centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 140

Taxonomía de productos STIC -
Anexo C.1-M: Herramientas IDS, IPS y AntiDDoS

Noviembre de 2022

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional
CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2023.01.03 14:50:55 +01'00'

Pº de la Castellana 109, 28046 Madrid
Centro Criptológico Nacional, 2022
NIPO: 083-22-102-1

Fecha de Edición: noviembre de 2022

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

1. El presente documento describe los Requisitos Fundamentales de Seguridad (RFS) exigidos a un producto de la familia 'Herramientas IDS, IPS y AntiDDoS' para ser incluido en el apartado de Productos Cualificados del Catálogo de Productos y Servicios STIC (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) Categoría MEDIA**. 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 '**Herramientas IDS, IPS y AntiDDoS'** 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 dispositivos de prevención de intrusiones (*IPS*[1]), dispositivos de detección de intrusiones (IDS[2]) y herramientas AntiDDoS son productos cuya funcionalidad principal es la de monitorizar a una o más redes con objeto de detectar el tráfico potencialmente dañino y reaccionar ante estos ataques. Esta funcionalidad pueden implementarla de manera independiente y/o en conjunción con otros componentes de red que formen parte de soluciones empresariales mayores.

7. Aunque estos productos deben tener capacidad de monitorizar, analizar y reaccionar a tráfico de red, también podrán:

    - Monitorizar todo el tráfico de red detectado pasivamente por uno o más interfaces, y/o monitorizar solo determinados flujos de tráfico que pasan a través del producto para ser inspeccionados.
    - Transmitir datos del producto a un servidor de auditoría externo y (opcionalmente) almacenar datos internamente.
    - Analizar tráfico de red basado en reglas que el administrador puede configurar localmente y (opcionalmente) basado en reglas importadas/aplicadas desde un sistema externo.
    - Reaccionar de forma independiente a tráfico potencialmente malicioso (bloqueando flujos de tráfico o transmitiendo reinicios de sesión a los puntos finales o *endpoints*), y (opcionalmente) reaccionar en colaboración con componentes externos incluidos en la solución global de la empresa.

8. El análisis de tráfico podría estar basado en identificación de amenazas conocidas o desconocidas. La identificación conocida puede ser implementada mediante la comparación de patrones, comparando cadenas de caracteres dentro de un paquete *IP*[3], mediante reconocimiento de patrones de tráfico comunes o detectando ataques de denegación de servicio.

9. La identificación de amenazas desconocidas puede ser desarrollada mediante uso de varias formas de detección anormal que consisten en dotar al producto con patrones de tráfico típicos o esperados con objeto de que sea capaz de detectar y reaccionar ante patrones de tráfico anómalos (no esperados o atípicos).

10. Por último, es importante destacar que, aunque existen numerosas similitudes entre los IPS y los IDS, también existen notables diferencias. La más importante de ellas es que el IDS se limita a generar un evento de auditoría u otra alerta cuando detecta un flujo de tráfico malicioso, mientras que el IPS debe ser capaz de iniciar

[1] *IPS Intrusion Prevention System*
[2] *IDS: Intrusion Detection System*
[3] *IP*: *Internet Protocol*

una respuesta proactiva para terminar/interrumpir una amenaza potencial, así como causar la interrupción en tiempo real de los flujos de tráfico sospechosos.

2.2 CASO DE USO

11. Aunque el administrador del dispositivo pueda configurarlo de manera que las respuestas proactivas no estén activadas y desplegarlo solo con las funcionalidades de IDS, estos RFS aplicarán siempre a los casos en los que actúe como IPS o herramienta AntiDDoS.
12. Dependiendo de las funcionalidades del producto explotadas y de la finalidad o el contexto en que se utilicen, se contemplan tres casos de uso para esta familia de productos tal como se definen a continuación.

2.2.1. CASO DE USO 1

13. El producto está operando en **modo promiscuo**[4]. Captura datos de dos redes separadas, los analiza y envía actualizaciones de filtros de tráfico a los dispositivos de protección de perímetro (enrutador y cortafuegos o *firewall*) para que bloqueen el tráfico no deseado en tiempo real.

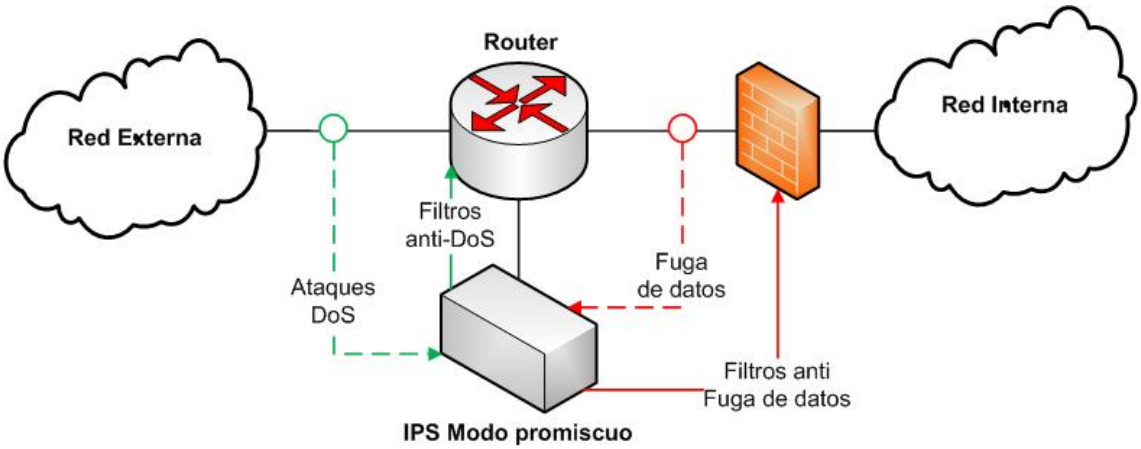

Figura 1. Modo promiscuo

2.2.2. CASO DE USO 2

14. El producto opera en **modo en línea**. Analiza tráfico desde o hacia un segmento de red y bloquea en tiempo real el tráfico que viole las políticas definidas por el administrador.

[4] Un interfaz de red que captura todos los paquetes que pasan por la red a la que está conectada, aunque no estén dirigidos a él.

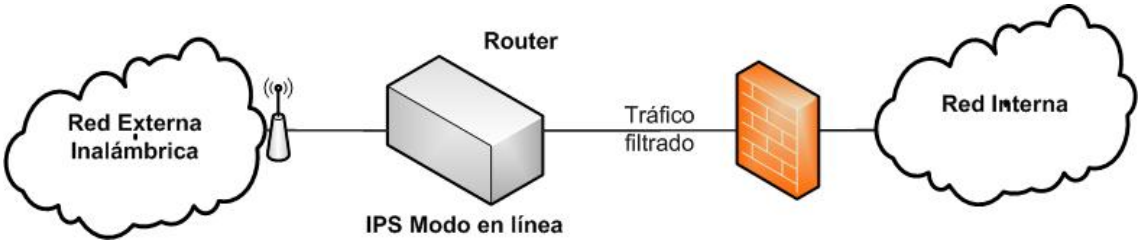

Figura 2. Modo en línea

2.2.3. CASO DE USO 3

15. El producto está operando en una **combinación de modo promiscuo y modo en línea**. Tiene al menos un par de interfaces que crean un puente *(bridge)* o enrutador que analiza y filtra en tiempo real el tráfico que lo atraviesa. Además, el mismo producto tiene uno o más interfaces promiscuos recogiendo y analizando tráfico que circula por cada red separada y reaccionando a actividad anormal, gusanos u otra actividad no aprobada.

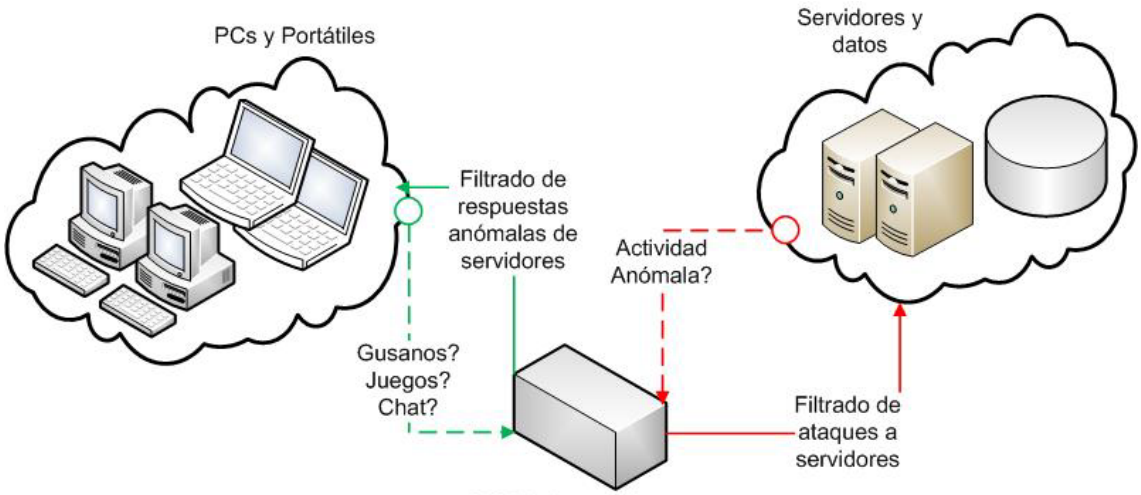

Figura 3. Modo promiscuo y en línea

2.3 HIPÓTESIS SOBRE EL ENTORNO DE EJECUCIÓN

16. Este tipo de dispositivos son de uso generalizado, tanto en el ámbito del sector público como en el privado, debido a su importancia en la mejora de la seguridad de redes, en combinación con otras medidas complementarias.
17. Para la utilización en condiciones óptimas de seguridad del producto, es necesario que se integre en un entorno de trabajo que cumpla una serie de condiciones mínimas de protección:
    - **Protección física.** El producto debe estar protegido físicamente por su entorno operacional y no sujeto a ataques físicos que puedan comprometer

su seguridad o interferir en su correcta operación. En caso de productos software, esta hipótesis aplica a la plataforma física sobre la que se ejecuta el producto.

- **Administración confiable**. Los administradores son miembros de plena confianza y velan por los mejores intereses en materia de seguridad de la organización. Dichas personas deben estar debidamente capacitadas y carecer de cualquier intención maliciosa o conflicto de intereses al administrar el producto.
- **Actualizaciones periódicas.** El *firmware/software* del producto es actualizado conforme aparezcan actualizaciones que corrijan vulnerabilidades conocidas.
- **Funcionalidad limitada.** El producto solo debe proporcionar la funcionalidad de *IDS, IPS o AntiDDOS* como función principal y no debe proporcionar ninguna otra funcionalidad o servicio.
- **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.
- **Plataforma confiable**. En caso de tratarse de un producto software, este se ejecutará sobre una plataforma confiable, incluyendo el sistema operativo o cualquier entorno de ejecución que la plataforma proporcione.

2.4 DELIMITACIÓN DEL ALCANCE DEL DISPOSITIVO

18. Los productos para los que serían de aplicación estos RFS son aquellos que inspeccionan tráfico IP (TCP[5], UDP[6], ICMP[7], etc.) y protocolos basados en IP (GRE[8], ESP[9], AH[10]).
19. No se incluyen dentro del alcance otros IPS que incluyan escáner, analizadores, sensores, etc. Ni la evaluación de otros protocolos no-IP incluyendo protocolos nivel 2 (enlace de datos) o Ethernet.
20. Además, los RFS definidos son aquellos que se consideran necesarios para un producto de prevención de intrusión, al margen de aquellas funcionalidades que pueda dar en conjunción con otros dispositivos de soluciones empresariales mayores.
21. En caso de que el IPS sea un producto distribuido a lo largo de toda la red IP el perímetro del dispositivo deberá dibujarse como la suma de todos sus componentes.

[5] *Transmission Control Protocol*. Protocolo de Control de Transmisión
[6] *User Datagram Procotol.* Protocolo de nivel de transporte de datagramas
[7] *Internet Control Message Protocol.* Protocolo de mensajes de control de Internet
[8] *Generic Routing Encapsulation* es un protocolo para el establecimiento de túneles a través de Internet
[9] *Encapsulating Security Payload*. Carga de seguridad encapsulada. Proporciona autenticidad de origen, integridad y confidencialidad de un paquete
[10] *Authentication Header.* Encabezamiento de autenticación

2.5 CERTIFICACIÓN LINCE

22. Para que un producto de esta familia pueda ser incluido en el CPSTIC bajo la categorización de ENS Categoría MEDIA, deberá disponer de una Certificación Nacional Esencial de Seguridad (LINCE)[11] que incluya los RFS reflejados en el apartado 4, que deberán ser evaluados considerando el problema de seguridad definido en el presente documento.

[11] Toda la información relativa a esta metodología se encuentra disponible en la web del Organismo de Certificación (https://oc.ccn.cni.es)

3. ANÁLISIS DE AMENAZAS

3.1 ACTIVOS SENSIBLES A PROTEGER

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

- **AC.Administración**. Interfaces de gestión del producto y la información transmitida a través de ellas, en ambos sentidos, que debe ser protegida en Confidencialidad, Trazabilidad, Autenticidad e Integridad.
- **AC.PSS.** Datos de configuración, registros auditoría y [***asignación**: listado de datos definidos por el fabricante]* que deben ser protegidos en Integridad.
- **AC.PSC**. [**selección**: credenciales; claves; [**asignación**: *listado de datos definidos por el fabricante*] que deben ser protegidos en Confidencialidad e Integridad.
- **AC.Actualizaciones**. Actualizaciones del producto susceptibles de afectar a su configuración y funcionalidad, que deben ser protegidos en Integridad y Autenticidad.
- **AC.Comunicaciones.** Comunicaciones del producto, establecidas entre sus propios componentes y con [**asignación**: *listado de entidades autorizadas*] que deben ser protegidas en Confidencialidad, Integridad y Autenticidad.

3.2 AMENAZAS

24. Las principales amenazas a las que el uso de esta familia de productos pretende hacer frente, atendiendo a los casos de uso expuestos en la sección 2.2, serían:

- **A.NOAUT Acceso no autorizado de administrador:** Un atacante puede obtener un acceso de administración no autorizado haciéndose pasar por un administrador ante el producto, haciéndose pasar por el producto ante un administrador, reproduciendo una sesión de administración, o realizando ataques del hombre en medio.
- **A.CRYPTO Mecanismos criptográficos débiles:** Utilización en el producto de mecanismos criptográficos o longitudes de clave débiles que permitan a un atacante comprometerlo, fundamentalmente mediante ataques de fuerza bruta.
- **A.COM Protocolos de comunicación no autorizados:** Utilización de protocolos no autorizados que permiten a un atacante comprometer la integridad y confidencialidad de las comunicaciones críticas del producto.
- **A.ACT Actualización maliciosa:** un atacante puede realizar una actualización maliciosa que comprometa las funcionalidades del producto.

- **A.AUD Actividades no detectadas:** Un atacante puede intentar acceder, cambiar o modificar las funcionalidades de seguridad del producto sin el conocimiento del administrador.
- **A.PSC Compromiso de parámetros de seguridad críticos:** Un atacante puede comprometer los parámetros de seguridad críticos y acceder de forma continuada al producto y a sus datos críticos.
- **A.FUN Fallo de las funcionalidades de seguridad:** Un atacante externo puede aprovechar fallos en las funcionalidades de seguridad declaradas del producto y podría acceder, cambiar o modificar información, funcionalidades de seguridad o tráfico de red en el producto.
- **A.NOAUTUSR Acceso no autorizado de usuario:** Un atacante puede obtener un acceso no autorizado haciéndose pasar por un usuario ante el producto, haciéndose pasar por el producto ante un usuario, reproduciendo una sesión de usuario, o realizando ataques del hombre en medio.
- **A.CRE Compromiso de credenciales:** Un atacante puede aprovecharse del uso credenciales débiles o desprotegidas, para ganar acceso privilegiado al producto.
- **A.RED Ataque a la red:** Un atacante consigue acceder a la red pudiendo realizar mapeos de las máquinas que residen en ella y obtener datos de dirección IP, servicios o cualquier otra información que le permita lanzar ataques a dichas máquinas y servicios, como denegación de servicio, sustracción de información o filtración de malware.

3.3 TRAZABILIDAD AMENAZAS/REQUISITOS DE SEGURIDAD

25. En la siguiente tabla se trazan que Requisitos Fundamentales de Seguridad definidos en el apartado **¡Error! No se encuentra el origen de la referencia.** cubren las amenazas definidas:

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSC	A.FUN	A.NOAUTUSR	A.CRE	A.RED
ADM.1	X									
ADM2	X									
ADM.3	X									
IAU.1	X							X		
IAU.2									X	
IAU.3									X	
IAU.4	X									
COM.1		X	X							

	A.NOAUT	A.CRYPTO	A.COM	A.ACT	A.AUD	A.PSC	A.FUN	A.NOAUTUSR	A.CRE	A.RED
COM.2			X							
COM.3			X							
COM.4		X	X							
ACT.1				X						
ACT.2				X						
ACT.3				X						
AUD.1					X					
AUD.2					X					
AUD.3					X					
AUD.4					X					
AUD.5					X					
PSC.1						X				
PRO.1										
CIF.1		X	X							
IDS.1					X					X
IDS.2										X
IDS.3										X
IDS.4										X
IDS.5										X
IDS.6										X
IDS.7										X
IDS.8										X
IPS.1										X

4. REQUISITOS DE SEGURIDAD

26. 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.

27. La convención utilizada en las descripciones de los RFS es la siguiente:

- Selección: se deberá seleccionar al menos una opción de las indicadas en el RFS y se incluirá en la declaración de seguridad. Ejemplo:

  RFS: Administración del producto [**selección***: local; remota*]

  DS: Administración del producto local y remota

- Asignación: se deberá especificar el listado de opciones que sean de aplicación al TOE (podría no haber ninguna). Ejemplo:

  RFS: El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación:** otros usuarios del producto] antes de otorgar acceso.

  DS: El TOE deberá identificar y autenticar a cada usuario administrador, auditor y usuario avanzado antes de otorgar acceso.

4.1 ADMINISTRACIÓN CONFIABLE

28. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
29. **ADM.1** El TOE debe definir, al menos, el rol de administrador y ser capaz de asociar usuarios a roles.
30. **ADM.2** El TOE debe ser capaz de realizar la gestión de las siguientes funcionalidades:
    - Administración del producto [**selección**: *local; remota*].
    - Configuración del tiempo de terminación de sesión o bloqueo al detectar inactividad.
    - [**asignación**: otras funcionalidades administrables del producto].
31. **ADM.3** El TOE deberá asegurar que solamente un usuario con permisos de administrador será capaz de realizar las funciones descritas en **ADM.2**.

> Nota de aplicación: en el caso de que existan distintos tipos de administrador, cada uno de ellos con distintos permisos, deberá probarse que únicamente pueden realizar aquellas funcionalidades para las que tengan permiso.

4.2 IDENTIFICACIÓN Y AUTENTICACIÓN

32. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

33. **IAU.1** El TOE deberá identificar y autenticar a cada usuario administrador y [**asignación**: *otros usuarios del producto*] antes de otorgar acceso, salvo para las siguientes funcionalidades [**asignación**: *listado funcionalidades*].

34. **IAU.2** El TOE deberá implementar mecanismos que impidan ataques de autenticación por fuerza bruta.

35. **IAU.3** El TOE debe disponer de la capacidad de gestión de las contraseñas:

    a) La contraseña debe poder configurarse con una longitud mínima o igual a 12 caracteres.

    b) La contraseña debe ser capaz de componerse por letras minúsculas, letras mayúsculas, números y caracteres especiales [“!”, “@”, “#”, “$”,“%”, “^”, “&”, “*”, “(“, “].

> Nota de aplicación: este requisito podría ser modificado en el caso de que el TOE implemente otros mecanismos de autenticación.

36. **IAU.4** El TOE debe [**selección***: bloquear; cerrar*] la sesión de un usuario después de [***asignación****: tiempo de inactividad*] de inactividad.

4.3 CANALES SEGUROS

37. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.

38. **COM.1** Protección de la información en tránsito. El TOE deberá establecer canales seguros cuando intercambie información sensible con entidades autorizadas: [**selección***: servidor de auditoría;* [***asignación****: otras entidades*]] o entre distintas partes del producto, usando [**selección***: IPSec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación****: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

39. **COM.2** El TOE debe permitir que los canales de comunicación definidos en **COM.1** sean iniciados por él mismo o por las entidades autorizadas.

40. **COM.3** El TOE hará uso de certificados digitales para la autenticación cuando utilice cualquiera de los protocolos definidos en **COM.1**.

41. **COM.4** Protección de la información del canal de administración. El TOE deberá establecer canales seguros cuando intercambie información con el administrador remoto, usando [**selección**: *IPsec; SSHv2 o superior; TLS 1.2 o superior; DTLS; HTTPS/TLS 1.2 o superior*] con los siguientes mecanismos criptográficos [***asignación**: listado de mecanismos o suites autorizadas de acuerdo a lo establecido en la guía CCN-STIC-807 para cada protocolo*].

4.4 CRIPTOGRAFÍA

42. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
43. **CIF.1** El TOE permitirá exclusivamente el empleo de mecanismos criptográficos: [***asignación**: listado de mecanismos*] autorizados de acuerdo a lo establecido en la guía CCN-STIC-807. La fortaleza de clave empleada será la indicada en esa guía para Categoría MEDIA del ENS, y de acuerdo al nivel de amenaza establecido.

4.5 INSTALACIÓN Y ACTUALIZACIÓN CONFIABLES

44. **ACT.1** El TOE ofrecerá la posibilidad de consultar la versión actual del firmware/software y podrá [**selección**: actualizarse automáticamente; iniciar actualizaciones manualmente] y [**selección**: comprobar si existen nuevas actualizaciones disponibles; ningún otro].
45. **ACT.2** El TOE deberá utilizar [**selección***: hashes publicados; firma digital*] que estén autorizados en la guía CCN-STIC-807 para autenticar las actualizaciones *firmware/software* antes de instalarlas.
46. **ACT.3** La actualización del *firmware/software* se permitirá únicamente a usuarios con rol de administrador.

4.6 AUDITORÍA

47. Estas funcionalidades podrán ser cubiertas por el producto o por su entorno operacional.
48. **AUD.1** El producto debe generar registros de auditoría cuando se produzca alguno de los siguientes eventos:
    a) Al inicio y finalización de las funciones de auditoría.
    b) *Login* y *logout* de usuarios registrados.
    c) Cambios en las credenciales de usuarios.
    d) Cambios en la configuración del producto [**asignación**: *listado de cambios*].
    e) Eventos relativos a la funcionalidad del producto [**asignación:** *listado de eventos*].

f) Si el TOE gestiona claves criptográficas, [**selección:** generación; importación; cambio; eliminación de claves criptográficas; ningún otro].

49. **AUD.2** Los registros de auditoría contendrán al menos la siguiente información: fecha y hora del evento, tipo de evento identificado, resultado del evento, usuario que produce el evento.

50. **AUD.3** A los registros de auditoría se aplicará la siguiente política de acceso:

    a) Lectura: usuarios autorizados.

    b) Modificación: ningún usuario.

    c) Borrado: [**selección**: solo administradores; ningún usuario]

51. **AUD.4** El TOE debe ser capaz de almacenar en sí mismo la información de auditoría generada y [**selección**: transmitir la información de auditoría generada a una entidad externa utilizando un canal seguro COM.1; no transmitir la información de auditoría generada].

52. **AUD.5** El TOE deberá [**selección**: sobreescribir los registros siguiendo el criterio de mayor antigüedad; enviar a una entidad externa y eliminar; otra opción validada por el CPSTIC] en el caso de que el espacio para almacenamiento de los registros alcance su límite.

4.7 PROTECCIÓN DE CREDENCIALES Y DATOS SENSIBLES

53. **PSC.1** En el caso en que el TOE almacene [***selección**: credenciales; claves privadas; [**asignación**: otros parámetros de seguridad críticos*] estos no deberán almacenarse en claro, sino que se utilizarán mecanismos de protección criptológica que cumplan con **CIF.1**.

4.8 PROTECCIÓN DEL PRODUCTO Y SUS SERVICIOS

54. **PRO.1** El TOE deberá ser capaz de realizar un test durante el arranque o encendido del producto, [**selección***: periódicamente durante la operación normal del producto; a petición de un usuario autorizado; ninguna*] para verificar la integridad del software/firmware, [***selección**: el correcto funcionamiento de los mecanismos criptográficos; [**asignación**: otros]; ninguno*].

4.9 DISPOSITIVOS DE PREVENCIÓN Y DETECCIÓN DE INTRUSIONES

4.9.1. AUDITORÍA Y REGISTROS DE SEGURIDAD

55. **IDS.1** El TOE generará un evento de auditoría, como mínimo, en los siguientes casos:

    a) Inicio y finalización de las funciones del producto.

    b) Cuando se produzca un evento diferenciado con respecto al resto. Se guardará junto con un sello temporal.

    c) Cuando se produzca una reacción del producto diferenciada con respecto al resto. Se guardará junto con un sello temporal.

    d) Cuando se produzcan un conjunto de eventos similares. Se guardará la descripción del evento junto con el número de ocurrencias y el período de tiempo en el que ocurrieron.

    e) Cuando se produzcan un conjunto de reacciones similares. Se guardará la descripción de la reacción junto con el número de ocurrencias y el período de tiempo en el que ocurrieron.

    f) Modificación de política de IPS, IDS o AntiDDoS, en función del tipo de producto.

    g) Tráfico inspeccionado que coincida con la política basada en anomalías del IPS, IDS o AntiDDoS, en función del tipo de producto.

    h) Trafico inspeccionado que coincida con listas blancas y negras de direcciones IP.

    i) Modificación de los interfaces asociados a cada política.

    j) Tráfico inspeccionado que coincida con la política basada en firma.

    k) Inspección de paquetes encapsulados.

    l) Fallo de reensamblado de paquete fragmentado.

    m) Normalización del tráfico realizada por el producto.

4.9.2. DETECCIÓN Y ANÁLISIS

56. **IDS.2** El TOE deberá soportar la definición de patrones de tráfico esperados y aprobados, anomalías, así como la descripción de la actividad de cada anomalía.

57. **IDS.3** El TOE deberá permitir la descripción de la actividad de las anomalías.

58. **IDS.4** El TOE permitirá la creación de listas blancas y negras de direcciones IP.

59. **IDS.5** El TOE permitirá a los administradores configurar elementos de la política de IPS como [**selección***: listas blancas y negras de direcciones; reglas; [****asignación****: otros]*].

60. **IDS.6** El TOE desarrollará un análisis del tráfico de red basado en IP y detectará violaciones de las políticas definidas por el administrador del IPS. El producto será capaz de inspeccionar, al menos, los siguientes tipos de tráfico: IPv4, IPv6, ICMPv4, ICMPv6, TCP, UDP.

61. **IDS.7** Tendrá la capacidad de inspeccionar el contenido de las cabeceras de paquetes/unidades de datos IPv4, IPv6, ICMPv4, ICMPv6, TCP, UDP y detectar las siguientes firmas basadas en cabeceras:

    a) Ataques IP: Solapamiento de fragmentos IP, IP origen y destino iguales.

    b) Ataques ICMP: Tráfico ICMP fragmentado.

    c) Ataque de ping de la muerte.

    d) Ataques TCP: *Flags TCP NULL, flags TCP SYN+FIN, flags solo TCP SYN, Flags TCP SYN+RST*

    e) Ataques UDP: Ataques bomba UDP, Ataques *DoS Chargen*

62. **IDS.8** El TOE tendrá la capacidad de inspeccionar el contenido del *payload* de paquetes/unidades de datos IPv4, IPv6, ICMPv4, ICMPv6, TCP, UDP y detectar las siguientes firmas basadas en patrones de tráfico:

    a) Ataques DoS a host: inundación ICMP, inundación TCP.

    b) Ataques DoS a red.

    c) Escaneo de puertos y protocolos (IP, TCP, UDP, ICMP).

4.9.3. REACCIÓN

63. **IPS.1** Ante la detección de un tráfico potencialmente dañino, el TOE deberá reaccionar permitiendo las siguientes operaciones, asociadas a una política basada en anomalías o en firmas:

    a) En cualquiera de los modos descritos en la sección 2.2:

        i. Permitir el flujo de tráfico.

    b) En el modo en línea permitirá además:

        i. Bloquear/descargar el tráfico.

        ii. Eliminar reglas (listas blancas/negras), en caso de políticas basadas en anomalías.

        iii. Otras acciones definidas por el fabricante, en caso de políticas basadas en anomalías.

4.10 NOTAS DE APLICACIÓN

64. En caso de que el producto no implemente la funcionalidad a la que aplica alguno de los requisitos anteriores (o algunas partes de ellos), y ésta sea proporcionada por el entorno operacional, el fabricante deberá indicarlo en la declaración de seguridad o justificarlo debidamente. En este caso, se evaluará si dada la misión y capacidades del producto, se puede considerar que el requisito ***no aplica***.

65. Lo anterior no es válido en caso de que tal funcionalidad solicitada en un requisito, sea proporcionada por un componente del producto que no forma parte de la configuración evaluada. En este caso ***sí aplica***, y el fabricante deberá demostrar el correcto cumplimiento del requisito por parte del producto.

5. ABREVIATURAS

CC	*Common Criteria*
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*
ICMP	*Internet Control Message Protocol*
IP	*Internet Protocol*
RFS	*Requisitos Fundamentales de Seguridad*
SFR	*Security Functional Requirements*
TCP	*Transmission Control Protocol*
UDP	*User Datagram Protocol*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL