GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo C.3: Captura, Monitorización y Análisis de Tráfico

Noviembre 2017

Edita:

GOBIERNO DE ESPAÑA
MINISTERIO DE LA PRESIDENCIA Y PARA LAS ADMINISTRACIONES TERRITORIALES

CCN Centro Criptológico Nacional

CENTRO CRIPTOLOGICO NACIONAL
2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, cn=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2017.11.27 11:19:43 +01'00'

NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017
ISDEFE ha participado en el desarrollo del presente documento y sus anexos.

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Captura, Monitorización y Análisis de Tráfico** 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 **Captura, Monitorización y Análisis de Tráfico** 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 monitorización, captura y análisis de tráfico, con el objeto de identificar los elementos significativos de la red y corregir problemas funcionales. Mediante el análisis de paquetes/tramas de datos y protocolos de comunicaciones, consiguen prevenir fallos, detectar amenazas, y ayudar a tomar decisiones correctas en relación al planeamiento de la red.
7. Dichos productos proporcionan apoyo al administrador en el correcto funcionamiento y mantenimiento del entorno a su cargo.
8. En este contexto, las funcionalidades básicas que desarrollan esta familia de productos son las siguientes:
    - Capturan y analizan el tráfico de red, visualizando tanto las cabeceras como el contenido de las tramas de datos.
    - Permiten adecuar la monitorización y el análisis a las necesidades de seguridad mediante distintos mecanismos:
        - Aplicación de filtros para limitar el número de paquetes que se capturan o se visualizan.
        - Aplicación de filtros teniendo en cuenta los paquetes que pertenezcan a determinados protocolos de red.
        - Elaboración de informes según diversos criterios impuestos por la entidad.

2.2 CASOS DE USO

9. En el caso de los productos de esta familia se contempla un caso de uso.

2.2.1. CASO DE USO 1 – DISPOSITIVO INTEGRADO EN LA RED

10. La herramienta debe tener un conocimiento completo de la red y de los elementos de comunicación que la componen para poder obtener información completa y fehaciente. En primer lugar, el producto monitorizará el tráfico en tiempo real y lo volcará en un fichero, mediante perfiles de tráfico, previamente definidos, y la aplicación mostrará la información recolectada, con el objetivo de identificar anomalías en la red.

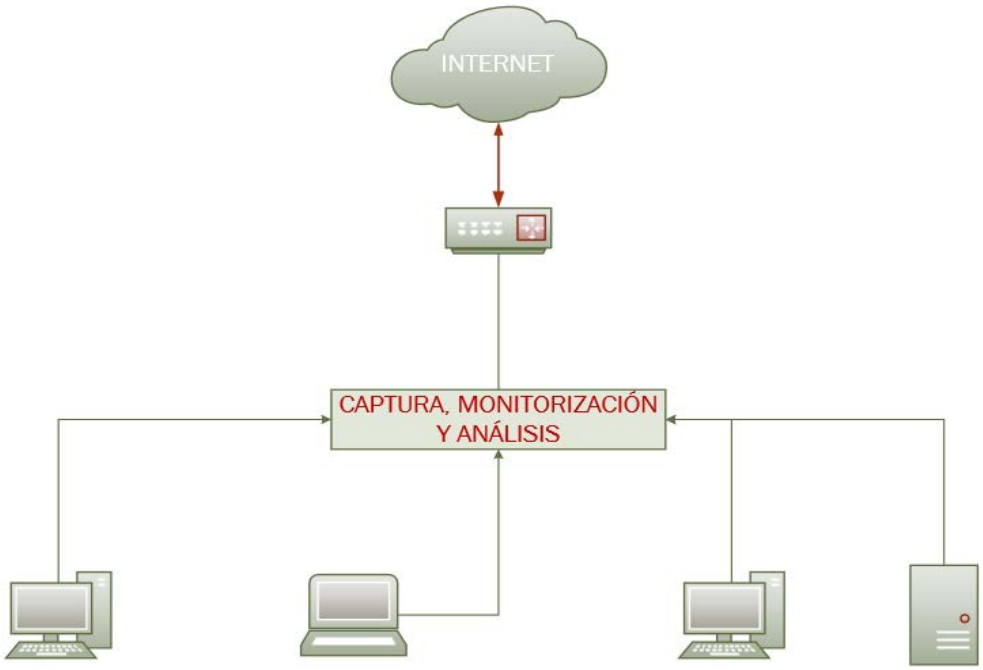

Figura 1. Ejemplo de Caso de Uso 1: Dispositivo integrado en la red.

2.3 ENTORNO DE USO

11. Por lo general, este tipo de dispositivos son de uso generalizado en cualquier ámbito para la implementación de redes informáticas y de comunicaciones, tanto en el caso de redes desplegadas para usuarios privados, empresas o el sector público, como en las infraestructuras de los proveedores de servicios de internet (ISP[1]).

12. Para la utilización en condiciones óptimas de seguridad, es necesaria su integración en un entorno operacional que cumpla las siguientes 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.
    - **Administración confiable**. El 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 capacitada, formada y carecerá de cualquier intención dañina al administrar el producto.
    - **Actualizaciones periódicas**. El producto será puesto al día conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
    - **Política de seguridad de la Información.** La política de seguridad deberá recoger el conjunto de principios, procedimientos y marco organizativo

[1] *Internet Service Provider.* Proveedor del Servicio de Internet.

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

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

13. Este tipo de productos se presentan en formato de paquete **Software** que se instala en dispositivos **Hardware** con las funcionalidades necesarias para cumplir su finalidad y acotadas al servicio específico que presten.
14. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, 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)

15. El estándar *Common Criteria* (CC)proporciona un conjunto común de requisitos funcionales y de aseguramiento para la evaluación de los productos de TI (Tecnologías de la Información).
16. 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.
17. Los productos dentro de esta familia deberán cumplir con los SFR (*Security Functional Requirements*) que se especifican en el siguiente perfil de protección certificado de acuerdo a la norma *Common Criteria*, junto con los restantes requisitos fundamentales de seguridad recogidos en la sección 4:

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Application Software.	1.2	25/04/2016	NIAP
Collaborative Protection Profile for Network Devices.[2]	1.0	27/02/2015	CCDB
Protection Profile for Network Devices.[3]	1.1	08/06/2012	NIAP

Tabla 1. Perfiles de protección

18. El nivel de confianza EAL (*Evaluation Assurance Level*) con el que deben ser evaluados los requisitos exigidos para esta familia será:

[2] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf
[3] https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V1.1.pdf

- **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** para los RFS adicionales que no encuentren incluidos dentro de un perfil.
- **EAL2 o superior** en el caso en el que el producto no se encuentre certificado contra ningún perfil.

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

19. Los recursos a proteger mediante el uso de estos productos, así como para su correcto funcionamiento, incluyen:

    - Información sensible obtenida a partir del tráfico de red capturado por el producto.
    - Interfaces de gestión del producto y la 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

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

    - **Escucha de red.** Un atacante se coloca en una conexión inalámbrica o en otro lugar de la infraestructura de red. El atacante puede supervisar y obtener el acceso a la comunicación y/o los datos intercambiados entre el producto y otros puntos finales de la red.
    - **Divulgación de la información no autorizada.** Un atacante consigue recopilar información no autorizada del dispositivo (p. ej., servicios de la organización, credenciales, etc.).
    - **Uso de canales de comunicación inseguros.** Permiten a un atacante comprometer la integridad y la confidencialidad de las comunicaciones del producto. El atacante puede tener acceso a la red o a partes de la red que contienen tráfico acerca de las políticas del servidor, manejo de fuentes y repositorios de políticas de seguridad.
    - **Compromiso de la funcionalidad del dispositivo.** Un atacante o un fallo en el dispositivo compromete la funcionalidad de seguridad, 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).
    - **Cifrado débil.** Utilización en el dispositivo de algoritmos criptográficos débiles que permitan a un atacante comprometerlo, fundamentalmente, mediante ataques de fuerza bruta.
    - **Acceso no autorizado.** Un atacante consigue acceder a información, intercambiada a través del producto, así como generada o almacenada en él,

para la que no estaba autorizado (p.ej., información almacenada en memoria).

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 PERFIL DE PROTECCIÓN

4.1.1. PRODUCTO APPLIANCE

22. **REQ. 1** En caso de que el producto sea un equipo dedicado o *Appliance,* deberá estar certificado con uno de los siguientes perfiles de protección publicados certificados de acuerdo a la norma *Common Criteria:*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile for Network Devices.[4]	1.0	27/02/2015	CCDB
Protection Profile for Network Devices.[5]	1.1	08/06/2012	NIAP

Tabla 2. Perfiles de protección

23. **REQ. 2** En caso de que el producto no esté certificado contra ningún perfil de los anteriores, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) del perfil *Collaborative Protection Profile for Network Devices. Version 1.0.* con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.1.2. PRODUCTO SOFTWARE

24. **REQ. 3** En caso de que el producto sea únicamente Software ,deberá estar certificado con uno de los siguientes perfiles de protección publicados certificados de acuerdo a la norma *Common Criteria:*

PERFIL DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Protection Profile for Application Software.[6]	1.2	25/04/2016	NIAP

Tabla 3. Perfil de protección

[4] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf
[5] https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V1.1.pdf
[6] https://www.commoncriteriaportal.org/files/ppfiles/pp_app_v1.2.pdf

25. **REQ. 4** En caso de que el producto no esté certificado contra el perfil indicado, la declaración de seguridad deberá contener al menos los SFR (*Security Functional Requirements*) de éste con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.2 REQUISITOS CRIPTOGRÁFICOS

26. **REQ. 5** 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 CAPTURA, MONITORIZACIÓN Y ANÁLISIS DE TRÁFICO

27. **REQ. 6** El producto permitirá monitorizar de forma pasiva todo el trafico de red detectado por cada una de sus interfaces o sólo flujos de tráfico de red específicos.
28. **REQ. 7** El producto permitirá seleccionar que flujos de tráfico de red almacenar y analizar basándose en al menos los siguientes parámetros:
    a. Dirección IP de origen
    b. Dirección IP de destino
    c. Puerto de origen
    d. Puerto de destino
    e. Protocolo
29. **REQ. 8** El producto deberá ser capaz de analizar, al menos, los siguientes protocolos de red:
    a. *Internet Protocol* (IPv4), RFC 791
    b. *Internet Protocol* versión 6 (IPv6), RFC 2460
    c. *Internet Protocol message Protocol* versión 4 (ICMPv4), RFC 792
    d. *Internet Protocol message Protocol* versión 6 (ICMPv4), RFC 2463
    e. *Transmission Control Protocol* (TCP), RFC 793
    f. *User Data Protocol* (UDP), RFC 768
30. **REQ. 9** El producto deberá ser capaz de analizar el contenido de al menos los siguientes campos de las cabeceras de los paquetes:

    a. **IPv4**: version; header lenght; packet length; id; ip flags; fragment offset; time to live; protocol; header checksum; source address; destination address y ip options.

b. **IPv6**: Version; payload length, next header; hop limit; source address; destination address y routing header.

c. **ICMP**: type; code y header checksum.

d. **ICMPv6**: type; code y header checksum.

e. **TCP**: source port, destination port, sequence number, acknowledgement number; offset; reserved; TCP flags; window; checksum; urgent pointer y TCP options.

f. **UDP**: Source port, destination port; length y UDP checksum.

31. **REQ. 10** El producto deberá ser capaz de analizar la carga útil de los paquetes, identificando cadenas de caracteres definidas en una lista personalizable por el usuario.

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*
DHCP	*Dynamic Host Configuration Protocol*
EAL	*Evaluation Assurance Level*
ENS	*Esquema Nacional de Seguridad*
GRE	*Generic Routing Encapsulation*
ICMP	*Internet Protocol Message Protocol*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
NIAP	*National Information Assurance Partnership*
RFS	*Requisitos Fundamentales de Seguridad*
SFR	*Security Functional Requirements*
TCP	*Transmission Control Protocol*
TIC	*Tecnología de la información y comunicación*
UDP	*User Data Protocol*