centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de referencia para productos de seguridad TIC - Anexo D.3: Cortafuegos

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 10:02:21 +02'00'

NIPO: 083-19-053-9.

Fecha de Edición: Agosto 2020

ÍNDICE

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Cortafuegos** 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 **Cortafuegos** 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 la familia Cortafuegos están orientados a la protección de interconexiones, fundamentalmente para permitir, limitar, cifrar

y/o descifrar el tráfico hacia o desde una red a la que protegen en base a un conjunto de normas y otros criterios establecidos por un usuario administrador.

7. Estos dispositivos interconectan dos o más redes, de forma que todas las comunicaciones que se establezcan entredichas redes pasen a través del cortafuegos, con objeto de examinar cada mensaje y bloquear aquellos que no cumplan los criterios de seguridad especificados.
8. En este contexto proporcionan las siguientes funciones básicas de seguridad:
   - Protección frente al tráfico de red externo a la red que protegen limitando los paquetes entrantes en función de la política aplicada.
   - Protección frente a ataque internos.
   - Restricción de acceso al exterior para elementos de la red interna. Sólo se permite la salida a aquellos dispositivos o usuarios especificados en la política aplicada.
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]y en particular se contemplan en este documento a nivel de red (capa 3) y nivel de transporte (capa 4).
10. Los productos incluidos en esta familia pueden ofrecer otras funcionalidades complementarias (p.ej. redes virtuales privadas o *proxy*), que deberán cumplir con los RFS de la familia correspondiente.

2.2 CASOS DE USO

11. Dependiendo de las funcionalidades del producto explotadas y de la finalidad o el contexto en que se utilicen, se contemplan dos casos de uso para esta familia de productos tal y como se definen a continuación.

2.2.1. CASO DE USO 1 - DISPOSITIVO FRONTERA

12. El dispositivo se encuentra en una zona donde protege una red frente a una red exterior, como por ejemplo Internet.

[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).

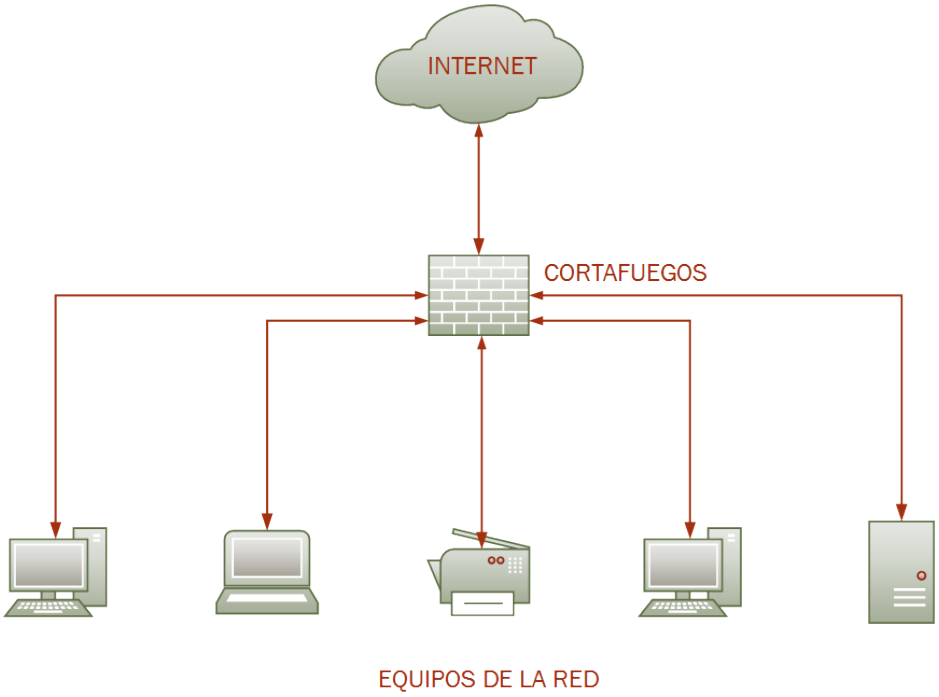

Figura 1 - Ejemplo de Caso de uso 1-Dispositivo frontera

2.2.2. CASO DE USO 2- SEGMENTACIÓN DE REDES

13. El dispositivo se encuentra en una zona donde protege dos redes internas entre sí, es decir, segmenta ambas redes y permite que únicamente el tráfico autorizado fluya de una a otra. El principal problema de este tipo de configuración será el de controlar los accesos entre las redes para limitarlos únicamente a los dispositivos deseados.

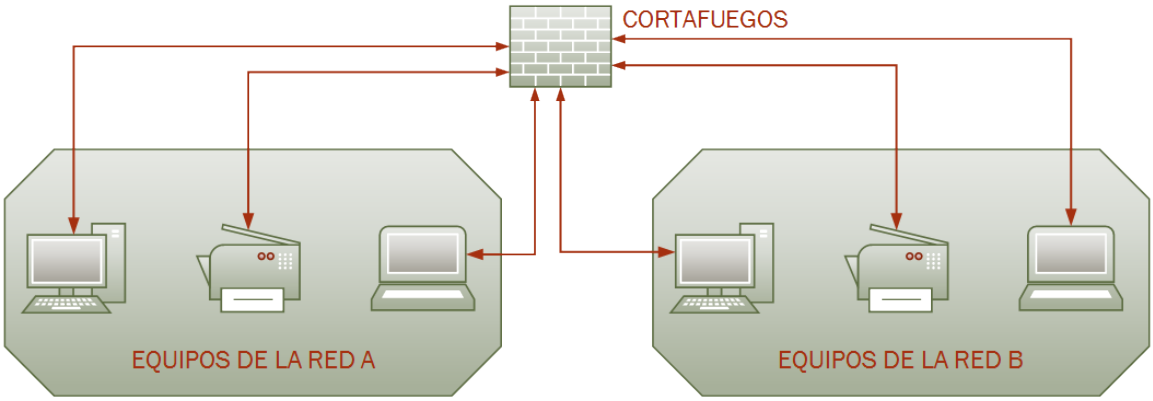

Figura 1 – Ejemplo de Caso de Uso 2: Segmentación de Redes

2.3 ENTORNO DE USO

14. Por lo general este tipo de dispositivos se encuentran en grandes o medianas empresas, así como en redes del sector público como parte de una arquitectura

de defensa en profundidad, existiendo medidas complementarias en diferentes capas de protección.

15. 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 enrutamiento y filtrado de red como su función básica y no proporcionar ninguna otra funcionalidad, salvo aquellas determinadas compatibles orientadas a la protección de las comunicaciones.
    - **Administración confiable**: El usuario administrador será un miembro de plena confianza y que vela por los mejores intereses en materia de seguridad de la organización. 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.
    - **Protección de las credenciales**: Todas las credenciales, en especial la del administrador, deberán estar correctamente protegidas por parte de la organización que utilice el producto.
    - **Política de seguridad de la información**: Una política de seguridad deberá recoger el conjunto de principios, organización y procedimientos impuestos por una organización para hacer frente a sus necesidades de seguridad de la información, incluyendo el uso de las TIC.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

16. Este tipo de productos se presentan en formato de equipo dedicado o (***Appliance:*** hardware provisto de firmware y software dedicado) con las funcionalidades necesarias para cumplir su finalidad y acotadas al servicio específico que presten. En caso de ofrecer funcionalidades adicionales a las definidas en la sección 2.1, éstas quedan fuera del alcance analizado, debiendo ser evaluadas conforme a los RFS específicos aplicables a tales funcionalidades complementarias.

17. En ocasiones pueden ir acompañados de ***Software*** instalable en un equipo informático estándar que sirva para realizar las funciones de control y administración del dispositivo.

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

18. 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 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 es necesario proteger mediante el uso de esta familia de productos, incluyen:
    - Dispositivos de red y subredes asociadas a la interfaz interna a la que se conecta el producto.
    - Información que atraviese el producto entre sus interfaces de red.
    - 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

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 consigue recopilar información no autorizada de una red desde otra, a través del dispositivo (p.ej. direccionamiento IP o mapa de dispositivos de la red).
- **Acceso no autorizado**: Un atacante consigue acceder a información intercambiada a través del dispositivo para la que no estaba autorizado (p.ej. recibir información transmitida entre dos interfaces pero no destinada a él) o utilizar el dispositivo como mecanismo de acceso a los recursos y servicios de una red para los que no está autorizado.
- **Envío de tráfico dañino**: Un atacante consigue enviar información a través del dispositivo de manera malintencionada, con el fin de poner en riesgo la seguridad de éste o de aquellos otros recursos a los que protege (p.ej. provocar una denegación de servicio).
- **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.
- **Mal uso de los servicios**: Uso no autorizado e inapropiado de los servicios que proporciona el dispositivo o la infraestructura que protege, en detrimento de éstos o en beneficio del atacante.
- **Compromiso de la funcionalidad del dispositivo**: Un atacante o un fallo en el dispositivo compromete la funcionalidad de seguridad, incluyendo el enrutamiento, 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[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 1. 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**.

28. **REQ.3.** Los productos deberán estar certificados con uno de los siguientes perfiles de protección de acuerdo a la norma *Common Criteria:*

PERFILES DE PROTECCIÓN			
Perfil de protección	**Versión**	**Fecha**	**Organismo responsable**
Collaborative Protection Profile Module for Stateful Traffic Filter Firewall.[6]	1.3	27/09/2019	*CCDB*
Collaborative Protection Profile for Stateful Traffic Filter Firewall.[7]	2.0E	14/03/2018	*CCDB*
Collaborative Protection Profile for Stateful Traffic Filter Firewall.[8]	1.0	27/02/2015	*CCDB*

Tabla 2. Perfiles de protección

[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
[6] https://www.commoncriteriaportal.org/files/ppfiles/MOD_CPP_FW_V1.3.pdf
[7] https://www.commoncriteriaportal.org/files/ppfiles/CPP_FW_V2.0.pdf
[8] https://www.commoncriteriaportal.org/files/ppfiles/CPP_FW_V1.0.pdf

29. **REQ.4.** 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 Module for Stateful Traffic Filter Firewall v1.3* con un nivel de confianza EAL (*Evaluation Assurance Level*) **EAL2 o superior**.

4.2 REQUISITOS CRIPTOGRÁFICOS

30. **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).

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*
IP	*Internet Protocol*
ISP	*Internet Service Provider*
NIAP	*National Information Assurance Partnership*
OSI	*Open System Interconnection*
RFS	*Requisitos Fundamentales de Seguridad*
SFR	*Security Functional Requirements*