x mod p) utilizando el RBG especificado y con una longitud de bits de al menos el doble de los "bits de seguridad" asociados con el grupo DH negociado.

72. **REQ. 67** El producto deberá implementar protocolo IPSEC ESP como se define en RFC 4303 utilizando AES junto con algún algoritmo para la autenticación de mensajes.

73. **REQ. 68** El producto deberá generar nonces para el intercambio en IKE. La probabilidad de repetir un nonce durante la vida de una determinada SA IPSec será menor o igual de $1/(2^{128})$.

6. ABREVIATURAS

AES	Advanced Encryption Standard
CBC	Cipher Block Chaining
CC	Common Criteria
CCDB	Common Criteria Development Board
CCM	Counter with CBC-MAC
CCN	Centro Criptológico Nacional
CMAC	Cipher-Based Message Authentication Code
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
CTR	Counter Mode
DSA	Digital Signature Algorithm
EAL	Evaluation Assurance Level
EAP	Extensible Authentication Protocol
ECDSA	Elliptic Curve Digital Signature Algorithm
ENS	Esquema Nacional de Seguridad
ESP	Encapsulating Security Payload
GCM	Galois/Counter Mode
HMAC	Hash-based message authentication code
HTTPS	Hypertext Transfer Protocol Secure
IPSec	Internet Protocol Security
MAC	Message Authentication Code
NAT	Network Address Translation
NIAP	National Information Assurance Partnership
IKE	Internet Key Exchange
PSC	Parámetros de Seguridad Críticos
PSS	Parámetros de Seguridad Sensibles
RBG	Random Bit Generator
RFC	Request For Comments
RFS	Requisitos Fundamentales de Seguridad
RSA	Rivest, Shamir y Adleman
SA	Security Association

SHA	Secure Hash Algorithm
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VPN	Virtual Private Network

PUBLICACIONES DE DEFENSA

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