sedian

Seguridad Digital
de Andalucía

Curso presencial virtualizado

Securización de redes desde el perímetro hacia el interior (I)

1ª sesión: 23 de noviembre de 2020

Junta de Andalucía

Índice de contenidos

- Principios básicos.
- Seguridad de interconexión.
- Arquitectura de protección perimetral.
- Requisitos del ENS sobre arquitecturas de protección de perímetro.
- Tipos de arquitecturas de protección de perímetro (APP).

1.- Principios básicos

- Dos o más sistemas de información pueden comunicarse entre sí para intercambiar información o servicios.

- Se produce una **conexión** cuando se proveen los medios físicos y lógicos de transmisión adecuados y susceptibles de ser empleados para el intercambio de información.

- Se produce una **interconexión** de sistemas cuando:
  - ✓ Existe una conexión.
  - ✓ Se habilitan flujos de comunicación entre los sistemas conectados y esa conexión se produce entre sistemas con diferente responsable de seguridad o de diferente categoría.

- Cuando una red se segrega en **subredes** pero todas las partes tienen la misma categoría y el responsable de seguridad es único, no se considera interconexión.

1.- Principios básicos

- Desde el punto de vista de seguridad se debe proteger la información almacenada estáticamente en cada sistema, además de información viajando dinámicamente por la interconexión.

- **Mínimo privilegio**. Los usuarios y procesos autorizados a atravesar el perímetro solo disfrutarán de los derechos mínimos imprescindibles para ello.

- **Nodo auto protegido**. Cuando un nodo se interconecta a otro, debe partir de la base de que el otro nodo no es fiable y por tanto hay que defenderse. Cada nodo debe protegerse a sí mismo como si los demás estuvieran comprometidos. Este principio impide la propagación de incidentes, accidentales o deliberados, entre nodos.

- **Despliegue mínimo**. En el perímetro solamente se desplegarán, configurarán y usarán los equipos, cuentas de usuarios y administradores, aplicaciones, protocolos, servicios y flujos de información, estrictamente imprescindibles para el cumplimiento de la misión de la interconexión.

2.- Seguridad de interconexión

Antes de interconectar dos sistemas, se requiere un **Acuerdo de Seguridad de la Interconexión** que es un documento formal, aprobado por los responsables de seguridad de los sistemas cuando estos sean diferentes, y que incluirá, al menos, los siguientes puntos:

- Identificación de roles, funciones y personas designadas para los mismos.
- Requisitos de negocio – la funcionalidad que se quiere proveer.
- Comunidad(es) de usuario(s), incluyendo sus niveles de habilitación, en su caso.
- Información que se va a intercambiar, incluyendo su clasificación y reglas de marcado, en su caso.
- Servicios (incluyendo el detalle de los protocolos que se van a emplear, directa o indirectamente).

2.- Seguridad de interconexión

- Topología del sistema de protección (nivel lógico y físico).
- Controles que se han desplegado para proteger los intercambios de información.
- Análisis de riesgos que concrete riesgos potenciales y residuales.
- Procedimientos operativos de seguridad; al menos los relativos a autorización, configuración, gestión de incidencias y gestión de cambios.
- Registros de actividad y sus procedimientos asociados.

Cuando la conexión se realice con una red pública (por ejemplo, Internet), el Acuerdo de Seguridad de la Interconexión vendrá aprobado únicamente por el Responsable de la Seguridad del sistema de información adscrito al ENS.

2.- Seguridad de interconexión

- Las Series CCN-STIC son normas, instrucciones, guías y recomendaciones desarrolladas por el Centro Criptológico Nacional con el fin de mejorar el grado de ciberseguridad de las organizaciones. Periódicamente son actualizadas y completadas con otras nuevas, en función de las amenazas y vulnerabilidades detectadas por el CCN-CERT.

- El grueso de las Series están especialmente dirigidas al personal de las Administraciones Públicas y empresas y organizaciones de interés estratégico (parte privada del portal) y otras de difusión pública para todos los usuarios. De igual modo, algunas de las series están clasificadas como Difusión Limitada (DL) o Confidencial (C) y por tanto, es necesaria su solicitud al CCN-CERT, con la condición imprescindible de estar registrado en la parte privada del portal.

https://www.ccn-cert.cni.es/guias/indice-de-guias.html

2.- Seguridad de interconexión

2.- Seguridad de interconexión

- Desde **AMPARO** se permite crear los pasos necesarios de la **implantación al ENS** de los sistemas de organismos a través de un asistente que guía al usuario por todas las partes de implantación:

  ✓ Aportar un Plan de adecuación del sistema (propio o creado por INES).
  ✓ Recorrer todas las medidas de seguridad recibiendo ayudas, plantillas, guías y herramientas para ayudar en la implantación del ENS.
  ✓ Aportar evidencias de la implantación de las medidas.
  ✓ Evaluar el sistema y resaltar posibles carencias y no conformidades.
  ✓ Obtener la declaración de conformidad.
  ✓ Solicitar una auditoría para conseguir el Certificado de Conformidad.
  ✓ Gestionar la auditoría y la conformidad del sistema.

2.- Seguridad de interconexión

3.- Arquitectura de protección perimetral (APP)

- Se deberá constituir una arquitectura de protección perimetral, utilizando para ello dispositivos que permitan proteger los flujos de información.

- Dentro de las posibilidades tecnológicas que podemos adquirir, para cumplir ese objetivo, nos centraremos en los siguientes dispositivos:
  - Enrutadores (router.s).
  - Cortafuegos (firewalls).
  - Intermediarios (proxies).
  - Pasarelas de intercambio seguro.
  - Diodos de datos.

- A continuación, se describe la funcionalidad de cada dispositivo, explicando brevemente el modelo de comunicación de interconexión de sistemas abiertos (modelo OSI).

3.- Arquitectura de protección perimetral

3.1.- Capas OSI implicadas

- El modelo de interconexión de sistemas abiertos (OSI) es un modelo conceptual desarrollado en los años 70 y publicado como norma ISO/IEC 7498. Buscaba una referencia independiente de los fabricantes de productos para que estos pudieran interoperar.

- Es un modelo prácticamente paralelo al desarrollo del modelo TCP5/IP6, sobre el que se sustenta Internet.

- Ambos modelos (OSI y TCP/IP) se basan en el concepto de agrupación de protocolos en capas. Así los protocolos de las capas inferiores realizan tareas que proporcionan servicios a las capas superiores.

3.- Arquitectura de protección perimetral

3.2.- Enrutadores (Routers)

* Son elementos que trabajan a nivel de red. En este nivel se inician, mantienen y terminan las conexiones que transmiten paquetes IP, permitiendo que estos paquetes pasen de una red a otra. Se trata por tanto de un elemento imprescindible para conectar dos redes, entendiendo por red el conjunto de equipos que se pueden conectar directamente entre sí sin necesidad de un enrutador. Permiten interconectar redes LAN y WAN.

* Los enrutadores o encaminadores o routers filtran los paquetes IP en función de las direcciones IP, servicios y puertos a los que se quiere acceder. Además, proporcionan control de tráfico y funciones de filtrado a nivel de red. Permiten también reencaminar (enrutar) dinámicamente para dirigir los paquetes IP.

* Los routers tienen la capacidad de controlar los flujos de información tanto entrante como saliente. Se trata por tanto de dispositivos que requieren de una configuración adecuada para proteger nuestro sistema.

3.- Arquitectura de protección perimetral

3.2.- Enrutadores (Routers)

Aruba 8325 Switch Series

Versión	Aruba OS-CX version 10.03
Fabricante	Aruba
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/11/2019
Revisión de Validez	30/04/2022

ens ALTA MEDIA BÁSICA ALTA

Descripción

Equipos orientados a ser equipos de núcleo de red (CORE) de Campus como de Centros de Datos. Es un equipo con categoría de operador. Dispone de una arquitectura interna de Sistema Operativo que proporciona una forma de trabajar con el completamente programable. Su motor de analíticas (NAE) permite la inserción de scripts de para la ejecución de tareas avanzadas de monitorización y respuestas a eventos.
Ofrecen interfaces a alta velocidad así como una tecnología de chasis virtual.

Observaciones

CCN-STIC-647C Seguridad en conmutadores HPE Aruba

3.- Arquitectura de protección perimetral

3.2.- Enrutadores (Routers)

ASR1K-1004	
Versión	IOS XE 16.3
Fabricante	Cisco Systems
Familia	Enrutadores
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/06/2018
Revisión de Validez	30/11/2020

Descripción

La serie ASR1K de Cisco ofrece aceleración de hardware integrada para múltiples servicios de Cisco IOS-XE Software. Además, los enrutadores de Cisco de la serie ASR1K presentan enrutado redundante y procesadores de servicios integrados, así como redundancia basada en software. Cisco ASR1K proporciona capacidades de conexión IPsec para comunicaciones seguras.

Observaciones

CCN-STIC-1414 Procedimiento de empleo seguro Router Cisco Systems ISR/ASR

3.- Arquitectura de protección perimetral

3.3.- Cortafuegos (Firewalls)

- Un cortafuegos es un dispositivo de seguridad fundamental para proteger el perímetro. Puede actuar en varias capas del modelo OSI (principalmente de red y transporte, aunque también pueden ser de aplicación). Puede ser una aplicación, un dispositivo o una combinación de ambos. Su función principal consiste en aislar redes internas y bloquear redes externas según las políticas de cada organización.

- Hay cortafuegos de red, que controlan el tráfico en tránsito de la red.

- Hay cortafuegos de equipo que controlan la conexión de un equipo a una red. Por ejemplo, en equipos personales, son frecuentes los cortafuegos personales que determinan qué paquetes pueden entrar y qué paquetes pueden salir.

- Los cortafuegos analizan paquetes IP, y teniendo en cuenta dirección origen, dirección destino, protocolo y puerto de destino, deciden permitir o bloquear su paso.

3.- Arquitectura de protección perimetral

3.3.- Cortafuegos (Firewalls)

FG-30E, FG-50E, FG-51E, FG-52E, FG-60E, FG-60E-DSL, FG-60E-PoE, FG-61E, FG-80E, FG-80E- PoE, FG-81E, FG-81E-PoE	
Versión	FortiOS 5.6
Fabricante	Fortinet
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/09/2019
Revisión de Validez	31/08/2020

Descripción

Firewalls de Nueva Generación con capacidades de inspección en capa 7, IPS y concentrador VPN IPSEC. Modelos para entornos pequeños y sedes remotas de pocos usuarios. Las funcionalidades de seguridad son similares a las del resto de modelos más grandes (reconocimiento de aplicaciones y usuarios de la red, protección frente a malware conocido, amenazas avanzadas y ataques zero-day, protección frente a botnets, filtro de navegación web, capacidades SDWAN, etc., como se describe en https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiOS.pdf).
Más información en: https://www.fortinet.com/products/next-generation-firewall.htm

Observaciones

CCN-STIC-1406 Procedimiento de empleo seguro cortafuegos Fortigate.

3.- Arquitectura de protección perimetral

3.3.- Cortafuegos (Firewalls)

PA-3000 Series (PA-3020, PA-3050, PA-3060) y PA-3200 Series (PA-3220, PA-3250, PA-3260)	
Versión	PAN-OS v8.0.12 y v8.1.3
Fabricante	Palo Alto Networks
Familia	Cortafuegos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/03/2019
Revisión de Validez	31/08/2021

Descripción

Firewalls de Nueva Generación orientados a empresas u organismos de tamaño medio, con capacidad de identificar la aplicación para la toma de decisiones de seguridad, independientemente del puerto, la técnica evasiva, o el tipo de cifrado.
Son capaces de aplicar políticas en base al usuario, para lo que se integran con diferentes sistemas de identificación y directorios LDAP.
Bloquean los ataques conocidos, además de realizar filtrado URL dinámico e identificar y generar protección contra el malware desconocido.

Observaciones

CCN-STIC-1413 Procedimiento de empleo seguro Cortafuegos NGFW de Palo Alto Networks

3.- Arquitectura de protección perimetral

3.4.- Intermediarios (Proxies)

- Se trata de un dispositivo que se sitúa en la red actuando de intermediario para prestar un servicio determinado. Su función es recibir todas las peticiones de los usuarios de una organización, a un determinado protocolo, y distribuir las entradas y salidas de información de acuerdo con unos filtros.

- Los intermediarios o proxies trabajan a nivel de aplicación. Existen proxies para diferentes protocolos, por ejemplo, mensajería electrónica (POP, SMTP), navegación web (HTTP), transferencia de ficheros (FTP) etc.

- Los proxies no trabajan con paquetes IP o, para ser más precisos, reciben paquetes TCP/IP por la entrada, examinan y extraen su contenido y crean nuevos paquetes TCP/IP en la salida. Esta operación desactiva los paquetes como mecanismos para trasladar carga maliciosa.

- La ventaja de los proxies es que examinan el contenido del paquete, comprenden el protocolo y pueden detectar un uso anómalo del mismo.

3.- Arquitectura de protección perimetral

3.4.- Intermediarios (Proxies)

Fortinet FortiProxy	
Versión	1.0
Fabricante	Fortinet
Familia	Proxies
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/07/2020
Revisión de Validez	31/12/2020

Descripción

A medida que las ciberamenazas se van haciendo más sofisticadas, las compañías necesitan cada vez más una aproximación integral para proteger a los usuarios del tráfico web malicioso, los websites peligrosos y aquel contenido que pueda suponer una amenazapara ellos. El Secure Web Gateway (SWG) de Fortinet, FortiProxy, aborda esta situación con un único producto que incluye URL filtering, protección contra amenazas avanzadas y malware, filtrado DNS, DLP, IPS... La protección de los usuarios contra amenazasprocedentes de internet facilita el cumplimiento de las políticas corporativas.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

3.- Arquitectura de protección perimetral

3.4.- Intermediarios (Proxies)

Blue Coat ProxySG S400 and S500

Versión	SW: SGOS v6.5
Fabricante	Symantec Corporation
Familia	Proxies
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2021

Descripción

Los dispositivos Blue Coat ProxySG S400 y ProxySG S500 con la versión software SGOS v6.5 realizan la función de proxy multiprotocolo (http, https, ftp, DNS, MAPI, diversos protocols de streaming de contenido multimedia, webex, CIFS, RPC) y pueden funcionar tanto como proxies directos (para la protección y control de usuarios) como proxies inversos con firewall de aplicaciones web, para la protección de servidores de aplicaciones web. El propósito de estos dispositivos es proporcionar una capa de seguridadentre la red Interna y una o más redes externas (típicamente una red corporativa e Internet), aislando el tráfico de los usuarios a nivel de aplicación (torre OSI) y proporcionando demás diferentes mecanismos de optimización WAN para el tráfico que procesan.

Observaciones

Procedimiento de empleo seguro pendiente de publicación.

3.- Arquitectura de protección perimetral

3.5.- Pasarela de intercambio seguro

- Las pasarelas de intercambio seguro de información son dispositivos de protección de perímetro más complejos que un cortafuegos o un proxy. Están orientadas a la protección de interconexiones entre redes que manejan información con diferentes categorías o políticas de seguridad, con el fin de evitar la entrada o salida de información no autorizada.

- Para ello, aportan las siguientes funcionalidades de seguridad:
  - Separación de redes. Ruptura de la continuidad de los protocolos de comunicaciones entre dos redes interconectadas en todas las capas del modelo OSI. Así, las pasarelas suelen estar formadas por dos unidades, una que se conecta a la red interna (la que se protege) y otra a la externa, unidas por un dispositivo pasivo de lectura y escritura.

  - Ambas unidades se comunican mediante un protocolo desarrollado ad-hoc, que impide que utilicen simultáneamente los mismos recursos. De esta forma se asegura que nunca se establece una conexión TCP/IP entre las entidades origen y destino, independientemente de la configuración software del dispositivo, ni que a la red externa lleguen paquetes con información de la red interna.

3.- Arquitectura de protección perimetral

3.5.- Pasarela de intercambio seguro

- Filtrado de contenidos. Las pasarelas analizan el contenido del paquete y permiten el paso de información siempre que cumpla las reglas de filtrado definidas, tanto para la entrada como para la salida. También posibilitan la utilización de mecanismos de firma digital para el control de flujo de información, de tal manera que solo aquello que se encuentre firmado pueda salir de la red interna. Este control basado en firma digital está enfocado a sistemas que manejan información a la que se le exige un nivel muy alto de confidencialidad.

- Las pasarelas son especialmente útiles para implementar mecanismos de defensa en profundidad y neutralizar o minimizar el efecto de las Amenazas Persistentes Avanzadas al no permitir la fuga de información sensible desde la red interna.

- Las pasarelas de intercambio seguro no se exigen en el Esquema Nacional de Seguridad, no obstante, pudieran ser una opción recomendable para algunos organismos dependiendo de los entornos y activos esenciales a proteger.

- Existen pasarelas de intercambio seguro para correo electrónico, servicios web o para transferencia de ficheros. Ver guía CCN-STIC 105 Catálogo de productos de la seguridad de las tecnologías de la Información y la Comunicación.

3.- Arquitectura de protección perimetral

3.5.- Pasarela de intercambio seguro

PSTmail	
Versión	v3.0.5
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2021

Descripción

PSTmail es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de correo electrónico entre dominios de seguridad. Posibilita el empleo de direcciones de correo de redes externas, desde una red interna, más segura. Soporta las versiones seguras de los protocolos de correo. Los mensajes de salida requieren autorización mediante firma digital (S/MIME).

Observaciones

Procedimiento de empleo seguro: CCN-STIC-1401 Configuración segura de pasarelas de AUTEK

3.- Arquitectura de protección perimetral

3.5.- Pasarela de intercambio seguro

PSTfile	
Versión	v4.4.2
Fabricante	Autek Ingeniería
Familia	Pasarelas seguras de intercambio de datos
Tipo	Producto
Categoría ENS	ALTA
Fecha Inclusión	01/12/2017
Revisión de Validez	31/05/2021

Descripción

PSTfile es un dispositivo de protección de perímetro de la familia PSTgateways. Permite el intercambio controlado de ficheros entre dominios de seguridad. Se establece una correspondencia entre carpetas, en servidores de ficheros de ambas redes y PSTfile,automáticamente, mueve o copia los ficheros del origen al destino. Soporta los protocolos FTP, FTPS, SFTP y SMB. La transferencia de ficheros desde el dominio de alta seguridad al de baja requiere autorización mediante firma digital.

Observaciones

Procedimiento de empleo seguro: CCN-STIC-1401 Configuración segura de pasarelas de AUTEK

3.- Arquitectura de protección perimetral

3.6.- Diodos de datos

- Los diodos de datos son los dispositivos de protección de perímetro que aportan una mayor seguridad frente a la fuga de información sensible, dado que garantizan el flujo unidireccional de la información mediante hardware, al no existir un canal de retorno físico.

- Están orientados a la protección de interconexiones entre redes que manejan información con diferentes categorías o políticas de seguridad, con el fin de evitar la salida de cualquier tipo de información del sistema que protegen.

- Dado que no existe este canal de retorno, en el caso en que ambos sistemas utilicen protocolos de comunicaciones orientados a conexión (p.ej.: TCP) o arquitecturas cliente/servidor que por definición exijan una bidireccionalidad, estos dispositivos requerirán de una lógica adicional a ambos lados del dispositivo hardware unidireccional en el que la lógica externa actúe como receptor frente a la red exterior y la lógica interna como emisor frente a la red interior y así permitir que la comunicación se realice con éxito.

3.- Arquitectura de protección perimetral

3.6.- Diodos de datos

- Esta imposibilidad de comunicación bidireccional extremo a extremo hace que el emisor nunca pueda disponer de un acuse de recibo real del resultado de la transmisión.

- Esta lógica podrá estar integrada o no dentro del propio dispositivo hardware unidireccional.

- Los diodos tampoco se exigen en el Esquema Nacional de Seguridad y sirven para implementar políticas muy restrictivas. Por ejemplo, en un sistema se permite que entre información; pero no que salga, impidiendo las fugas de información.

3.- Arquitectura de protección perimetral

3.6.- Diodos de datos

PSTdiode

Versión	v1.0.0
Fabricante	Autek Ingeniería
Familia	Diodos de datos
Tipo	Producto
Clasificación	TODOS LOS NIVELES
Fecha Inclusión	01/09/2019
Revisión de Validez	28/02/2022

Descripción

El diodo de datos hardware PSTdiode es un dispositivo de protección de perímetro que permite la transferencia de información en un único sentido entre dos dominios de seguridad con garantía física de transmisión unidireccional. Su aplicación principal esla introducción de información en una red aislada en entornos clasificados. También se puede aplicar para extraer información de una red de control industrial en entornos de infraestructuras críticas.
En ambos casos se garantiza que no existe tráfico en el sentido inverso.
Existen modelos de transferencia de ficheros y tráfico UDP.

Observaciones

Procedimeinto de empleo seguro: CCN-STIC 1408 Procedimiento de empleo seguro Diodo Autek Ingeniería

4.- Requisitos ENS sobre arquitectura protección perímetro

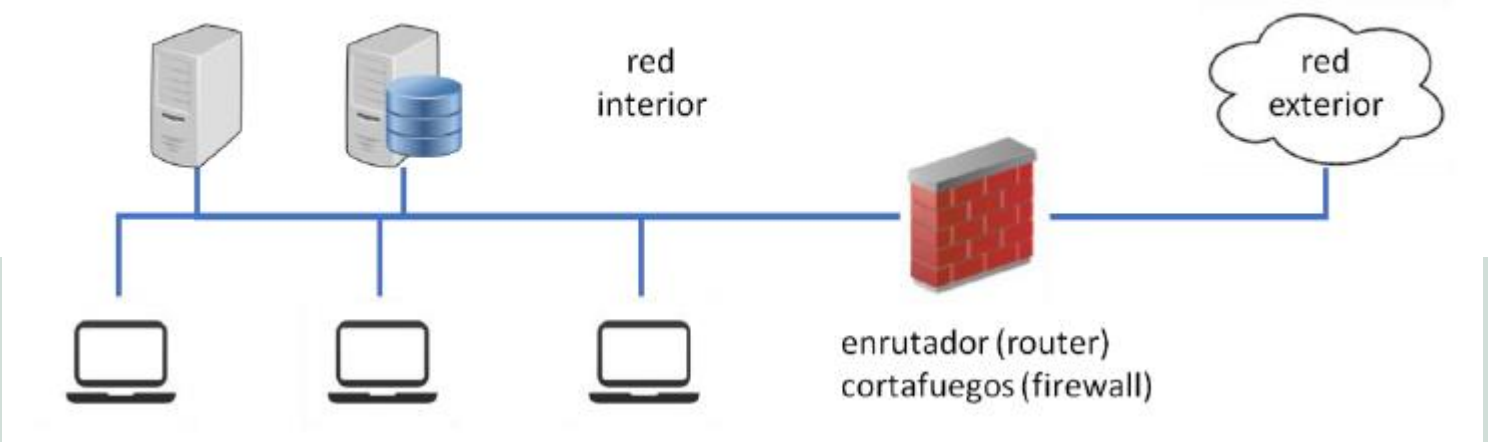
- Para sistemas de las tecnologías de la información sujetos al Esquema Nacional de Seguridad, se autorizan las siguientes arquitecturas de protección del perímetro.

Categoría del sistema	Arquitectura de Protección de Perímetro
Básica	APP-3 o superior
Media	APP-4 o superior
Alta	APP-5 o superior

5.- Arquitectura de protección perimetral

5.1.- Arquitectura de protección de perímetro tipo APP-1

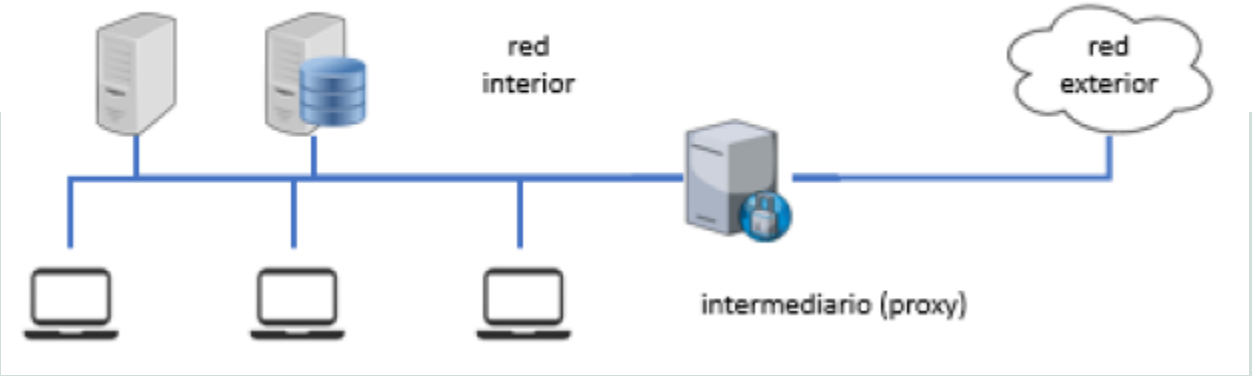
- Se despliega, un cortafuegos entre nuestra red y el exterior. Como se ha comentado el cortafuegos aúna las funciones de encaminamiento y filtro de paquetes o de circuito.
- Esta arquitectura no controla contenidos, solamente controla el tráfico permitido.
- El cortafuegos está expuesto a ataques desde el exterior y desde el interior.
- Un fallo (vulnerabilidad) en el cortafuegos, tiene como consecuencia directa la posibilidad de acceso al interior de nuestro sistema, o la fuga de datos.



5.- Arquitectura de protección perimetral

5.2.- Arquitectura de protección de perímetro tipo APP-2

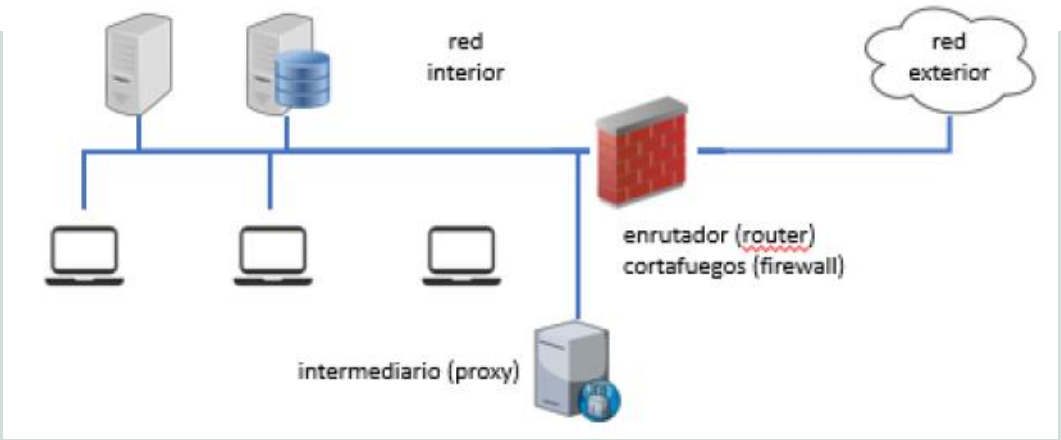
- Simplemente se despliega un intermediario (proxy) entre nuestra red y el exterior. El mismo intermediario aúna las funciones de encaminador (router).
- Esta arquitectura permite monitorizar y controlar los intercambios de datos y los contenidos, pudiendo establecer reglas precisas de autorización y registro de actividad.
- El intermediario o proxy está expuesto directamente a ataques desde el exterior y desde el interior.
- Un fallo (vulnerabilidad) en el intermediario tiene como consecuencia directa el acceso al interior o la fuga de datos.



5.- Arquitectura de protección perimetral

5.3.- Arquitectura de protección de perímetro tipo APP-3

- Combinamos un cortafuegos con un intermediario.
- Esta arquitectura permite monitorizar y controlar los intercambios de datos y los contenidos, pudiendo establecer reglas precisas de autorización y registro de actividad.
- El elemento que hace de cortafuegos está expuesto directamente a ataques desde el exterior; pero el elemento que hace de intermediario ve reducida su superficie de ataque a lo que permita el cortafuegos, además de los ataques procedentes del interior.
- Un fallo (vulnerabilidad) en el cortafuegos tiene como consecuencia directa el acceso al interior, o la fuga de datos.
- Si el intermediario se viera comprometido, el atacante tendría acceso a la red interior.



5.- Arquitectura de protección perimetral

5.4.- Arquitectura de protección de perímetro tipo APP-4

- Similar a la arquitectura APP-3; pero el cortafuegos tendrá configurados 3 puertos, uno para la red interior, otro para la red exterior y un tercero para el proxy. De este modo conseguimos que el proxy no esté ni en la red interior ni en la exterior, sino en un tramo de red intermedio, que se denomina zona desmilitarizada (DMZ). La diferencia funcional radica en que todo el tráfico de entrada y de salida a nuestra red es filtrado a través del proxy y todos los accesos al proxy deben ser autorizados en los cortafuegos.

- La zona DMZ es un tramo de acceso controlado, filtrado por el cortafuegos que protege sus conexiones interna y externa. Es habitual desplegar en esta zona servicios como pasarelas de correo electrónico o de páginas web, de forma que es sencillo filtrar el contenido de los intercambios. También es frecuente desplegar en esta zona servidores DNS que limitan la visibilidad exterior a lo estrictamente necesario.

5.- Arquitectura de protección perimetral

5.4.- Arquitectura de protección de perímetro tipo APP-4

- Esta arquitectura controla entre qué elementos pueden circular paquetes IP, limitando el tráfico permitido:

  ✓ entre la red interior y el intermediario o proxy.

  ✓ entre el intermediario (proxy) y la red exterior.

  ✓ no debe autorizarse el paso de paquetes directamente de la red exterior a la interior sin atravesar el intermediario o proxy.

5.- Arquitectura de protección perimetral

5.4.- Arquitectura de protección de perímetro tipo APP-4

- Esta arquitectura permite reducir la exposición de nuestro sistema ante ataques externos o errores internos, ya que el tráfico es filtrado por el cortafuegos. Se controla qué flujos de información se permiten entre el interior y el intermediario. Esto reduce la exposición a ataques o errores internos que puedan llevar flujos no autorizados al intermediario. Así mismo, si el intermediario se viera comprometido, se limita su accesibilidad a la red interior.

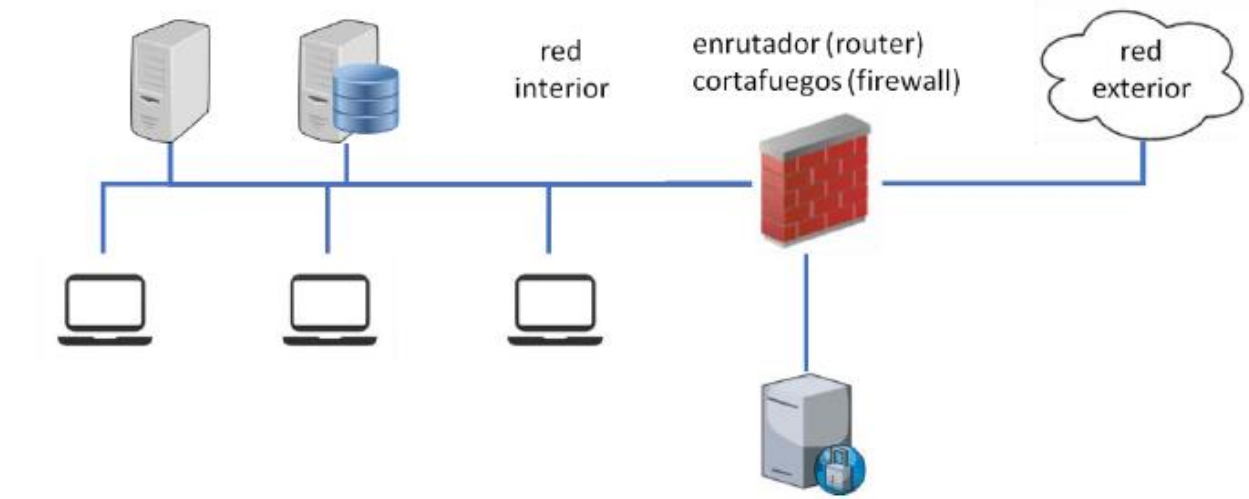
- Un fallo (vulnerabilidad) en el cortafuegos, tiene como consecuencia directa la posibilidad de acceso al interior, o la fuga de datos.

5.- Arquitectura de protección perimetral

5.4.- Arquitectura de protección de perímetro tipo APP-4

- Esta arquitectura permite reducir la exposición de nuestro sistema ante ataques externos o errores internos, ya que el tráfico es filtrado por el cortafuegos. Se controla qué flujos de información se permiten entre el interior y el intermediario. Esto reduce la exposición a ataques o errores internos que puedan llevar flujos no autorizados al intermediario. Así mismo, si el intermediario se viera comprometido, se limita su accesibilidad a la red interior.

- Un fallo (vulnerabilidad) en el cortafuegos, tiene como consecuencia directa la posibilidad de acceso al interior, o la fuga de datos.



5.- Arquitectura de protección perimetral

5.5.- Arquitectura de protección de perímetro tipo APP-5

- Se despliegan, un intermediario (proxy) y dos cortafuegos, dejando un tramo de red intermedio. Esta red intermedia se denomina coloquialmente zona desmilitarizada (DMZ) y no se autoriza que circulen paquetes, directamente entre los cortafuegos.

- Un cortafuegos permite la entrada de datos al proxy, mientras que el otro cortafuegos permite la salida de datos del proxy. En ambas direcciones, según requieran los flujos autorizados.

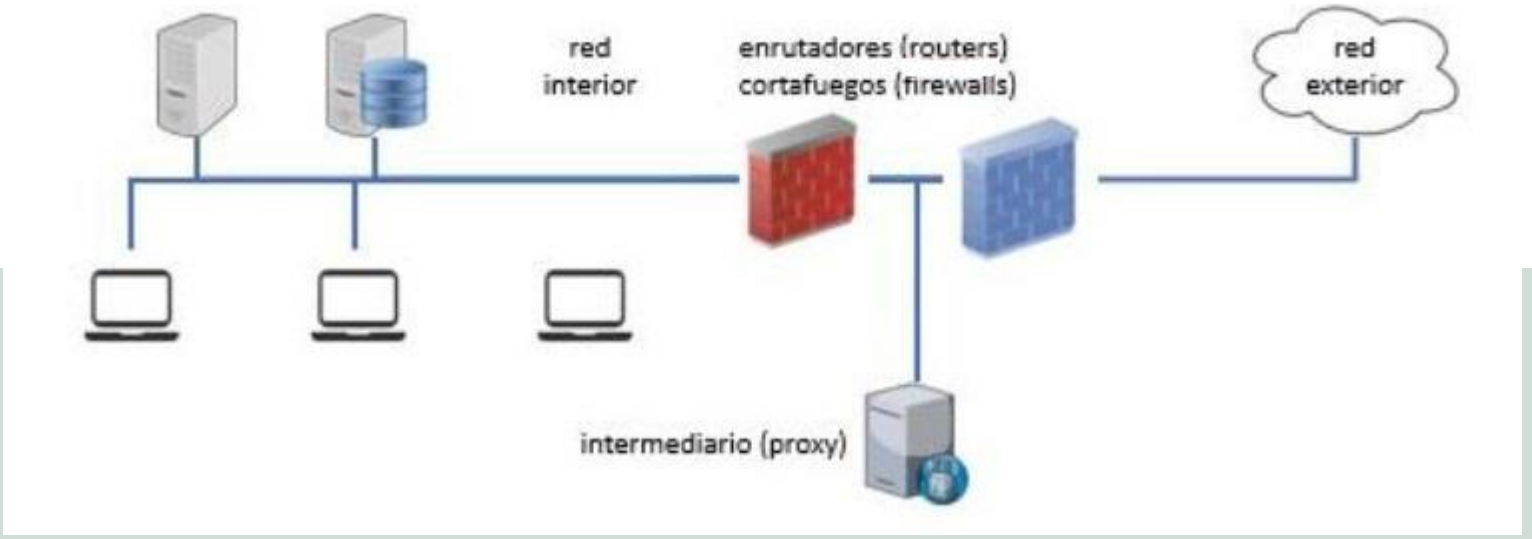
- Funcionalmente, esta arquitectura funciona de forma similar a la APP-4; pero dificultamos los ataques al cortafuegos: ahora deben comprometerse 2 cortafuegos para atravesar el perímetro sin ser interceptados por el proxy. Para potenciar esta característica se evita que ambos cortafuegos puedan sucumbir como consecuencia de un único vector de ataque, forzando a que sean diferentes: diferente fabricante, diferente software, diferente configuración, diferentes administradores de seguridad, etc.

5.- Arquitectura de protección perimetral

5.5.- Arquitectura de protección de perímetro tipo APP-5

- Esta arquitectura controla entre qué elementos pueden circular paquetes IP, limitando el tráfico permitido:
  - ✓ entre la red interior y el intermediario (proxy).
  - ✓ entre el intermediario (proxy) y la red exterior.
  - ✓ no debe autorizarse el paso de paquetes directamente de la red exterior a la interior sin atravesar el intermediario o proxy.

- Comparado con APP-4 se ha eliminado el riesgo de que una vulnerabilidad en un solo cortafuegos se traduzca en una posibilidad de acceso directo a la red interna.

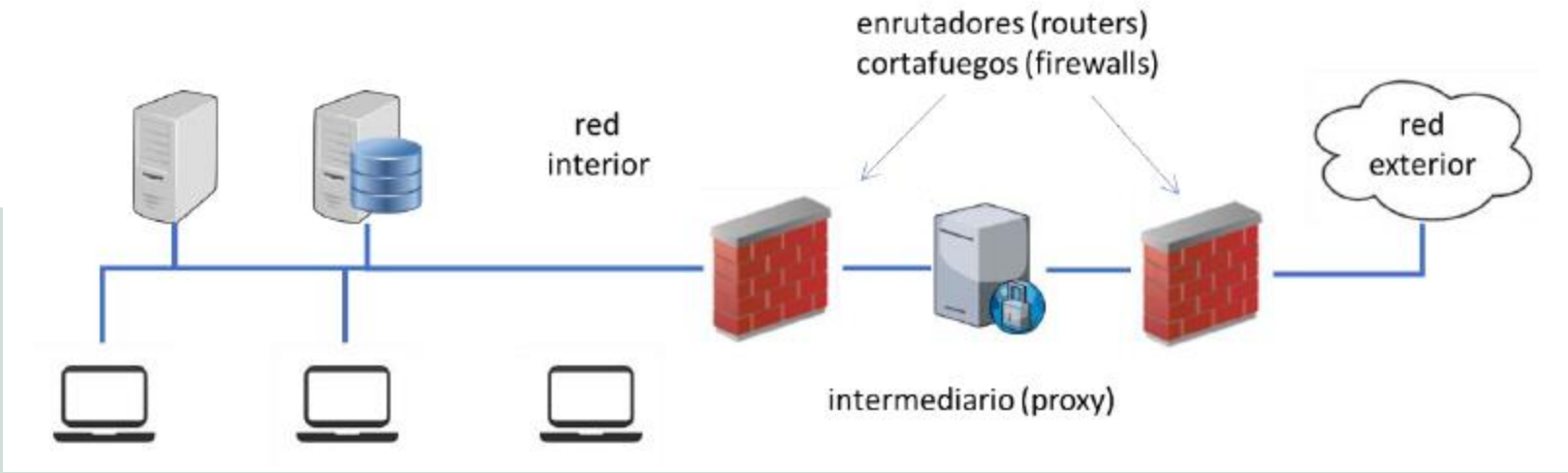


5.- Arquitectura de protección perimetral

5.6.- Arquitectura de protección de perímetro tipo APP-6

- Se despliegan, un intermediario (proxy) y dos cortafuegos, pero, a diferencia de la arquitectura APP-5, no existe un tramo de red directo entre los cortafuegos.

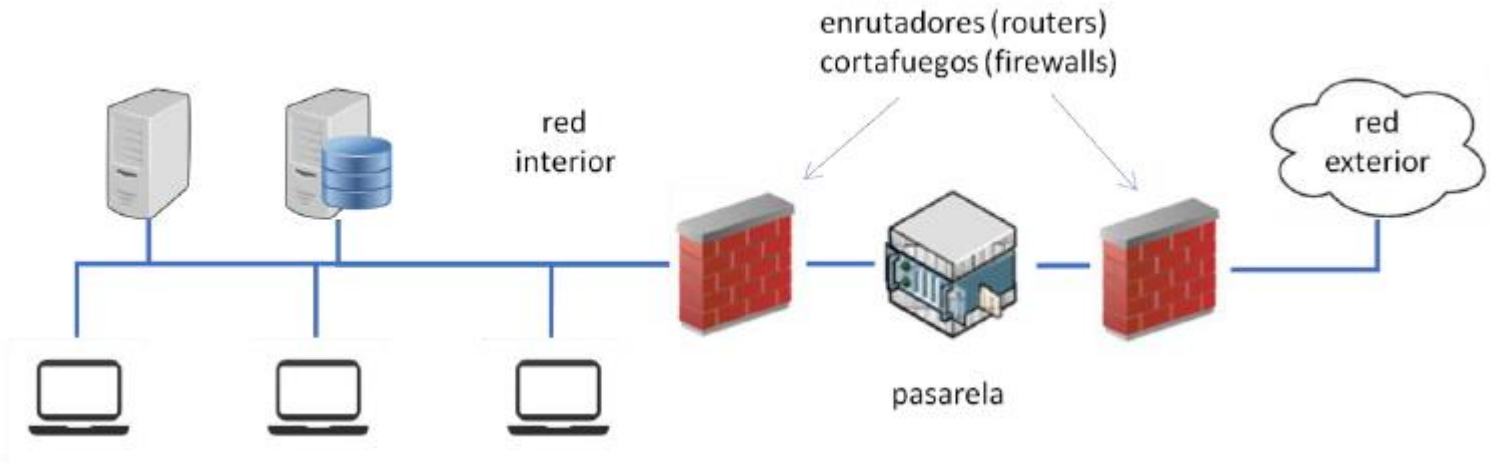
- Comparado con APP5, eliminamos el requisito de que los cortafuegos deban ser diferentes, al no existir conexión directa entre ellos. El razonamiento tras el requisito de que los cortafuegos sean diferentes es reducir la posibilidad de que una vulnerabilidad en uno de ellos se reproduzca automáticamente en el otro, bien sea una vulnerabilidad hardware, software o de la configuración. Si la vulnerabilidad afecta al encaminamiento de paquetes, en APP-5 sería posible pasar de la red exterior a la red interior directamente. Al no existir la red física en APP-6, ese peligro desaparece.



5.- Arquitectura de protección perimetral

5.7.- Arquitectura de protección de perímetro tipo APP-7

- Como se ha indicado anteriormente puede haber casos en los que el organismo tenga unos requisitos de confidencialidad superiores a los que marca el Esquema Nacional de Seguridad, para los que sea recomendable sustituir el intermediario o proxy por una pasarela de intercambio seguro o incluso un diodo.



sedian Seguridad Digital de Andalucía