

Edita:



© Centro Criptológico Nacional, 2017

NIPO: 785-17-037-2.

Fecha de Edición: noviembre 2017

ISDEFE ha participado en el desarrollo del presente documento y sus anexos.

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

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

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 - DISPOSITIVO FRONTERA.....	5
2.2.2. CASO DE USO 2- SEGMENTACIÓN DE REDES	6
2.3 ENTORNO DE USO	7
2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO.....	7
2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)	8
3. ANÁLISIS DE AMENAZAS	9
3.1 RECURSOS QUE ES NECESARIO PROTEGER.....	9
3.2 AMENAZAS	9
4. REQUISITOS FUNDAMENTALES DE SEGURIDAD (RFS).....	10
4.1 PERFIL DE PROTECCIÓN	10
4.2 REQUISITOS CRIPTOGRÁFICOS.....	10
5. ABREVIATURAS	11

1. INTRODUCCIÓN Y OBJETO

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia **Enrutadores** 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 **Enrutadores** 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 facilitar la interconexión de dos o más redes, encaminando los paquetes de datos entre ellas, a la vez que proporcionan determinados mecanismos de protección. Fundamentalmente proveen conectividad a nivel de red (capa 3) conforme al modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1)¹.
7. Su función principal consiste en enviar o encaminar paquetes de datos de una red a otra, es decir, interconectar subredes, entendiendo por subred un conjunto de máquinas IP² que se pueden comunicar sin la intervención de un enrutador (mediante puentes de red), y que por tanto tienen prefijos de red distintos.
8. En este contexto proporcionan las siguientes funciones básicas de seguridad:
 - Administración de puertos, habilitándolos o deshabilitándolos para su uso, así como asignándoles prioridades.
 - Reenvío o encaminamiento entre las diferentes interfaces y filtrado del tráfico de red en función de listas de control de acceso (ACLs³), en base a: dirección IP, dirección MAC⁴, tipo de protocolo o puerto de uso (en origen o destino).
9. Los productos incluidos en esta familia pueden ofrecer otras funcionalidades complementarias (p.ej. redes virtuales privadas o comunicaciones inalámbricas) no específicamente contempladas en este documento.

2.2 CASOS DE USO

10. 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

11. El dispositivo se encuentra en una zona donde protege una red frente al exterior, es decir, frente a Internet. En estos casos el dispositivo debe aplicar una política muy agresiva de protección ya que los posibles ataques pueden venir desde cualquier sitio y ser de cualquier tipo.

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 *Internet Protocol*

³ *Access Control List*

⁴ *Media Access Control*

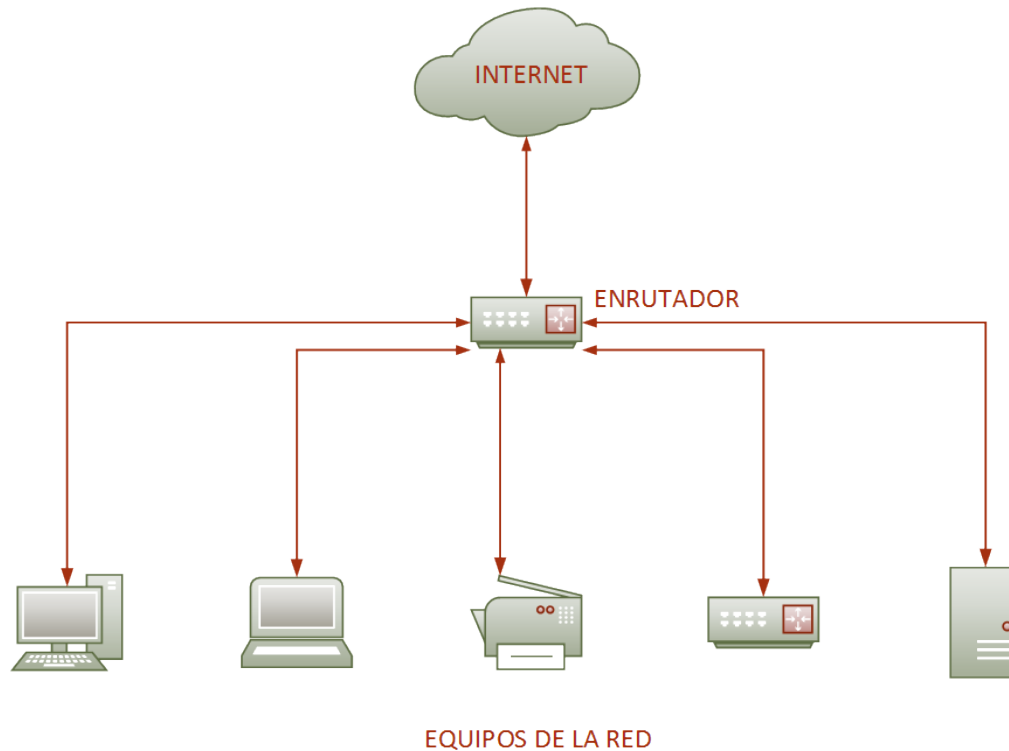


Figura 1-Caso de uso 1-Dispositivo frontera

2.2.2. CASO DE USO 2- SEGMENTACIÓN DE REDES

12. El dispositivo se encuentra en una zona donde protege dos o más redes internas entre sí, es decir, segmenta las redes que están bajo su control permitiendo únicamente que el tráfico autorizado fluya entre ellas. En estos casos el dispositivo podría aplicar una política algo menos restrictiva de protección ya que a priori no existe una exposición a redes inseguras como Internet, siendo el principal problema el de controlar los accesos entre las redes para limitarlos únicamente a los dispositivos deseados.

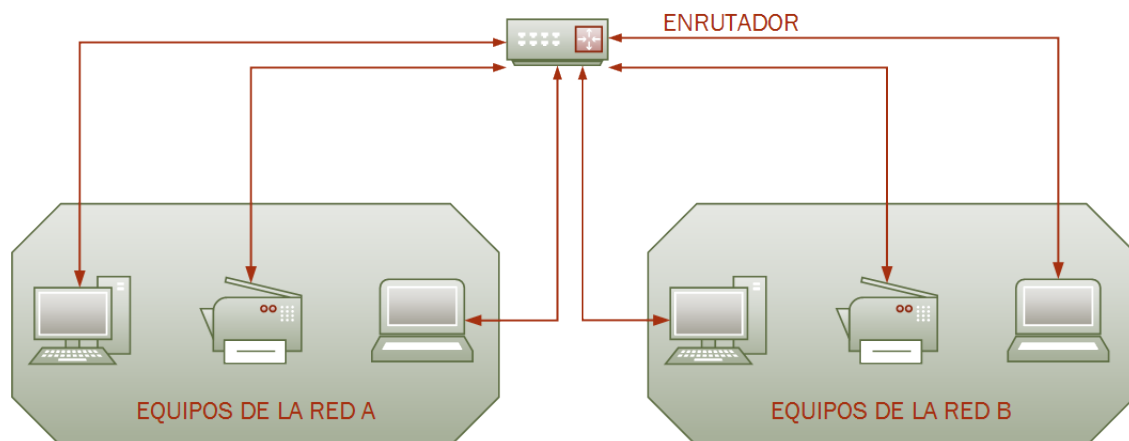


Figura 1 – Ejemplo de Caso de Uso 2: Segmentación de Redes

2.3 ENTORNO DE USO

13. Este tipo de dispositivos son de uso generalizado en cualquier tipo de ámbito, debido a su trascendencia para la implementación de redes informáticas y de comunicaciones, tanto en el caso de redes desplegadas para usuarios privados, empresas u organismos del sector público, como en las infraestructuras de los proveedores de servicios de internet (ISP⁵).
14. Para la utilización en condiciones óptimas de seguridad de estos dispositivos, es necesario que se integre 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 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
 - **Actualizaciones periódicas:** El 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

15. Este tipo de productos se presentan en formato de **Equipo dedicado** o (**Appliance:** hardware provisto de firmware 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.

⁵Internet Service Provider

2.5 ALINEAMIENTO CON CRITERIOS COMUNES (COMMON CRITERIA)

16. 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).
17. 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.
18. Los productos dentro de esta familia deberán cumplir con los requisitos Fundamentales de Seguridad reflejados en el apartado 4 y con los SFR (*Security Functional Requirements*) que se especifican en alguno de los siguientes perfiles de protección certificados de acuerdo a la norma *Common Criteria*:

PERFILES DE PROTECCIÓN			
Perfil de protección	Versión	Fecha	Organismo responsable
<i>Collaborative Protection Profile for Network Devices.</i> ⁶	1.0	27/02/2015	CCDB
<i>Protection Profile for Network Devices.</i> ⁷	1.1	08/06/2012	NIAP

Tabla 1. Perfiles de protección

19. 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 del perfil *Collaborative Protection Profile for Network Devices. Version 1.0* con un nivel de confianza EAL (Evaluation Assurance Level) **EAL2 o superior**.

⁶https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V1.0.pdf

⁷https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V1.1.pdf

3. ANÁLISIS DE AMENAZAS

3.1 RECURSOS QUE ES NECESARIO PROTEGER

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

21. 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 (p.ej. acceder a un segmento de red no 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.
 - **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)

22. 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

23. **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
<i>Collaborative Protection Profile for Network Devices.</i> ⁸	1.0	27/02/2015	CCDB
<i>Protection Profile for Network Devices.</i> ⁹	1.1	08/06/2012	NIAP

Tabla 2. Perfiles de protección

24. **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**.

4.2 REQUISITOS CRIPTOGRÁFICOS

25. **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).

⁸https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf

⁹https://www.commoncriteriaportal.org/files/ppfiles/PP_ND_V1.1.pdf

5. ABREVIATURAS

ACL	<i>Access Control List</i>
CC	<i>Common Criteria</i>
CCDB	<i>Common Criteria Development Board</i>
CCN	Centro Criptológico Nacional
CPSTIC	Catálogo de Productos de Seguridad de las Tecnologías de Información y las Comunicaciones
EAL	<i>Evaluation Assurance Level</i>
IP	<i>Internet Protocol</i>
ISP	<i>Internet Service Provider</i>
MAC	<i>Media Access Control</i>
NIAP	<i>National Information Assurance Partnership</i>
OSI	<i>Open System Interconnection</i>
RFS	Requisitos Fundamentales de Seguridad
SFR	<i>Security Functional Requirements</i>
SW	Software