centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC - Anexo D8.B: VPN SSL

Junio 2021

MINISTERIO DE DEFENSA

Edita:

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 16:42:13 +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 de **Redes Privadas Virtuales SSL (VPN SSL)** 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 de **Redes Privadas Virtuales SSL (VPN SSL)** 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.

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. El alcance del presente documento, y los Requisitos Fundamentales de Seguridad que aquí se recogen, se refieren a las VPN basadas en el protocolo SSL/TLS, que a partir de ahora serán referenciadas como "VPN SSL"[1].

8. Una VPN SSL proporciona un canal de acceso seguro a los recursos de la organización. Está formada por uno o más Servidores VPN (también llamados Terminadores o *Gateways* VPN) a los que los usuarios se conectan, bien a través de sus navegadores Web (*Web browsers*), bien a través de un software específico instalado en su equipo, llamado cliente VPN. Todo el tráfico entre el navegador Web o cliente VPN, y el servidor VPN SSL, estará protegido y cifrado a través del protocolo SSL/TLS.

9. Las funcionalidades y los servicios de seguridad que puede proporcionar una VPN SSL, dependen mucho del producto. Cada producto ofrece sus propias características, y estas pueden diferir en gran medida de las ofrecidas por otro producto. A continuación, se indican las funcionalidades más comunes:

    a) **Autenticación.** Cada Servidor VPN SSL puede soportar diversos métodos de autenticación que van, desde métodos integrados, hasta el uso de servidores externos de autenticación.

    La autenticación del cliente puede utilizar métodos basados en contraseñas, tarjetas inteligentes (*smartcards*) o *tokens*. Uno de los métodos más extendidos es el uso de certificados digitales X.509.

    Muchos productos VPN SSL soportan la integración con servidores externos de autenticación, como RADIUS o Directorio Activo (AD). Hacen uso, por lo tanto, de las bases de datos de autenticación existentes en la organización. De hecho, normalmente, los productos VPN SSL necesitan acceder a la información de grupos de los servidores de autenticación, para proporcionar las funciones de Control de Acceso.

    b) **Control de Acceso.** Las funciones de Control de Acceso son uno de los objetivos principales de las VPN SSL. Se utilizan diversas políticas de

[1] El protocolo SSL se encuentra obsoleto en la actualidad y finalizó en la versión 3.0. TLS es su sucesor, y es el protocolo solicitado en los requisitos de las secciones posteriores. Sin embargo, se denominará a este tipo de VPNs "VPN SSL" dado que es el término comúnmente extendido para su denominación.

control de acceso para proporcionar el acceso a los servicios, en función de múltiples parámetros. Por ejemplo: en función de la aplicación o fichero particular al que se solicita acceso, día y hora, tipo de navegador Web, tipo de dispositivo (ordenador, Tablet, Smartphone, etc.), identificación del usuario, etc. Algunos productos VPN SSL incluso permiten integrar el control de acceso con los controles de seguridad de los equipos remotos (*endpoints*). Esto permite realizar un chequeo del equipo (*host check*) tras la autenticación, y en base a él, determinar los controles de acceso.

c) **Protección de Confidencialidad e Integridad.** Estos servicios son proporcionados por los protocolos SSL/TLS.

d) **Controles de seguridad de los equipos remotos (*endpoint host check*).** Los productos VPN SSL pueden proporcionar capacidades para verificar el cumplimiento de las políticas de seguridad de la organización, por parte de los equipos remotos (*endpoints*), previo a permitirles el acceso a la VPN. Por ejemplo: verificación de que el software antivirus y anti malware están actualizados y en ejecución en el equipo, de la actualización de los parches de seguridad, etc. En estos controles de seguridad se incluyen mecanismos de protección que se ejecutan en el equipo, como por ejemplo limpiadores de la caché del navegador Web, que eliminan información sensible.

e) **Operación y Gestión.** Los productos VPN SSL disponen de funcionalidades para facilitar la operación y gestión de la infraestructura VPN. Por ejemplo: registro de eventos y logs, funciones de auditoría, informes, etc.

f) **Alta disponibilidad y Escalabilidad.** Los productos VPN SSL pueden proporcionar mecanismos de protección frente a fallos de componentes de la VPN, de forma que el servicio no se vea interrumpido. Pueden ser proporcionados a través de métodos de balanceo de carga, que proporcionan a su vez escalabilidad.

g) **Personalización.** Los productos VPN SSL disponen de funcionalidades para personalizar las características y el aspecto del portal Web al que acceden los usuarios remotos para conectarse a las aplicaciones internas de la organización.

10. Los productos incluidos en esta familia pueden ofrecer otras funcionalidades complementarias (p.ej. cortafuegos, prevención de intrusiones, etc.) no específicamente contempladas en este documento.

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

2.2 CASOS DE USO

12. En las VPN SSL se contemplan dos casos de uso principales: VPN SSL Portal, y VPN SSL Túnel.

13. Existe un tercer caso que es la VPN SSL punto a punto (*gateway-to-gateway*) que se establece entre dos Servidores VPN. Este tipo de VPN SSL prácticamente no se implementa, ya que para ello suelen emplearse las VPN IPsec, que tienen características muy similares y mayor flexibilidad.

2.2.1. CASO DE USO 1 – VPN SSL PORTAL

14. Permiten a un usuario remoto acceder mediante conexión SSL/TLS, a un "Portal Web" (implementado por el Servidor VPN SSL) desde el cual, se accede de forma segura a las aplicaciones y servicios de la red interna de la organización para los que el usuario tenga autorización. El acceso a este portal Web se realiza a través de un navegador web estándar (*web browser*).

15. El Portal Web normalmente realiza funciones de proxy. Esto significa que no se establece conexión directa entre el usuario y las aplicaciones internas, sino que es el proxy quien establece ambas conexiones, por un lado, con el usuario (recibe sus peticiones de información) y por otro lado con las aplicaciones, solicitando la información y enviándosela posteriormente al usuario.

16. Las aplicaciones y servicios accesibles desde este Portal Web, deben ser basados en web (*web-based*) o deben poder ser accedidos mediante un interfaz Web. Para aplicaciones no basadas en Web, es necesario que el servidor VPN disponga de una funcionalidad adicional que le permita llevar a cabo la "traducción de protocolo" y ser así capaz de convertir información de un protocolo a otro.

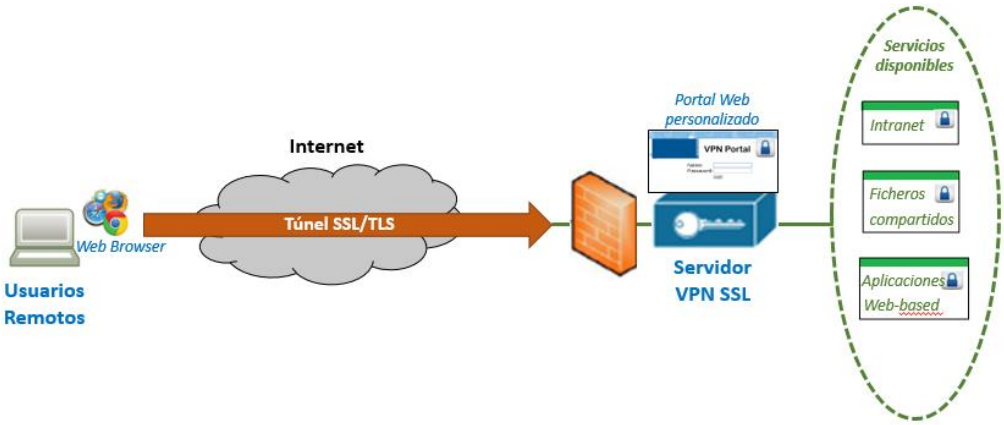

Figura 1 - Ejemplo de Caso de Uso 1: VPN SSL Portal

2.2.2. CASO DE USO 2 – VPN SSL TÚNEL

17. La VPN SSL Túnel proporciona un túnel de capa 3 a través del cual, los usuarios pueden acceder a la red interna de la organización. Para ello el usuario necesita instalar un software específico en su equipo, llamado “cliente VPN”.
18. Mientras que la VPN SSL Portal en ciertos casos puede no proporcionar la suficiente flexibilidad a los usuarios, al no soportar ciertas aplicaciones (por ejemplo, si el usuario quiere usar un cliente mail que se comunica con un servidor POP3), la VPN SSL Túnel permite el acceso a todos los recursos de la red interna de la organización, incluyendo aquellos que no están basados en Web.
19. Este tipo de VPN normalmente permite, además, dividir el tráfico (*split tunneling*), de forma que sólo el tráfico que se especifique y que necesite ser protegido, circulará a través de la VPN, mientras que otro tráfico que no necesite protección, no será redirigido a la VPN.
20. Sin embargo, la necesidad de instalación del cliente VPN puede ser un obstáculo importante para este tipo de VPN, ya que requiere permisos de administración en el equipo.

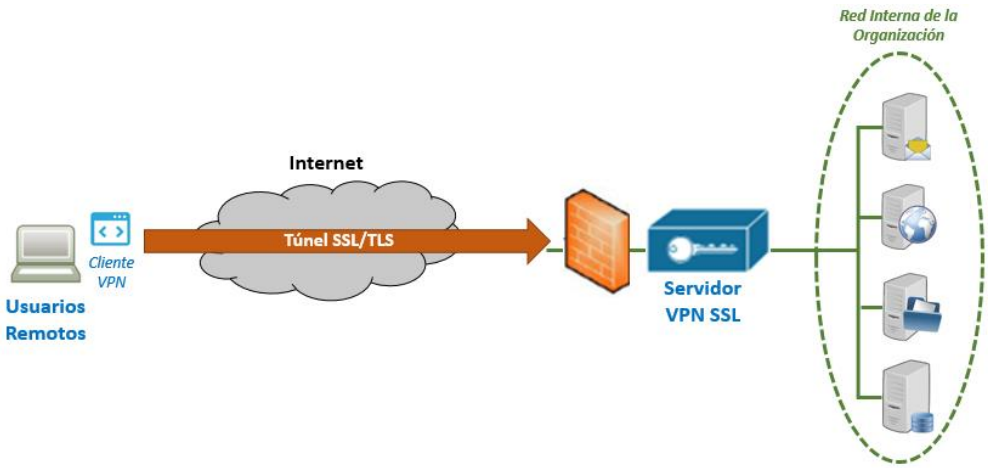

Figura 2 – Ejemplo de caso de Uso 2: VPN SSL Túnel

2.3 ENTORNO DE USO

21. Por lo general este tipo de dispositivos se encuentran en grandes o medianas empresas, así como en redes de las Administraciones Públicas como parte de una arquitectura de defensa en profundidad, existiendo medidas complementarias en diferentes capas de protección.
22. Para la utilización en condiciones óptimas de seguridad de las VPN, es necesaria su integración en un entorno que cumpla una serie de condiciones mínimas de protección:

a) **Protección física:** Los productos hardware deberán instalarse en áreas donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.

b) **Aislamiento de red:** Cuando dos redes o sistemas internos se comunican con una VPN, no se debe permitir ningún otro flujo de datos entre ellos, todo el tráfico debe ser protegido por la VPN. Cualquier tráfico de red entre redes internas y externas que no se realice a través de una VPN (p. ej., acceso a servicios de internet) debe estar debidamente protegido.

c) **Administración confiable:** Los usuarios administradores serán miembros de plena confianza y que vela por los mejores intereses en materia de seguridad de la empresa/administración. Dichas personas deberán estar debidamente capacitadas y carecerán de cualquier intención maliciosa o conflictos de intereses al administrar los productos VPN. Habitualmente los productos no son capaces de defenderse contra un usuario administrador con malas intenciones, aunque debería prevenir errores accidentales (p.ej. con mensajes pidiendo confirmación para todas las acciones de administración).

d) **Actualizaciones periódicas:** El firmware y/o software de los productos será parcheado y actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.

e) **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. El producto deberá asegurar que las credenciales de usuario se almacenan de forma segura.

f) **Política de seguridad de la información:** La política de seguridad de la organización deberá recoger el conjunto de principios, organización y procedimientos impuestos por la 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

23. Típicamente los servidores VPN SSL 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.

24. 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 c.

25. En caso de ofrecer funcionalidades adicionales a las definidas, éstas quedan fuera del alcance analizado, y deberán ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

26. 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).
27. 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.
28. 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.
29. 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.
30. 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

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

    a) Información que atraviese el producto entre sus interfaces de red interna y externa en el caso de los Servidores VPN, o entre el cliente VPN y la red externa, en ambos sentidos.

    b) Información que atraviese el túnel VPN.

    c) Claves criptográficas utilizadas para proteger el canal de comunicaciones.

    d) Información sobre la topología de las redes y sistemas conectados mediante el túnel VPN.

    e) Datos de configuración del producto y de auditoría generados por éste.

    f) Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

32. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente serían:

    a) **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.

    b) **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).

    c) **Divulgación de información:** Si la VPN permite obtener información sobre las redes y/o sistemas internos, esta información podría ser utilizada por un atacante.

    d) **Propagación de virus y malware:** Propagación de virus y malware entre las distintas redes/sistemas conectados por la VPN.

    e) **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.

f) **Cifrado débil:** Utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.

g) **Uso de canales de comunicación inseguros:** Mala implementación de protocolos estándar (p.ej. TLS), utilización de versiones antiguas, o utilización de protocolos no estandarizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones del dispositivo.

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

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

    Este apartado debe utilizarse para dispositivos empleados en los siguientes casos de uso:

    a) VPN SSL Portal.

    b) VPN SSL Túnel.

    La información relativa a los requisitos para los programas software que actúan como cliente VPN en el caso de uso VPN SSL Túnel, 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[2]	2.2e	27/03/2020	CCDB
Collaborative Protection Profile for Network Devices[3]	2.1	24/09/2018	CCDB
Collaborative Protection Profile for Network Devices[4]	2.0 + Errata 20180314	14/03/2018	CCDB
Collaborative Protection Profile for Network Devices.5	1.0	27/02/2015	CCDB

Tabla 2. Perfiles de protección

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 SFR (*Security Functional Requirements*) de *Collaborative Protection Profile for*

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

Network Devices V.2.2e con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.2 REQUISITOS GENERALES

2. **REQ. 1**. En caso de que el producto implemente la VPN tipo Portal, debe proporcionar las capacidades de Proxy, haciendo de intermediario en la comunicación entre el cliente, y el servidor o aplicación destino. Se presentará a sí mismo como el servidor o la aplicación frente al cliente (usuario), y viceversa.
3. **REQ. 2**. En caso de que el producto implemente la VPN tipo Túnel, debe proporcionar al administrador capacidades que permitan obligar a que todo el tráfico de los clientes remotos pase a través del túnel VPN (*full tunneling*).

4.3 CONTROL DE SESIÓN

4. **REQ. 3**. El producto debe permitir la configuración de un tiempo máximo durante el cual la sesión VPN podrá permanecer inactiva, de forma que, transcurrido este tiempo, el sistema solicitará al usuario una nueva autenticación o finalizará la sesión.
5. **REQ. 4**. El producto debe permitir la configuración de un tiempo máximo de duración de la autenticación de la sesión VPN, de forma que, transcurrido este tiempo, el sistema solicitará de nuevo al usuario que lleve a cabo la autenticación o finalizará la sesión.
6. **REQ. 5**. El producto debe permitir a un administrador terminar una sesión VPN activa de cualquier usuario remoto conectado.
7. **REQ. 6**. Una vez finalizada la sesión VPN SSL, el producto debe limpiar los datos residuales que hayan podido quedar en el equipo del usuario remoto, como ficheros temporales o cachés de aplicaciones, especialmente la caché del navegador web.

4.4 MONITORIZACIÓN

8. **REQ. 7**. El producto debe permitir monitorizar las sesiones VPN activas. Para cada una de ellas deberá mostrar, al menos, el nombre del usuario remoto que ha establecido la sesión, la dirección IP del equipo conectado, y la hora de inicio de la conexión.

4.5 AUDITORÍA

9. **REQ. 8**. El producto debe realizar un registro (log) de los eventos relevantes relacionados con las sesiones VPN SSL. Los eventos registrados serán, al menos, éxito y fallo en el establecimiento de una sesión, fallo en la autenticación de cliente y finalización de una sesión.

10. **REQ. 9**. Cada registro contendrá, al menos, los siguientes datos: fecha/hora del evento, nombre del usuario asociado al evento, motivo del fallo o de la finalización de sesión.
11. **REQ. 10**. El producto debe permitir, tanto almacenar estos registros en local, como enviarlos a un servidor de auditoría a través de un canal de comunicaciones seguro (mediante protocolo TLS 1.2 (o superior) o IPsec).
12. **REQ. 11**. El producto debe permitir restringir el acceso a los eventos y logs del sistema a usuarios administradores específicos (auditor).

4.6 PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

13. **REQ. 12**. El producto debe implementar auto chequeos de arranque, donde se verifique la integridad del software o firmware, los mecanismos criptográficos y las funciones críticas, si procede.
14. **REQ. 13**. El producto debe apagarse (*shutdown*) en caso de que se detectase un error en los chequeos anteriormente citados.
15. **REQ. 14**. El producto debe permitir a usuarios autorizados consultar la versión de software/firmware e iniciar actualizaciones de éstos.
16. **REQ. 15**. El producto debe 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.

4.7 AUTENTICACIÓN

17. **REQ. 16**. El producto debe llevar a cabo la autenticación del servidor a través de certificados X.509v3 que cumplan con la RFC 5280.
18. **REQ. 17**. El producto debe soportar doble factor de autenticación para el cliente. En caso de que se configure esta autenticación de doble factor, uno de los factores será que el cliente disponga de un certificado X.509v3 que cumpla la RFC 5280. El otro factor debe ser “algo que el usuario sabe”, y para ello el producto deberá soportar, al menos, el uso de contraseñas almacenadas en local en el servidor VPN, y/o el uso de protocolos de autenticación remota como RADIUS, TATACS+, LDAP o Active Directory.

4.7.1. CERTIFICADOS

19. **REQ. 18**. El producto debe admitir certificados con una seguridad equivalente a 128 bits o superior. Esto implica que la clave pública contenida en el certificado debe proporcionar, al menos, 128 bits de fortaleza[6].

[6] Una fortaleza de 128 bits es equivalente a una clave RSA o DH de 3072 bits o a una clave ECC de 256 bits (cuerpos primos).

20. **REQ. 19**. El producto debe permitir obtener el certificado a través de Solicitudes de Certificado (*Certificate Message Request*) a una CA, siguiendo las especificaciones de la RFC 2986.

21. **REQ. 20**. El certificado usado por el producto en el proceso de autenticación del servidor durante la negociación TLS (TLS *Handshake*), solo debe ser empleado para esta misión y para ninguna otra. Para ello, este certificado debe soportar el uso de la extensión "*extendedKeyUsage*", y el valor de este campo debe corresponder a "*Server Authentication purpose*" (id-kp 1 según la RFC 5280).

4.7.2. AUTENTICACIÓN DE CLIENTE

22. **REQ. 21**. En caso de que se configure la autenticación de cliente, el producto debe llevar a cabo la validación de la ruta del certificado cliente (*certificate path validation*) según la RFC 5280. En caso de que la validación falle, el servidor finalizará la conexión TLS.

23. **REQ. 22**. La validación del certificado del cliente incluirá la revisión del estado de revocación del mismo, empleando alguno de los siguientes mecanismos:

    a) Una lista CRL (*Certification Revocation List*) según se especifica en la RFC 5280 (sección 6.3) o en la RFC 5759 (sección 5).

    b) El protocolo OCSP (*Online Certificate Status Protocol*) según se especifica en la RFC 6960.

    En caso de que el certificado del cliente esté revocado, el servidor finalizará la conexión TLS.

24. **REQ. 23**. En caso de que no se pueda obtener el estado de revocación del certificado del cliente (por ejemplo, por un problema de conexión), el producto finalizará la conexión TLS o permitirá al administrador configurar dicha opción.

25. **REQ. 24**. La validación del certificado del cliente incluirá la revisión del campo "*extendedKeyUsage*", cuyo valor deberá corresponder a "*Client Authentication purpose*" (id-kp 2, según la RFC 5280) para los certificados que el cliente presente para autenticación de la conexión TLS. En caso de que no corresponda, el servidor finalizará la conexión TLS.

26. **REQ. 25**. El producto deberá validar que el certificado del cliente contiene, en los campos Sujeto (*Subject Distinguished Name*) o Nombre Alternativo del Titular (*Subject Alternative Name*), el identificador del cliente configurado para la conexión TLS. En caso contrario, finalizará la conexión.

4.8 PROTOCOLO TLS (TRANSPORT LAYER SECURITY)

27. **REQ. 26**. El producto debe soportar versiones de TLS 1.2 (RFC 5246) o superior.

28. **REQ. 27**. El producto debe denegar la conexión (o poder configurarse para hacerlo) cuando la versión TLS solicitada por el cliente sea inferior a TLS 1.2 (SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1).

29. **REQ. 28**. El producto no debe utilizar la extensión TLS "client_certificate_url". De esta forma, en caso de que se configure la autenticación de cliente, este no podrá enviar una URL del certificado, sino que deberá enviar el certificado en sí.

4.9 REQUISITOS CRIPTOGRÁFICOS

30. **REQ. 29**. El producto debe soportar el uso de *ciphersuites* compuestas únicamente por funciones y algoritmos criptográficos aceptados para nivel Alto del ENS según la guía CCN-STIC-807, así como proporcionar capacidades de configuración que permitan obligar el uso de estas *ciphersuites* exclusivamente.
31. **REQ. 30**. El producto debe soportar el uso de longitudes de clave que proporcionen una fortaleza equivalente a 128 bits o superior.
32. **REQ. 31**. En caso de que el producto suministre un servicio de generación de bits aleatorios (RBG) determinísticos, debe utilizar Hash_DRBG (any), HMAC_DRBG (any) o CTR_DRBG (AES).
33. **REQ. 32**. El RBG determinístico empleado por el producto, debe 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.
34. **REQ. 33**. El producto debe implementar los métodos de borrado de claves que se indican a continuación. En todos los casos tras el borrado se llevará a cabo una lectura de verificación, de forma que si esta falla, el proceso debe repetirse de nuevo.
    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.

c. **REQ. 34**. Destrucción del material criptográfico. Todos los parámetros intermedios y claves criptográficas serán destruidas cuando finalice su uso, utilizando los métodos de borrado seguro establecidos.

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

35. Esta sección abarca los requisitos aplicables a los programas (software) que actúan como cliente VPN. Estos programas se instalan en el equipo del usuario remoto, y le permiten establecer la conexión VPN con la red interna de la organización.

    Este apartado es aplicable al caso de uso VPN SSL Túnel.

    La información relativa a los requisitos para los Servidores VPN no queda cubierta por este apartado.

5.1 REQUISITOS GENERALES

36. **REQ. 35**. La instalación, configuración y administración del producto sólo podrá realizarla un usuario administrador.
37. **REQ. 36**. Una vez finalizada la sesión VPN SSL, el producto debe limpiar los datos residuales que hayan podido quedar en el equipo del usuario, como ficheros temporales o cachés de aplicaciones que podrían almacenar nombres de usuario, contraseñas, datos que haya introducido el usuario, etc.
38. **REQ. 37**. El producto debe proporcionar capacidades que permitan llevar a cabo un chequeo del equipo del usuario (*host checking*), para determinar el estado de su seguridad previo al establecimiento de la conexión VPN, en función de la política de seguridad que se haya configurado en el Servidor VPN SSL.

5.2 PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

39. **REQ. 38**. El producto debe implementar auto chequeos de arranque, donde se verifique la integridad del software o firmware, los mecanismos criptográficos y las funciones críticas, si procede.
40. **REQ. 39**. El producto debe apagarse (*shutdown*) en caso de que se detectase un error en los chequeos anteriormente citados.
41. **REQ. 40**. El producto debe permitir a usuarios autorizados consultar la versión de software/firmware e iniciar actualizaciones de éstos.
42. **REQ. 41**. El producto debe 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.
43. **REQ. 42**. El producto debe ser capaz de detectar intentos de acceso indiscriminado al servicio para evitar posibles denegaciones de servicio, a través de cualquier interfaz.

44. **REQ. 43**. 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.

5.3 AUTENTICACIÓN

5.3.1. CERTIFICADO

45. **REQ. 44**. El producto deberá tener la capacidad para utilizar certificados X.509v3 que cumplan la RFC 5280, para llevar a cabo la autenticación de cliente, si procede.
46. **REQ. 45.** El producto debe admitir certificados con una seguridad equivalente a 128 bits o superior. Esto implica que la clave pública contenida en el certificado debe proporcionar una fortaleza de al menos 128 bits.
47. **REQ. 46**. El certificado usado por el producto en el proceso de autenticación del cliente durante la negociación TLS (TLS Handshake), solo debe ser empleado para esta misión y para ninguna otra. Para ello, este certificado debe soportar el uso de la extensión "extendedKeyUsage", y el valor de este campo debe corresponder a "Client Authentication purpose" (id-kp 2 según la RFC 5280).

5.3.2. AUTENTICACIÓN DEL SERVIDOR

48. **REQ. 47.** El producto deberá llevar a cabo la validación de la ruta del certificado servidor (*certificate path validation*) según la RFC 5280. En caso de que la validación falle, el producto finalizará la conexión TLS.
49. **REQ. 48.** El producto deberá comprobar el estado de revocación del certificado del servidor, empleando alguno de los siguientes mecanismos:

    a) Una lista CRL (Certification Revocation List) según se especifica en la RFC 5280 (sección 6.3) o en la RFC 5759 (sección 5).

    b) El protocolo OCSP (Online Certificate Status Protocol) según se especifica en la RFC 6960.

    En caso de que el certificado del servidor esté revocado, el cliente finalizará la conexión TLS.
50. **REQ. 49.** En caso de que no se pueda obtener el estado de revocación del certificado del servidor (por ejemplo, por un problema de conexión), el producto finalizará la conexión TLS o permitirá al administrador configurar dicha opción.
51. **REQ. 50.** El producto deberá validar que el certificado del servidor contiene, en los campos Sujeto (*Subject Distinguished Name*) o Nombre Alternativo del Titular (*Subject Alternative Name*), el identificador del servidor configurado para la conexión TLS. En caso contrario, finalizará la conexión.

5.4 REQUISITOS CRIPTOGRÁFICOS

52. **REQ. 51**. El producto debe soportar el uso de *ciphersuites* compuestas únicamente por funciones y algoritmos criptográficos aceptados para nivel Alto del ENS según la guía CCN-STIC-807, así como proporcionar capacidades de configuración que permitan obligar el uso de estas *ciphersuites* exclusivamente.
53. **REQ. 52**. El producto debe soportar el uso de longitudes de clave que proporcionen una fortaleza equivalente a 128 bits o superior.
54. **REQ. 53**. En caso de que el producto suministre un servicio de generación de bits aleatorios (RBG) determinísticos, debe utilizar Hash_DRBG (any), HMAC_DRBG (any) o CTR_DRBG (AES).
55. **REQ. 54**. El RBG determinístico empleado por el producto, debe 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. 55**. El producto debe implementar los métodos de borrado de claves que se indican a continuación. En todos los casos tras el borrado se llevará a cabo una lectura de verificación, de forma que si esta falla, el proceso debe repetirse de nuevo.

    a) Para memoria volátil, la destrucción debe ser ejecutada empelando uno de los siguientes métodos:

        i. Una pasada de sobrescritura utilizando un patrón pseudoaleatorio generado por el RBG del producto, ceros, unos, o un nuevo valor de clave o algún otro valor que no contenga ningún parámetro de seguridad crítico (PSC).

        ii. Apagado de la alimentación de la memoria.

        iii. Destrucción de la referencia a la clave directamente seguida por una llamada al “recolector de basura” de la memoria.

    b) Para memoria no volátil, la destrucción debe ser ejecutada empleando uno de los siguientes métodos:

        Si emplea un algoritmo de wear-leveling:

        i. Una pasada de sobrescritura con ceros, unos, o un nuevo valor de clave de la misma longitud o algún valor que no contenga ningún parámetro de seguridad crítico (PSC).

        ii. Borrado de bloque.

        Si no emplea un algoritmo de wear-leveling:

        i. Una pasada de sobrescritura utilizando un patrón pseudoaleatorio generado por el RBG del producto o ceros.

ii. Tres o más pasadas de sobrescritura utilizando un patrón aleatorio que se irá cambiando antes de cada escritura.

iii. Una o varias pasadas de sobrescritura con unos, o con algún valor que no contenga ningún parámetro de seguridad crítico (PSC), seguidos de una lectura de verificación y sobrescrito con un nuevo valor de una clave con la misma longitud seguido por una lectura de verificación.

iv. Borrado de bloque.

57. **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.

5.5 PROTOCOLO TLS (TRANSPORT LAYER SECURITY)

58. **REQ. 57**. El producto debe soportar las versiones TLS 1.2 (RFC 5246) o superiores.

59. **REQ. 58**. El producto debe denegar la conexión (o poder configurarse para hacerlo) cuando la versión TLS solicitada por el cliente sea inferior a TLS 1.2 (SSL 1.0, SSL 2.0, SSL 3.0, TLS 1.0, TLS 1.1).

60. **REQ. 59**. El producto debe ser configurable para establecer la versión TLS preferente, con la que se solicitará la conexión.

61. **REQ. 60**. El producto no debe utilizar la extensión TLS "*client_certificate_url*". De esta forma, en caso de que se configure la autenticación de cliente, el producto no podrá enviar una URL del certificado, sino que deberá enviar el certificado en sí.

6. ABREVIATURAS

AES	*Advanced Encryption Standard*
CA	*Certification Authority*
CC	Criterios Comunes / *Common Criteria*
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de la Información y la Comunicación
CRL	*Certification Revocation List*
EAL	*Evaluation Assurance Level*
ENS	Esquema Nacional de Seguridad
HMAC	*Hashed Message Authentication Code*
HTTPS	*Hypertext Transfer Protocol*
IPS	*Intrusion Prevention System*
IPSEC	*Internet Protocol Security*
OCSP	*Online Certificate Status Protocol*
OSI	*Open Systems Interconnection*
PP	Perfil de Protección
PSC	Parámetros de Seguridad Críticos
RBG	*Random Bit Generator*
RFS	Requisitos Fundamentales de Seguridad
SSL	*Secure Socket Layer*
STIC	Seguridad de las Tecnologías de la Información y la Comunicación
TIC	Tecnologías de la Información y la Comunicación
TLS	*Transport Layer Security*
URL	*Uniform Resource Locator*
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