centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos de STIC - Anexo D.2: Switches

Agosto 2020

MINISTERIO DE DEFENSA

Edita:

MINISTERIO DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN
centro criptológico nacional

NIPO: 083-19-053-9

Fecha de Edición: Agosto 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 3
2. DESCRIPCIÓN DE LA FAMILIA DE PRODUCTOS 4
2.1 FUNCIONALIDAD 4
2.2 CASOS DE USO 4
2.2.1. CASO DE USO 1 - UNIÓN DE SEGMENTOS DE UNA RED 5
2.2.2. CASO DE USO 2- CREACIÓN DE REDES VIRTUALES DENTRO DE UNA RED FÍSICA 5
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 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 de ***Switches*** 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 ***Switches*** 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 se utilizan para interconectar los segmentos físicos de una red y habilitar la circulación de datos entre dichos segmentos. Los conmutadores trabajan a nivel de enlace (capa 2) del modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1)[1]y dirigen el tráfico según direccionamiento físico o Media Access Control (MAC[2]) de Ethernet. Algunos conmutadores también ofrecen funciones adicionales tales como segmentación de redes virtuales (VLAN[3]) y conmutación a nivel de red (capa 3).
7. Salvo que existan características avanzadas que deban configurarse de manera específica siendo un dispositivo “administrado” (p.ej.: VLANs), el conmutador no requiere configuración ya que ésta es automática siendo considerados como dispositivos “no administrados”. Para ello, su funcionalidad les permite escuchar el tráfico en cada puerto y descubrir en cuál está conectado cada dispositivo, para a continuación enviar el tráfico directamente al puerto de destino correspondiente. El proceso de conmutación se realiza en hardware a la velocidad que permite el cable sin prácticamente período de latencia.
8. En este contexto proporcionan las siguientes funciones básicas de seguridad:
   - Administración de puertos, asignándoles prioridades, habilitándolos o deshabilitándolos para su uso.
   - Filtrado MAC y otros tipos de funciones de "seguridad de puertos".
   - Definición de redes VLAN para la segregación en segmentos lógicos de una red.
9. Los productos incluidos en esta familia pueden ofrecer otras funcionalidades complementarias (p.ej. enrutamiento a nivel de enlace, capa 3) 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.

[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] *Media Access Control*
[3] *Virtual Local Area Network*

2.2.1. CASO DE USO 1 - UNIÓN DE SEGMENTOS DE UNA RED

11. En este caso se utiliza uno o varios conmutadores (*switches)* dentro de una red para realizar la conexión de múltiples equipos dentro del mismo segmento de red. Los equipos enviarán información por la red que pasará por los *switches* que la encauzarán hacia su destino dentro de la misma red o hacia otras redes interconectadas mediante dispositivos capaces de realizar el debido enrutamiento.

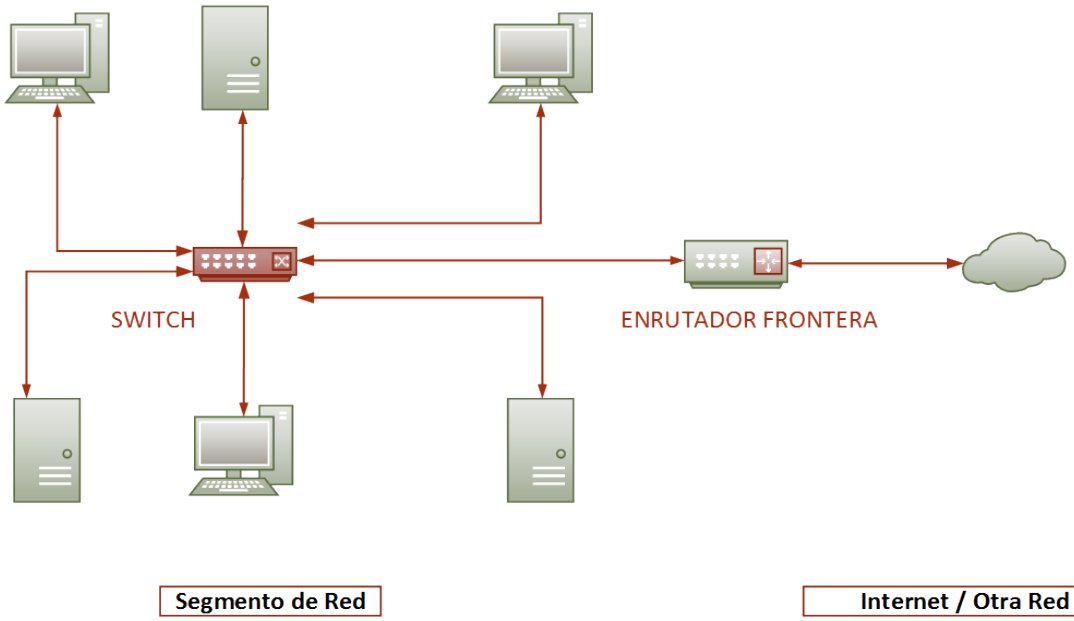

Figura 1 - Caso de uso 1-Unión de segmentos de una red

2.2.2. CASO DE USO 2- CREACIÓN DE REDES VIRTUALES DENTRO DE UNA RED FÍSICA

12. Este caso de uso es compatible con el anterior, siendo una funcionalidad añadida que se explota en determinados entornos con la intención de crear redes aisladas/segregadas de forma virtual.

13. Las Redes de Área Local Virtuales (VLAN) son redes lógicas independientes configuradas dentro de una misma red física. Varias VLAN pueden coexistir en un único conmutador físico o en una única red física. En este caso de uso, el conmutador o *switch* se utiliza para la creación de varias redes VLAN permitiendo el aislamiento de las redes virtuales (A, B y C en el ejemplo) o bien la interconexión sólo de aquellas que se desee.

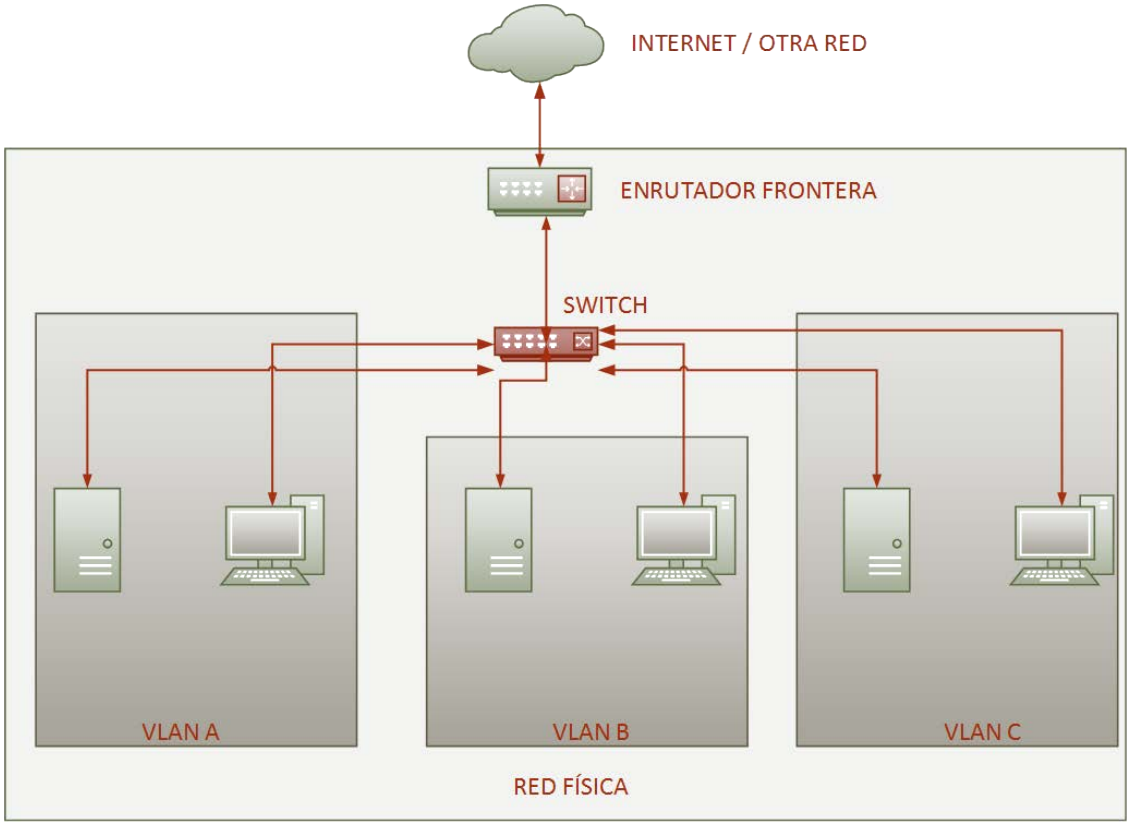

Figura 2 – Ejemplo de Caso de Uso 2: Creación de VLANs

2.3 ENTORNO DE USO

14. 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 como en empresas u organismos del sector público.

15. 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 la conmutación de redes 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 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 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 2.2, 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)

17. 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).
18. 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.
19. 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.
20. 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.
21. 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

22. 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

23. 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)

24. 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

25. **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[4]	2.2e	27/03/2020	CCDB
Collaborative Protection Profile for Network Devices[5]	2.1	24/09/2018	CCDB
Collaborative Protection Profile for Network Devices[6]	2.0 + Errata 20180314	14/03/2018	CCDB
Collaborative Protection Profile for Network Devices.7	1.0	27/02/2015	CCDB

Tabla 1. Perfiles de protección

26. **REQ. 1** 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

27. **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-807Criptología de empleo en el ENS (Categoría ALTA).

[4] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.2E.pdf
[5] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.1.pdf
[6] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V2.0E.pdf
[7] https://www.commoncriteriaportal.org/files/ppfiles/CPP_ND_V1.0.pdf

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*
MAC	*Media Access Control*
NIAP	*National Information Assurance Partnership*
OSI	*Open System Interconnection*
RFS	Requisitos Fundamentales de Seguridad
SFR	*Security Functional Requirements*
SW	Software
VLAN	*Virtual Local Area Network*