centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo D.4-M: Proxies

Enero 2020

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
2020.02.13 17:39:31 +01'00'

NIPO: 083-19-053-9

Fecha de Edición: enero 2020

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 ***Proxies*** 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) Categoría MEDIA**. 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 ***Proxies*** 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 interconexiones, actuando de intermediarios en el intercambio de peticiones entre los usuarios de una red y recursos ubicados en otra red diferente.
7. Un ejemplo sería el escenario en el que una máquina S1 dentro de una red interna (red A) solicita un recurso a un servidor S3 situado en una red externa (red B), como Internet, para lo que lanzará una petición a través del sistema S2 equipado con el intermediario o *proxy* y ubicado en algún punto de la frontera entre ambas redes, quién a su vez trasladará la petición a S3. De esta forma S3desconocerá la procedencia original de la petición teniendo por único interlocutor al sistema S2.
8. En este contexto proporcionan las siguientes funciones básicas de seguridad:
   - Ruptura de la continuidad de los protocolos de comunicaciones entre las redes interconectadas.
   - Enmascaramiento de la infraestructura o composición de la red, haciendo anónimos los sistemas en la red protegida que establecen comunicaciones con el exterior.
   - Restricción o filtrado de determinados tipos de tráfico conforme a las políticas que defina la organización.
   - Registro del tráfico que atraviesa la interconexión entre las redes conectadas.
9. La protección puede tener lugar a diferentes niveles dentro de las capas definidas por el modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1)[1], fundamentalmente a nivel de capa 3 (de red), 4 (de transporte) y/o 7 (de aplicación).
10. Los productos incluidos en esta familia pueden ofrecer otras funcionalidades complementarias (p.ej. cortafuegos o enrutamiento) recogidas en otra familia de productos.

2.2 CASOS DE USO

11. Se contempla un único caso de uso.

2.2.1. CASO DE USO 1 - INTERMEDIARIO EN LA CONEXIÓN

12. El dispositivo se encuentra desplegado como parte de la arquitectura de interconexión entre la red interna o protegida y la(s) red(es) externa(s) con el fin

[1] Modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1) es un modelo de referencia para los protocolos de la red de arquitectura en capas creado por la Organización Internacional de Normalización (ISO) y la Comisión electrotécnica Internacional (IEC).

de recibir, registrar y reenviar el tráfico en ambos sentidos, siempre y cuando cumpla con las políticas de filtrado establecidas, y modificando los parámetros necesarios del protocolo de comunicación para enmascarar los dispositivos de la red protegida que intervienen en ella.

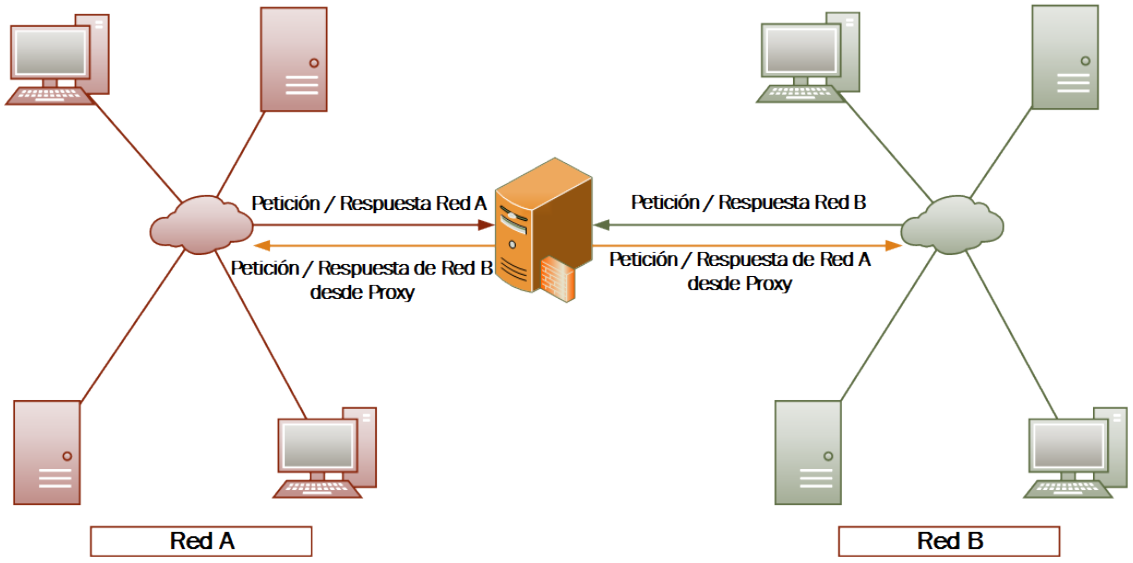

Figura 1 – Ejemplo de Caso de Uso: Intermediario en la conexión

2.3 ENTORNO DE USO

13. Este tipo de dispositivos son de uso generalizado en grandes o medianas empresas, así como en redes del sector público como parte de una arquitectura de defensa en profundidad, existiendo medidas complementarias en diferentes capas de protección.

14. Para la utilización en condiciones óptimas de seguridad de estos dispositivos, es necesaria su integración en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:

    - **Protección física**: El producto deberá instalarse en un área donde el acceso sólo sea posible para el personal autorizado y con condiciones ambientales adecuadas.
    - **Control de flujos de información**: La red interna no debería disponer de otras interfaces con la red externa que permitan evadir el control de los flujos de información a través del producto, salvo que sean debidamente autorizadas y controladas.
    - **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 los dispositivos. El producto no será capaz de defenderse contra un usuario administrador con malas intenciones.

- **Actualizaciones periódicas**: El firmware y el software del producto será actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **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

15. Este tipo de productos se presentan en formato **equipo dedicado o *Appliance*** (*hardware* provisto de *firmware*[2] dedicado) con las funcionalidades estrictamente necesarias para cumplir su finalidad y acotadas al servicio específico que presten.
16. Adicionalmente, suele ser habitual que en las máquinas y dispositivos que protegen se incluya un ***software*** instalable o una **configuración personalizada** que sirva para poder realizar la función de intermediario correctamente.
17. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2, éstas quedan fuera del alcance analizado, debiendo ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 CERTIFICACIÓN LINCE

18. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS Medio, deberá disponer de una Certificación Nacional Esencial de Seguridad (LINCE)[3] que incluya los RFS reflejados en el apartado 4, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.

[2] *Firmware* funciona como el nexo de unión entre las instrucciones (software) que llegan al dispositivo desde el exterior y las diversas partes electrónicas (hardware)
[3] Toda la información relativa a esta metodología se encuentra disponible en la web del Organismo de Certificación (https://oc.ccn.cni.es)

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

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

- **AC.Administración.** Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos.
- **AC.Datos.** Datos de configuración del producto y de auditoría generados por éste. Información que atraviese el producto entre sus interfaces de red.
- **AC. Actualizaciones**. Actualizaciones del dispositivo susceptibles de afectar a su configuración y funcionalidad.

3.2 AMENAZAS

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

3.2.1. COMUNICACIONES CON EL PRODUCTO

- **A.NOAUT Acceso no autorizado de administrador:** Un atacante puede obtener un acceso cómo administrador del producto haciéndose pasar por un administrador ante el producto, por el producto ante un administrador, reproduciendo una sesión de administración, realizando ataques del hombre en medio.
- **A.CIFRA Cifrado débil:** Utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **A.COM Canales de comunicación no confiables:** Mala implementación de protocolos estándar o utilización de protocolos no estandarizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones del dispositivo.
- **A.AUT Autenticación débil de los nodos:** Un producto puede utilizar protocolos de autenticación seguros que utilicen métodos de autenticación débiles (contraseñas no robustas, contraseñas cómo texto en claro, contraseñas precompartidas) para hacerse pasar por un usuario administrador u otro nodo para realizar un ataque de hombre en el medio.

3.3 ACTUALIZACIONES VÁLIDAS

- **A.ACT Actualización maliciosa:** un atacante puede realizar una actualización maliciosa que debilite las funcionalidades de seguridad del producto.

3.4 AUDITORÍA

- **A.AUD Actividades no detectadas:** Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.

3.5 INFORMACIÓN Y CREDENCIALES

- **A.CRED Funcionalidades de seguridad comprometidas:** un atacante puede comprometer las credenciales o información del producto permitiendo un acceso continuado al producto y a su información sensible.
- **A.CON Contraseñas débiles:** Un atacante puede aprovecharse del uso contraseñas débiles para acceder con acceso privilegiado al dispositivo.

3.6 FALLO DEL PRODUCTO

- **A.FUN Fallo de las funcionalidades de seguridad:** Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

21. A continuación, se recogen los requisitos fundamentales de seguridad que deben cumplir los productos que quieran optar a la inclusión en el CPSTIC en esta familia.

4.1 ADMINISTRACIÓN

22. **ADM.1** El producto debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles (A.NOAUT).
23. **ADM.2** El producto debe ser capaz de realizar la gestión de las siguientes funcionalidades: (A.NOAUT).
    - Administración del producto de forma local y remota.
    - Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
    - Otros parámetros de configuración del producto.
24. **ADM.3** El producto deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones anteriormente descritas (ADM.2) (A.NOAUT).

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

25. **IAU.1** El producto deberá identificar y autenticar a cada usuario antes de otorgar acceso (A.NOAUT).
26. **IAU.2** El producto debe implementar mecanismos que impidan ataques de autenticación por fuerza bruta. (A.CON).
27. **IAU.3** El producto debe proteger contra lectura y modificación no autorizadas las credenciales de autenticación (A.CRED).
28. **IAU.4** El producto debe disponer de la capacidad de gestión de las contraseñas (A.CON):
    a) La contraseña debe de poder configurarse con una longitud mínima o igual a 9 caracteres.
    b) La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “]
29. **IAU.5** El producto debe bloquear o cerrar la sesión de un usuario después de un determinado periodo de tiempo de inactividad (A.NOAUT).

4.3 CANALES DE COMUNICACIÓN CONFIABLES

30. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades

autorizadas o entre distintas partes del producto empleando funciones, algoritmos y protocolos que estén de acuerdo a lo establecido en la guía CCN-STIC-807 (p.ej.: HTTPS/TLS 1.2, TLS 1.2 o superior, IPSec, etc.) (A.NOAUT, A.CIFRA).

31. **COM.2** El TOE debe permitir que estos canales de comunicación seguros sean iniciados por él mismo o por entidades autorizadas. (A.COM).
32. **COM.3** El producto hará uso de certificados digitales para la autenticación cuando utilice cualquiera de estos protocolos (A.COM).

4.4 CRIPTOGRAFÍA

33. **CIF.1** El TOE permitirá exclusivamente el empleo de funciones, algoritmos y protocolos que utilicen suites de cifrado que estén incluidas entre las autorizadas para Categoría Media del ENS, de acuerdo a lo establecido en la guía CCN-STIC-807 (A.CIFRA. A.COM).
34. **CIF.2** El producto deberá impedir el acceso en claro a los parámetros de seguridad críticos del sistema (claves simétricas y claves privadas) (A.CIFRA. A.COM).

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

35. **ACT.1** El producto debe ofrecer la posibilidad de consultar la versión actual del firmware/software (A.ACT).
36. **ACT.2** El producto debe ofrecer mecanismos (conforme a la criptografía de empleo en el ENS) a través de hashes o firma digital para autenticar las actualizaciones de firmware/software antes de instalarlas (A.ACT).
37. **ACT.3.** La actualización del firmware/software se permitirá únicamente a usuarios con rol de administrador (A.ACT).
38. **ACT.4** El producto debe ofrecer la posibilidad de iniciar actualizaciones de forma manual y de comprobar si existen nuevas actualizaciones disponibles (A.ACT).

4.6 AUDITORÍA

39. **AUD.1** El producto debe generar información de auditoría al comienzo y finalización de las funciones de auditoría y cuando se produzca alguno de los siguientes eventos (A.AUD):
    a) *Login* y *logout* de usuarios registrados.
    b) Cambios en las credenciales de usuarios.
    c) Cambios en la configuración del producto.
    d) Eventos relativos a la funcionalidad del producto.
    e) Generación, importación, cambio o eliminación de claves criptográficas.

40. **AUD.2** Los registros de auditoría contendrán al menos la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento (si aplica) (A.AUD).
41. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:
    a) Lectura: usuarios autorizados.
    b) Modificación: ningún usuario.
    c) Borrado: administradores.
42. **AUD.4** El producto debe ser capaz de almacenar la información de auditoría generada en sí mismo o en una entidad externa (A.AUD).
43. **AUD.5** El producto debe ser capaz de eliminar o sobrescribir registros de auditoría anteriores cuando el espacio de almacenamiento esté lleno (A.AUD).

4.7 PROTECCIÓN CONTRA FALLOS

44. **PRO.1** El producto deberá ser capaz de realizar un test (durante el arranque o encendido del producto, periódicamente durante la operación normal del producto y a petición de un usuario autorizado) para demostrar el funcionamiento correcto del producto determinado previamente (A.FUN).

4.8 PROXIES

45. **FLU.1** Los paquetes de comunicaciones recibidos por una interfaz de red serán reproducidos por el producto en un nuevo paquete, conforme al protocolo utilizado en la comunicación, que será enviado a su destinatario a través de una conexión establecida por otra interfaz de red entre el producto y dicho destinatario.
46. **FLU.2** La información sobre el origen de los flujos de información de salida, desde la red interna hacia la externa, deberá poder ser eliminada, de forma que sea imposible distinguir su origen dentro de la red interna o protegida (p.ej.: direccionamiento IP del equipo que origina la comunicación) o facilitar información de la arquitectura de red interna.
47. **FLU.3** El producto debe asegurar que el contenido de los datos (*payload*), una vez utilizados para su transmisión o recepción, deja de estar disponible y no se reutiliza.
48. **FLU.4** El producto debe proporcionar la funcionalidad necesaria para permitir romper la continuidad de las comunicaciones que usen protocolos cifrados (p.ej.: HTTPS[4]).
49. **FLU.5** El producto debe permitir aplicar políticas de seguridad o restricciones aplicables a los flujos de información (p.ej.: volumen máximo de datos admitidos).

[4] *Hypertext Transfer Protocol Secure*. Protocolo seguro de transferencia de hipertexto

50. **FLU.6** El producto debe tener la capacidad de aplicar políticas de configuración que incluyan lista de aplicaciones blancas (explícitamente autorizadas) y negras (explícitamente denegadas). Dichas listas deberán permitir ser configuradas, al menos, en base a direcciones, puertos y protocolos utilizados para sus comunicaciones.
51. **FLU.7** El producto no permitirá los flujos de información entre ambas interfaces que no se ajusten a las políticas de seguridad y/o restricciones configuradas conforme a los dos requisitos anteriores.

5. ABREVIATURAS

CC	*Common Criteria*
CCDB	*Common Criteria Development Board*
CCN	*Centro Criptológico Nacional*
CPSTIC	*Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones*
EAL	*Evaluation Assurance Level*
ENS	*Esquema Nacional de Seguridad*
HTTPS	*Hypertext Transfer Protocol Secure*
IP	*Internet Protocol*
NIAP	*National Information Assurance Partnership*
OSI	*Open System Interconnection*
RFS	*Requisitos Fundamentales de Seguridad*
SFR	*Security Functional Requirements*