centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo D.4: *Proxies*

Agosto 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN 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
2020.08.10 10:00:52 +02'00'

NIPO: 083-19-053-9.

Fecha de Edición: Agosto 2020
ISDEFE ha participado en el desarrollo del presente documento.

ÍNDICE

1. INTRODUCCIÓN Y OBJETO 4
2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS 5
2.1 FUNCIONALIDAD 5
2.2 CASOS DE USO 5
2.2.1. CASO DE USO 1 - INTERMEDIARIO EN LA CONEXIÓN 6
2.3 ENTORNO DE USO 6
2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO 7
2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA) 7
3. ANÁLISIS DE AMENAZAS 8
3.1 RECURSOS QUE ES NECESARIO PROTEGER 8
3.2 AMENAZAS 8
4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS) 9
4.1 PERFIL DE PROTECCIÓN 9
4.2 REQUISITOS CRIPTOGRÁFICOS 10
4.3 CONTROL DE LOS FLUJOS DE INFORMACIÓN 10
5. ABREVIATURAS 12

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). 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.

[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).

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 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.

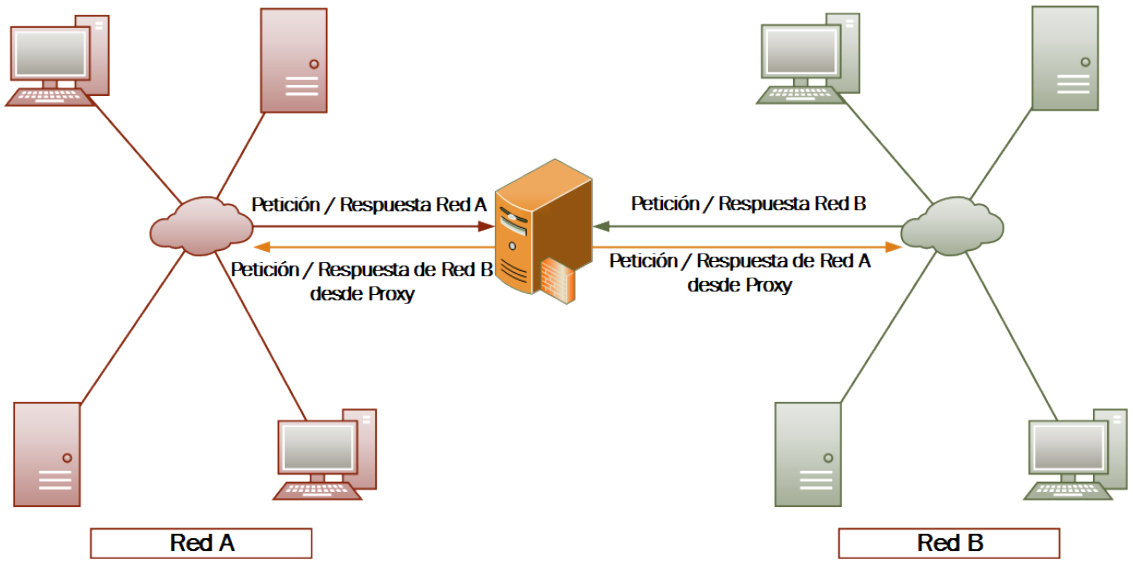

Figura 1 – Ejemplo de Caso de Uso: Intermediario en la conexión

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.
    - **Funcionalidad limitada**: El producto deberá utilizarse para el enmascaramiento y filtrado de las conexiones como su función básica y no proporcionar ninguna otra funcionalidad, salvo aquellas determinadas compatibles orientadas a la protección de las comunicaciones.
    - **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 4, éstas quedan fuera del alcance analizado, debiendo ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

18. E 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).
19. 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.
20. Los productos dentro de esta familia deberán estar certificados de acuerdo a la norma *Common Criteria*. Dicha certificación deberá evidenciar el problema de

[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)

seguridad definido en el presente documento e incluir los requisitos fundamentales de seguridad recogidos en el apartado 4.

21. 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.

22. 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

23. Los recursos que deben protegerse mediante el uso de estos productos son:

    - Información que atraviese el producto, que provenga de los equipos y dispositivos para los cuales se realiza la función de intermediario, en ambos sentidos.
    - Interfaces de gestión del producto e información transmitida a través de ellas, en ambos sentidos.
    - 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

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

    - **Divulgación de información no autorizada:** Un atacante ya sea desde dentro de la red o desde fuera consigue enviar información no autorizada de la red interna al exterior a través del dispositivo (p.ej.: direccionamiento IP de la red protegida o mapa de dispositivos de la red).
    - **Acceso no autorizado**: Un atacante ya sea desde dentro de la red o desde fuera consigue acceder a información intercambiada a través del dispositivo para la que no estaba autorizado (p.ej.: recibir información transmitida a

través del dispositivo, pero no destinada a él) o utilizar el dispositivo como mecanismo de acceso a la red protegida.

- **Envío de tráfico dañino**: Un atacante ya sea desde dentro de la red o desde fuera consigue eludir las políticas de filtrado configuradas y/o enviar información no autorizada desde el exterior a la red interna a través del dispositivo (p.ej.: introducir información maliciosa de manera encubierta proveniente de la red externa).
- **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 o utilización de protocolos no estandarizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones del dispositivo.
- **Compromiso de la funcionalidad del dispositivo**: Un atacante o un fallo en el dispositivo compromete la funcionalidad de seguridad, incluyendo el enmascaramiento, filtrado y registro de actividad, permitiendo modificarla o desactivarla de manera no conforme a las políticas de seguridad (p.ej. instalación de actualizaciones maliciosas o administración no autorizada del dispositivo).

4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS)

25. 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 PERFIL DE PROTECCIÓN

26. **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

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

4.2 REQUISITOS CRIPTOGRÁFICOS

28. **REQ. 3** 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 Criptología de empleo en el ENS (Categoría ALTA).

4.3 CONTROL DE LOS FLUJOS DE INFORMACIÓN

29. **REQ. 4** El producto debe tener la capacidad de conectarse a dos interfaces de red entre las que debe transmitir la información, identificando claramente, física y lógicamente, cada una de las redes.

30. **REQ. 5** 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.

[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

31. **REQ. 6** 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.
32. **REQ. 7** El producto debe filtrar y evitar el uso de campos no aplicables, irrelevantes o innecesarios de los protocolos de comunicación que utilice, que pudieran permitir la ocultación y transmisión encubierta de información no autorizada o relativa a la configuración de la red interna.
33. **REQ. 8** El producto debe asegurar que el contenido de los datos (*payload*) del paquete no se modifica desde que entra por una interfaz hasta que sale por la otra.
34. **REQ. 9** 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.
35. **REQ. 10** El producto debe ser capaz de mantener la coherencia en las comunicaciones para los flujos de información de entrada en la red protegida, recomponiendo las cabeceras del protocolo con los datos necesarios para que la comunicación sea viable y alcance al destinatario correcto dentro de la red interna.
36. **REQ. 11** El producto debe proporcionar la funcionalidad necesaria para permitir romper la continuidad de las comunicaciones que usen protocolos cifrados (p.ej.: HTTPS[7]).
37. **REQ. 12** El producto debe permitir aplicar políticas de seguridad o restricciones aplicables a los flujos de información (p.ej.: volumen máximo de datos admitidos).
38. **REQ. 13** 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.
39. **REQ. 14** 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.

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

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*