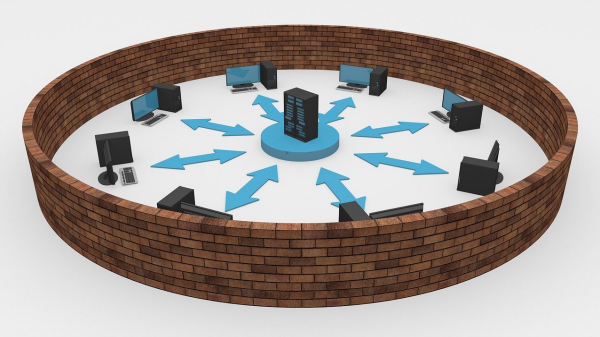
Configuración de dispositivos y sistemas informáticos I.

Caso práctico

La red de las organizaciones tienen muchos "atajos" que los administradores y los usuarios conocen. Esto les permite poder acceder a los servicios que desean, sin que para ello necesiten tener permisos, como por ejemplo el servicio de impresión. Las compañías suelen disponer de servicios como:



pixabay (Dominio público)

- Servicio Web con una base de datos asociada. Este es el servicio que presta a sus clientes, con una web que permite realizar la gestión del stock de almacenes.

- Gestor de contenidos de la Web

- Un servidor de directorio Activo

- Un servicio de resolución de nombres (DNS)

- Un servicio de impresión.

- Un servicio de ficheros.

- Portal para los empleados (Intranet). Este servicio se nutre de fuentes de noticias de información externas.

El objetivo siempre deber ser que la arquitectura sea más segura, permitiendo controlar los flujos de información entre los diferentes servicios, y analizando los flujos que son necesarios y cuales no.

En esta unidad se trabajará los conceptos que tienen relación con la definición de la arquitectura de red desde un punto de vista de la seguridad. Estudiando conceptos básicos de redes que son necesarios conocer para implementar medidas de seguridad de la red como son VLAN, IP, segmentación, protocolos, puertos,.....

Conoceremos los tipos de firewall que existen en el mercado y cómo ha ido evolucionado en funcionalidades y funcionamiento. Analizando específicamente los que protegen los servicios web.

Apoyado en los capítulos anteriores analizaremos en detalle los pautas de seguridad a implementar en la zona más externa de nuestra red que alberga los servicios que se ofrecen

hacia el exterior.

Finalmente analizaremos la seguridad de lo servicios que proporciona el paradigma de los servicios prestado por terceros en la nube y que forman parte de nuestro sistema.

1.- Seguridad perimetral. Firewalls de próxima generación.

Caso práctico

No han llamado de la empresa cárnicas Celada SA para analizar la seguridad que les proporciona un firewall de primera generación que ha sido instalado en el perímetro hace años. El dispositivo lo operan en base a las recomendaciones del proveedor del equipo. El firewall está gestionado por una empresa externa que actualiza con reglas el equipo en base IPs maliciosas que se intentan conectar con las empresas o que el proveedor considera peligrosas.

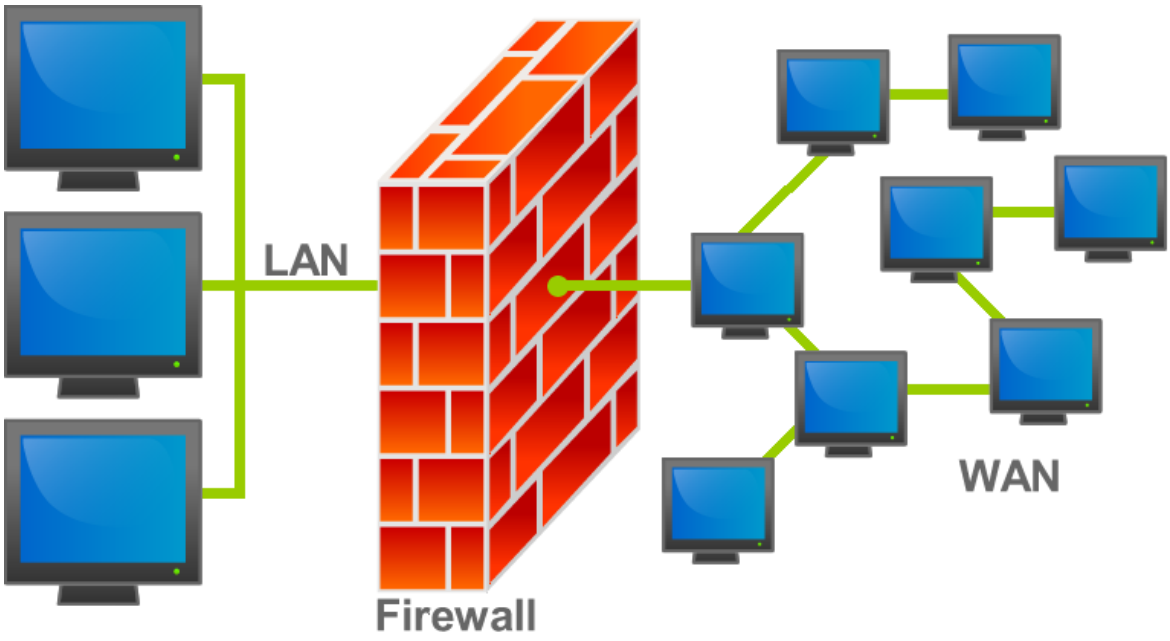
Describe al menos 3 mejoras en la seguridad del firewall.

Evoluciona

- Las reglas de firewall deben establecerse no sólo en base a IP origen, sino también a puerto, flags y protocolo.
- El acceso a la administración del dispositivo debe estar controlado por IP
- Aunque la operación del firewall esté delegado a una empresa externa, establece puntos de control sobre lo que se está realizando sobre el dispositivo: actualizaciones, copias de seguridad, monitorización,... La gobernabilidad de la seguridad es del propietario del sistema.
- Estudia si todas las interconexiones de la empresa salen por ese firewall o se hacen por dispositivos no controlados.
- Incluye reglas de las conexiones de salida y no sólo de las conexiones entrantes

-....

Un firewall un dispositivo de seguridad de protección, que puede ser un software o hardware. Su función es controlar el tráfico de la red en base a un conjunto de reglas.

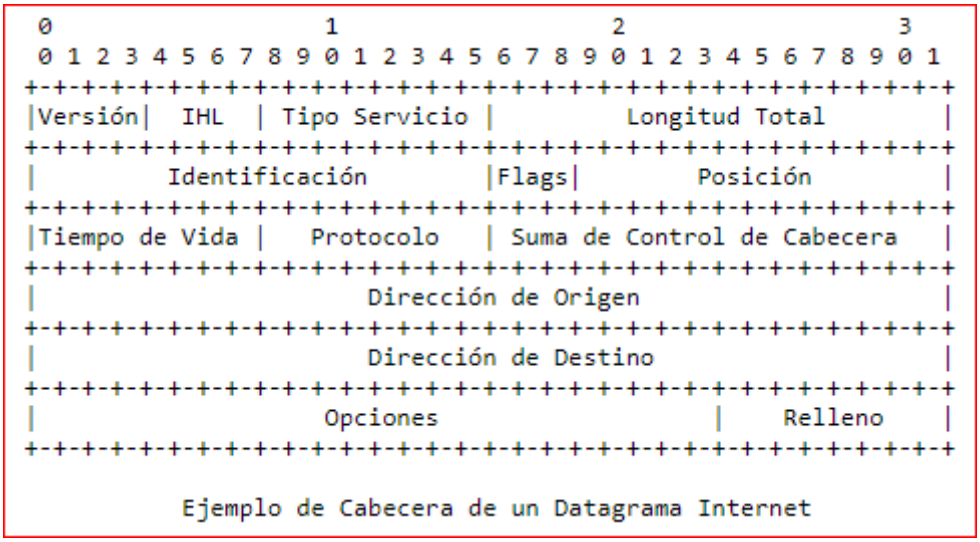


Bruno Pedrozo (CC BY-SA)

Antes de entrar en más detalles sobre los firewalls, es útil recordar el contenido de un paquete IP y un segmento TCP. De estos paquetes sólo nos interesan algunos campos:

IP

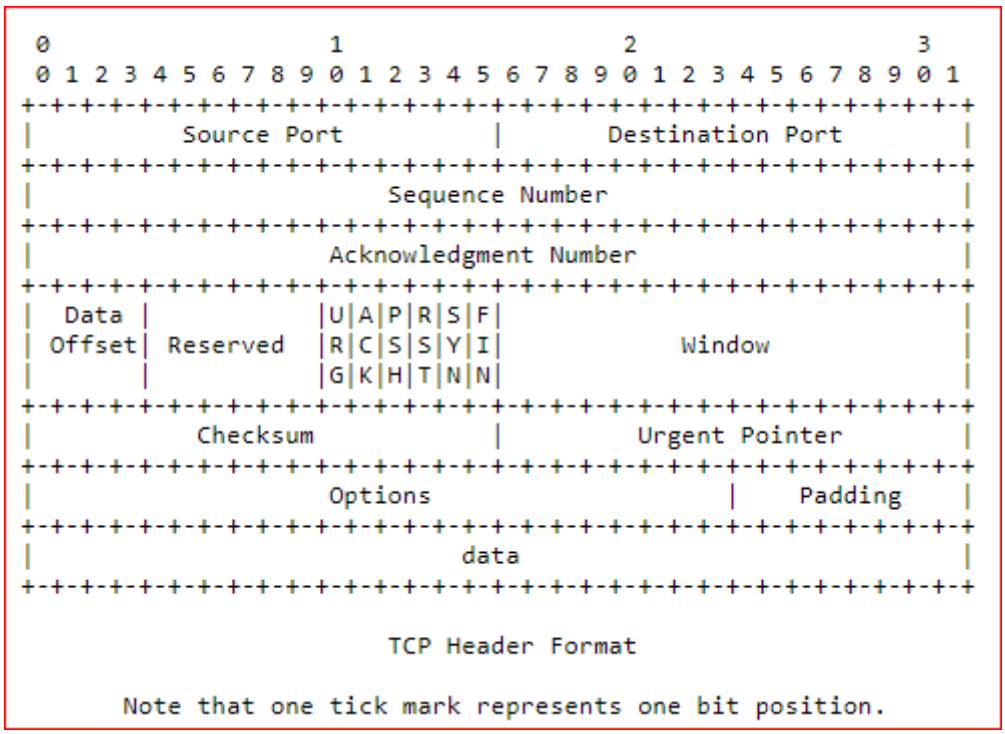
- Protocol
- Source Address
- Destination Address



University of Southern California (Dominio público)

TCP

- Source Port Number
- Destination Port Number



University of Southern California (Dominio público)

Para conocer los puertos asociados a cada protocolo, la IANA dispone de un registro de número de puertos, protocolos y servicios asociados.

1.1.- Seguridad perimetral.

Uno de los elementos principales en la seguridad perimetral son los **Firewall**. Son uno de los dispositivos de seguridad más importantes de la red, ya que nos permite ser una de las principales líneas de defensa para tener el **control de los flujos de información**. La finalidad de estos programas o dispositivos es proteger, controlar y monitorizar el acceso a otras redes (internas o Internet) con el fin de impedir accesos no autorizados.

El ENS indica que se dispondrá de un sistema cortafuegos que separe la red interna del exterior, como medida de protección - Perímetro seguro [mp.com.1]. - Todo el tráfico deberá atravesar dicho cortafuegos que sólo dejará transitar los flujos autorizados que previamente se hayan definido.

Si comparamos el firewall con un control de acceso a un concierto en un recinto, el firewall sería el personal encargado de controlar la entrada de personas al evento. Por lo tanto, los administradores de seguridad del firewall tienen la tarea de configuración del dispositivo para permitir o denegar la entrada o salida de información red en función de numerosos factores, como:

- ¿De dónde viene el tráfico?. El firewall que acepta/rechaza el tráfico de una red o equipo específico.
- ¿Hacia dónde va el tráfico? El firewall que acepta/rechaza el tráfico destinado red o equipo específico.
- ¿En qué puerto es el tráfico? El firewall que acepta/rechaza el tráfico con determinado puerto de destino.
- ¿Qué protocolo está utilizando el tráfico? El firewall que acepta/rechaza el tráfico con determinado protocolo (TCP/UDP)

Para contestar a estas pregunta, los firewall inspeccionan los paquetes para poder responder a estas preguntas y tomar una decisión.

Los cortafuegos pueden ser productos hardware o software, cada uno con sus capacidades de control dependiendo del volumen de la red y del propósito del mismo.

Autoevaluación

¿Cómo nos ayuda el firewall a proteger nuestro sistema?

- ○ Controlando los flujos de información
- ○ Nos defiende de phishing
- ○ Gestionar vulnerabilidades

Correcto. Es la característica principal del firewall desde el punto de vista de la seguridad. CONTROL

Incorrecto. Ante estos ataques, la concienciación y las reglas de seguridad del correo electrónico son las que nos defienden.

Incorrecto. Puede ayudarnos restringir flujos de comunicación en base a IPs, puertos o protocolos pero no detecta ni gestiona vulnerabilidades del nuestro sistema.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto

1.2.- Generación de Firewalls.

La **primera generación** de firewall tenía la funcionalidad de inspeccionar los paquetes que pasaban por el dispositivo, cotejándolo contra una serie de reglas y tomando la acción de permitir o denegar el paso del paquete según estas reglas. Estos firewall trabajan en las capas 3 y 4 del modelo OSI (Red y Transporte). El filtrado se produce en base a:

- Direcciones IP
- Protocolo
- ToS (Tipo de Servicio)
- Puerto TCP o UDP (Capa 4)
- Flags TCP (SYN, ACK, FIN…),…

Estos firewall de primera generación tienen las siguientes **limitaciones**:

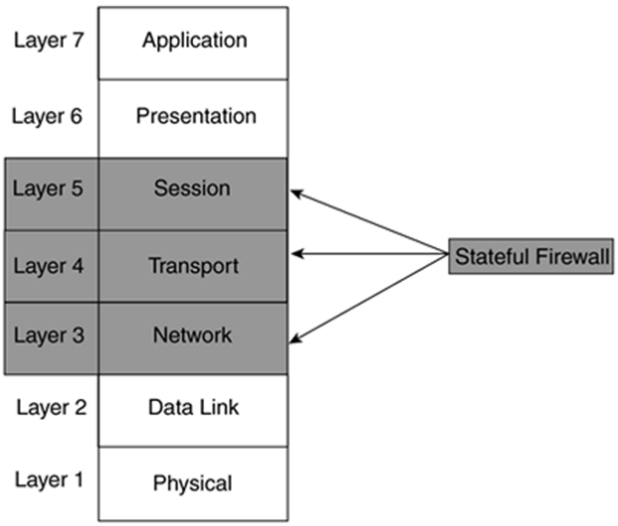
- Se debe establecer un **procedimiento de gestión de reglas**. Porque si el número de reglas es muy elevado es muy costoso crear y mantener todas las reglas si no existe un procedimiento.
- **No** protegen de ataques de **capa de aplicación** (XSS en HTTP por ejemplo)
- Son **susceptibles a algunos ataques de capa TCP/IP** (TCP SYN floods o IP Spoofing)
- Tienen capacidades de **información (logs) limitadas**, ya que sólo nos proporcionan información sobre las capas 3 y 4.

Los firewall de primera generación son estáticos (stateless), porque se utilizan un conjunto el conjunto de reglas definido con cada paquete de manera individual. Por ejemplo, se puede denegar un paquete específico enviado por un dispositivo pero no significa que el dispositivo esté bloqueado.

Si alguna de la reglas definidos no coincide con la características del paquete, la última regla definirá la acción a tomar sobre este. Por lo que es necesario definir una regla de denegación ante este tipo de situaciones.

Sin embargo, estos cortafuegos son excelentes cuando se reciben grandes cantidades de tráfico de un conjunto de hosts (como un ataque de denegación de servicio distribuido).

La **segunda generación** de firewall están basado en estado (stateful) y añaden la capacidad de analizar la información de las conversaciones en lugar de inspeccionar un paquete individual, recordando los puertos que se han usado en capa 4 para permitir analizar el intercambio de paquetes, esta capacidad se denomina Stateful Inspection. Este tipo de cortafuegos utiliza toda la información de una conexión y si una conexión de un host es mala, bloqueará todo el dispositivo.



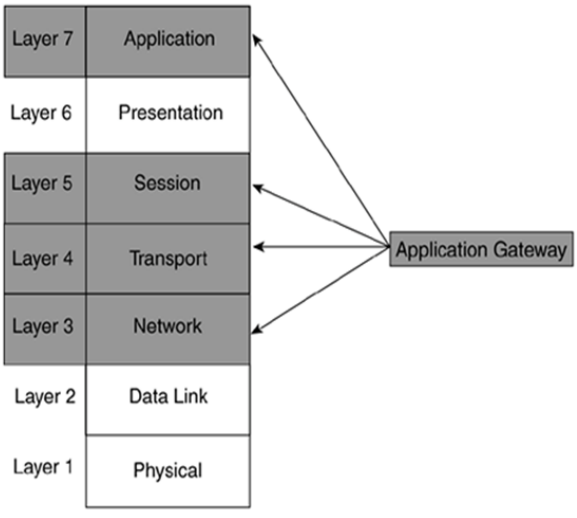
etutorials. *Firewall con estado* (Dominio público)

Estos firewall de segunda generación tienen las siguientes limitaciones:

- Tiene una **mayor complejidad de configuración** que los de primera generación.
- **No protegen de ataques de capa de aplicación** como los de primera generación.
- No soportan el análisis de **conexiones cifradas**.
- **Ralentizan** la red porque necesitan realizar el **análisis** de los paquetes en base a la tabla de estados.
- Tiene **limitaciones** con aplicaciones **multimedia.**
- Son **susceptibles** ataque a **DoS** por la limitación en el tamaño de la tabla de estado.

En los firewall de **tercera generación** los fabricantes han diseñado nuevas funcionalidades que se añaden a las funcionalidades básicas del firewall y que permite darle un mayor control de las comunicaciones a las distintas capas de los protocolos de red y a tecnologías de inspección de paquete (**DPI**) para permitir o denegar el tráfico.

Son capaces de entender elementos de la capa de aplicación (FTP o HTTP…) permitiendo detectar aplicaciones usando puertos no comunes (SSL over DNS). También tienes la funcionalidad de permitir iniciar sesión a los usuarios antes de realizar la conexión portal cautivo.



etutorials. *Firewall a nivel de aplicación* (Dominio público)

Tipos de Firewall de tercera generación:

- **Connection Gateway Firewall (CGF):** en esto firewall las comunicaciones están asociadas a una cuenta que necesita autenticación, se aplican las reglas en base a las capas de aplicación, sesión, transporte y red y se monitoriza la conexión con un alto nivel de detalle.
- **Cut-Through Proxy Firewalls (CTPF):** también se conocen como cortafuegos de aplicaciones (AF). Hacen de intermediarios entre el cliente y el servicio final de las aplicaciones para dotar al firewall de capacidad de análisis de la información de la capa de aplicación. Son muy específicos por aplicación por lo que no funcionan de manera genérica para todos los protocolos.

1.3.- Firewalls de próxima generación.

Firewalls de próxima generación

Linux Screenshots (CC BY)

Los cortafuegos de próxima generación (NGFW) ofrecen mayor nivel de protección que los cortafuegos originales. Uno de los motivos es que inspeccionan todas las capas del modelo OSI.

Los nuevos firewall están **aglutinando las capacidades** de otros dispositivos de seguridad como **IPS, IDS o WAF,** siendo este un elemento más crítico en la arquitectura. Al disponer de más funcionalidades existe la posibilidad de incluir en estos dispositivos la información relativa a la inteligencia de amenazas o **IOCs**: dominios, IPs,.. lo que que permite trabajar a estos dispositivos con una mayor eficiencia.

Todo este volumen de datos que se integran en las nuevas soluciones a través de tecnologías Big Data e IA es lo que permite detectar de una manera más temprana los nuevos mecanismos de ataque, ya que muchos de los indicadores van cambiando rápidamente.

También existen los firewall proporcionados por un proveedor como un servicio en cloud Firewall (FWaaS), sustituyendo el firewall de on premise e la compañía por un entorno de nube. Sus características suelen ser las de NGFW . Un ejemplo es AWS WAF para la protección de aplicaciones web y AWS Shield para la protección DDoS.

Además de realizar un bastionado de este elemento clave, no se debe olvidar que existen **procedimientos operativos de seguridad (POS)** para que la gestión/administración del dispositivo no se realice de una manera aleatoria, sino que esté basado en procedimientos corporativos que permitan no perder el control de las reglas aplicadas y el motivo de su inclusión. La aplicación de excepciones también debe tener un **procedimiento para que las excepciones** no pongan en peligro la seguridad de la red.

Se deben conocer las diferentes técnicas que intentan evitar los controles de seguridad aplicadas por el firewall. En el siguiente enlace se indica métodos de evasión de Firewall a través de nmap. Con el objetivo de controlar que la configuración del firewall pueda evitar estas técnicas.

Estas son algunas de las medidas de bastionado asociado al firewall:

- Proteger el descubrimiento de la arquitectura de red y los activos que lo componen, bloqueando el protocolo ICMP por defecto (ping) y sólo permitirlo para ciertos equipos que realicen tareas de administración.
- Todas las reglas tienen que ir alineadas con las políticas de seguridad de la empresa.
- Al ser la parte de la red que es la más expuesta, es la que debe tener un mayor control de la seguridad: actualizaciones, backup, gestión de incidentes, gestión de accesos, registro de eventos,...
- Las reglas deberán estar basada en IP de origen, IP de destino y servicio utilizado.
- Se debe poner especial cuidado en la reglas del tráfico de salida porque es el medio que impedirá la exfiltración de información.
- Poner especial cuidado en el protocolo DNS. Se debe controlar toda conexión a un servidor DNS externo, que no provenga de nuestro sistema DNS corporativo, estas acciones debe ser bloqueada a nivel de firewall.
- Debido al aumento del volumen de datos de conexiones en las organizaciones y el número de reglas a chequear y contrastar, deben ser equipos rápidos y con alta disponibilidad.
- La última regla marca la “política del FW”, por lo que se debe establecer como regla base de denegar todo el tráfico (deny-any) para que sólo se permitan las comunicaciones en base a las reglas definidas.

Autoevaluación

¿Qué firewalls pueden analizar los datos de capas superiores a las capa 4 de modelo OSI?

- ○ Firewalls de primera generación
- ○ NGFW
- ○ Firewall stateful

Incorrecto. Sólo analizan la capa 3 (red) y capa 4 (transporte)

Correcto. Estos firewalls son capaces de analizar la capa 7. Aunque no analizan todos los servicios de capa 7. Los relativos a servicios web son los WAF

Incorrecto. Aunque son más evolucionados que los de stateless ya que guardan todos los datos de la conexión. Sólo analiza los datos de capa 3 y capa 4

Solución

1. Incorrecto
2. Opción correcta
3. Incorrecto

2.- Seguridad de Portales y aplicativos web. Soluciones WAF (Web Application Firewall)

Caso práctico

Pixabay (Dominio público)

En el Instituto se ha implantado un nuevo sistema para que los alumnos puedan gestionar varias de la tareas con la secretaría: consulta de notas, justificación de asistencia, solicitud de duplicado de expediente, pago de excursiones, reserva de material,... La nueva funcionalidad estará publicada en la página oficial del Instituto, pero para sacar la aplicación a producción debemos realizar un conjunto de pruebas relativas a la seguridad acorde a OWASP.

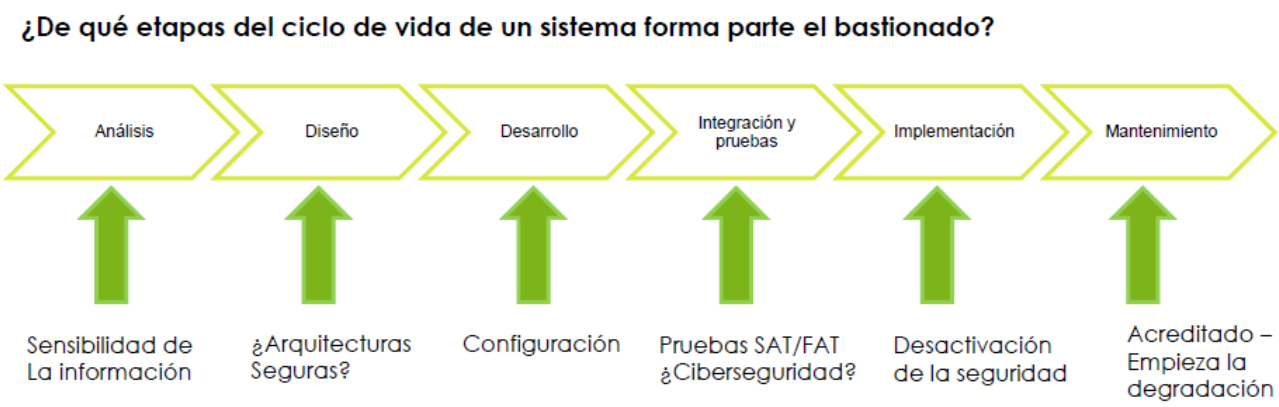
Identifica los al menos 5 pruebas relacionadas con la seguridad que estén relacionados con el OWASP TOP 10 de 2021 vulnerabilidades más explotadas por falta de desarrollo seguro.

Descubre OWASP

Broken Access ControlSensitive Data Exposure - Criptografic Failures Injection - Cross-site ScriptingInsecure DesignSecurity Misconfiguration - XML External EntityComponents with Known Vulnerabilities - Vulnerable and Outdated componentsBroken Authentication - Authentication and Identification FailuresInsecure Deserialization - Software and data Integrity failuresInsufficent Logging & Monitoring - Security Logging and Monitorin failuresServer-Side Request Forgery

La seguridad de los servicios web se debe establecer en las distintas etapas de ciclo de vida:

- Desarrollo: Desarrollo seguro de las aplicaciones.
- Instalación: Configuración segura del servicio.
- Mantenimiento: Monitorización y mejora continua del servicio.



Héctor Fernández Bardal. *Seguridad en el ciclo de vida del sistema* (Dominio público)

Para este capítulo el alumno dispone de las siguientes referencias.

- Guía CCN-STIC-812 - Seguridad en entornos y aplicaciones Web
- Bastionado básicos de apache.
- NIST SP 800-44 - Guidelines on Securing Public Web Servers

2.1.- Desarrollo e instalación.

La seguridad del desarrollo (security by design) debe estar basado en la seguridad desde el diseño. El diseño de aplicaciones de manera segura es fundamental para no tener que implementar medidas de protección adicionales, como indican algunas guías de referencia de desarrollo como por ejemplo OWASP .

Esto también es aplicable para los desarrollos web. Una vez finalizado el desarrollo de estos productos, la verificación se realiza a través de auditorías de seguridad y la inclusión de las pruebas de seguridad dentro del ciclo de desarrollo del producto.

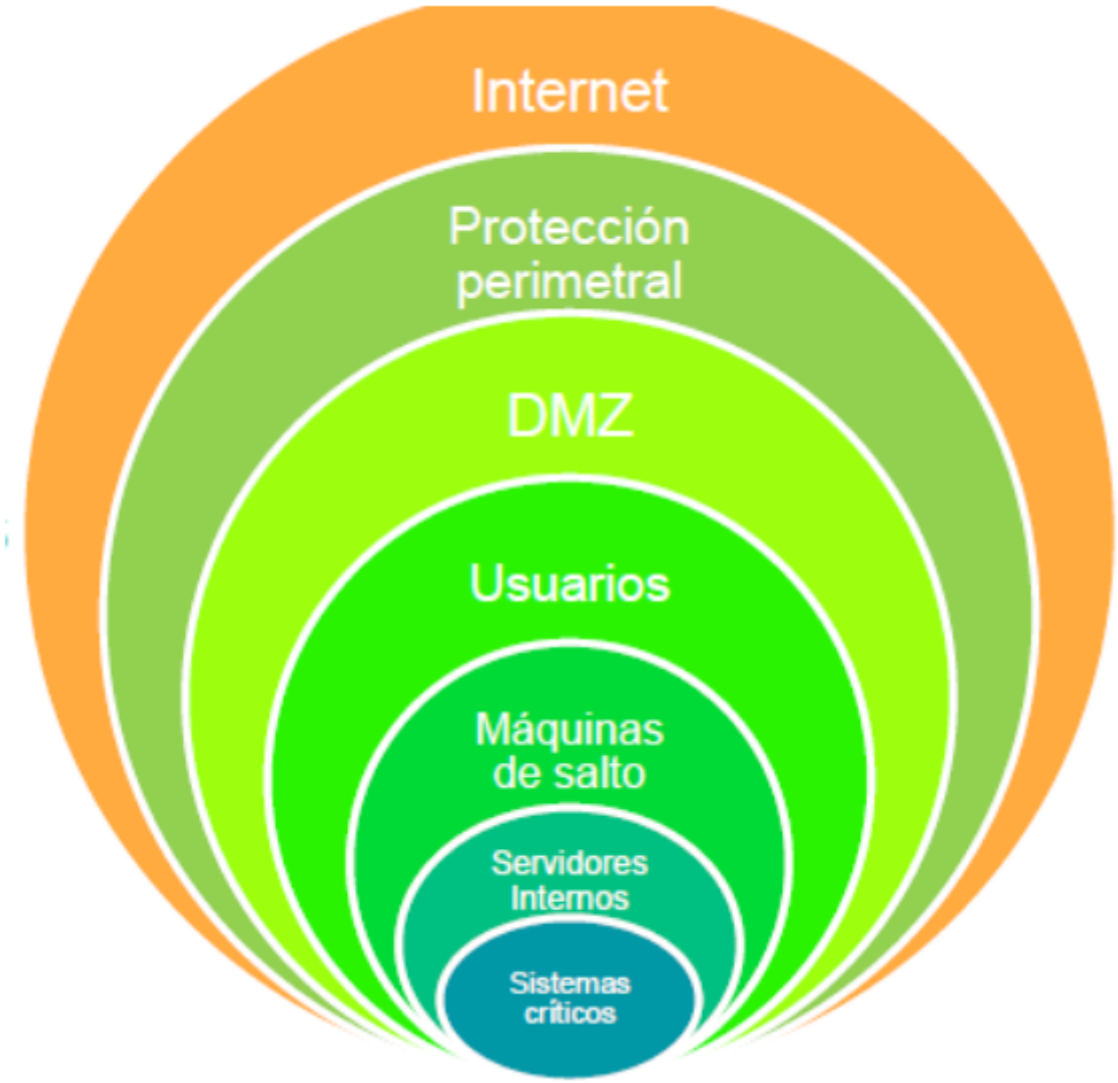
El sistema se debe configurar sobre una **arquitectura basada en capas**. En el que la capa de presentación es la que debe estar expuesta al exterior y está alojada en la DMZ.

La protección del servicio web tiene que estar sustentada por la configuración segura de los distintos componentes del servicio:

- Sistema operativo base que alberga el servicio.
- El servicio web
- Los servicios asociados al servicio web. Como por ejemplo la bases de datos.

Para este tipo de servicios, se debe implementar una seguridad basada en la **defensa en profundidad**, donde se vayan colocando cada uno de los diferentes elementos del sistema en una arquitectura basada en capas. A continuación, se indica un ejemplo de arquitectura basada en capas desde la capa más externa (frontal) a la más interna:

- Capa 1: Dispositivo de protección perimetral (DPP). Firewall, proxy inverso, WAF, IDS, …
- Capa 2: Servidor web
- Capa 3: Dispositivo de protección perimetral entre el servicio web y los servicios asociados: Firewall interno.
- Capa 4: Servicios asociados: bases de datos, servidores de ficheros,…



Héctor Fernández Bardal. *Defensa en profundidad* (Dominio público)

Los dispositivos más externos y perimetrales tendrán la misión de protegernos de los ataques externos. En la siguiente capa, zonas desmilitarizadas (DMZ), se colocará la parte más expuesta del servicio hacia el exterior y protegido por los dispositivos de protección perimetral. Existirá una protección de acceso desde la DMZ hacia la red exterior y existirá otro control de acceso desde la DMZ hacia la red interna por un firewall.

Uno de los dispositivos específicos que protegerá los servicios web es un WAF, un dispositivo de seguridad que permite proteger los servicios web de ataques específicos sobre tecnologías web. Como los indicados en el Top Ten de OWASP.

La mayoría de estos ataques web son protegidos por controles aplicados sobre la capas de aplicación (Capa 7 del modelo OSI).

Al igual que sucede con los firewalls de red, se debe disponer de un conjunto de reglas que permitan detectar los ataques más comunes, pero las reglas se deben adaptar siempre a las particularidades y contexto de la compañía.

Desde el punto de vista de los usuarios de la red, se debe proteger la navegación hacia los distintos servicios web externos a la compañía. Existen 2 políticas de actuación ante la aplicación de reglas de navegación de los usuarios en la red, que son:

- Basado en listas blancas.
- Basadas en listas negras.

Las listas negras requieren de reglas que permitan detectar comportamientos anómalos ante nuevas webs o dominios maliciosos de navegación que están en listas de IOCs recopilados por empresas y organismos de ciberseguridad. Mientras que la política basada en listas blancas sólo se permite la navegación aquellos dominios permitidos por política de empresa y acorde a su contexto empresarial. Es más costosa su configuración inicial, pero una vez implementado la lista inicial permite realizar un mayor control sobre los sitios web permitidos. La inclusión de nuevos elementos en la lista constituye un proceso sencillo. Con esta política la navegación estaría más controlada pero la gestión de accesos a recursos web es más costosa porque necesita de un procedimiento de análisis de riesgos previo.

2.2.- Mantenimiento.

Todos los dispositivos del servicio deben ser configurados de manera segura y deben tener una vigilancia a través de la monitorización. De tal manera que la información de los eventos que sucedan en el sistema esté sincronizado con el SOC, registrando todas las interacciones que existan con el servicio web con el objetivo de monitorizar el servicio y responder ante un incidente de seguridad.

Durante la fase de mantenimiento debe existir un procedimiento de mejora continua de la monitorización ante los diferentes incidentes o cambios en la arquitectura.

Si la **gestión del servicio es externa**, deberá existir un protocolo de notificación de incidente, definiendo claramente tareas asociadas al proveedor del servicio y a la organización. El procedimiento operativo incluirá información de cómo se realiza el aviso del incidente, tiempos de resolución, canal de comunicación con el cliente y actores asociados. Toda esta información se puede reflejar en una **matriz RACI**.

Es necesario dimensionar la infraestructura de monitorización en base al tiempo de retención de cada uno de los registros (logs) de las diferentes fuentes. Y en el caso de producirse un incidente poder realizar un análisis completo de lo sucedido. Por lo que se deben incluir logs de los elementos de las diferentes capas: firewall, servidor web, proxy, base de datos,...

Autoevaluación

¿En qué fase del ciclo de vida de un sistema es más ventajoso aplicar seguridad?

- ○ Diseño
- ○ Pruebas
- ○ Mantenimiento

Correcto. En cuanto antes se empiecen a tener en cuenta la seguridad del sistema más beneficios aportará. Security by design

Incorrecto. El sistema tendría que volver a ser rediseñado al no haberse tenido en cuenta la seguridad.

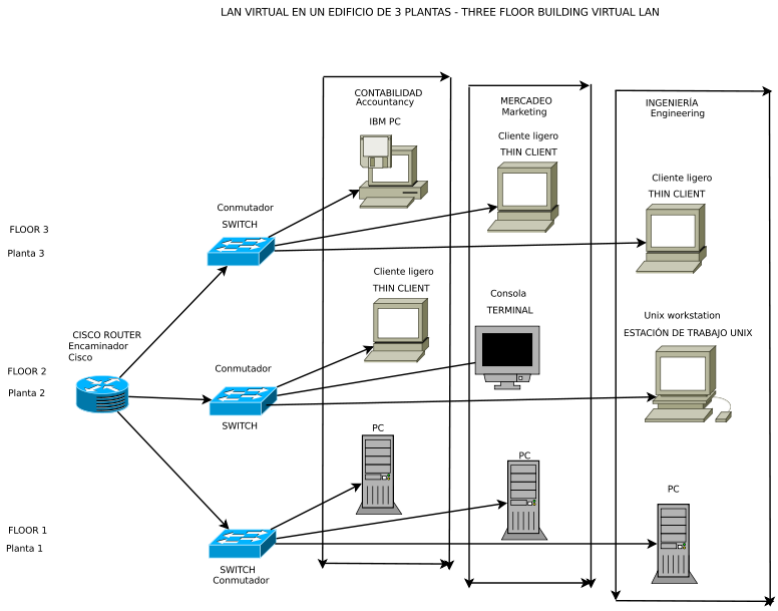
Incorrecto. El sistema está en producción y es probable que sufra o va a sufrir incidentes de seguridad (assume the breach). En este momento hay que proteger el equipo, pero existirán riesgos que habrá que asumir.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto

2.3.- Medidas de seguridad sobre servicios web.

- Los portales de nuestra compañía deben estar configurados con protocolos seguros de transmisión de la información (HTTPS). Estableciendo la protección del servicio con un certificado web de confianza(https). Esto permitirá el cifrado de las comunicaciones entre los usuarios y el servidor web. El certificado del servidor web debe ser de la CA de reconocida.



Rafax (CC BY)

- El acceso a la administración del servicio debe estar segmentada en una VLAN propia de administración y a través de protocolos seguros y no vulnerables.
- Si el servicio está alojado en un proveedor externo, cuando se configure el servicio, se debe establecer una matriz RACI de cara a que ninguno de los aspectos relativos a la seguridad esté sin cubrir. Cada una de las responsabilidades debe establecerse con el fin de que la seguridad sobre el servicio esté garantizada.
- Deben existir mecanismos de autenticación de los usuarios al servicio web.
- Deben existir mecanismos de identificación única única por usuario en su parte privada.
- Existirá un mecanismo de protección contra los ataques de fuerza bruta con CAPTCHA.
- Se dispone de procedimientos operativos seguros de recuperación de contraseñas, cambio de contraseñas, bloqueo de usuarios, alta de usuarios,…
- Existirá una política de contraseñas segura, no permitiendo el establecimiento de contraseñas débiles.
- Las contraseñas de administración de cada uno de los componentes del servicio web deben establecerse con 2FA y se indicará desde qué dispositivos se realizará la administración de los equipos. Se debe poner especial atención a mantener usuarios por defecto tras su instalación, dichos usuarios se deben deshabilitar o cambiar su nombre y contraseña
- De cara a la protección de la información interna, los documentos publicados no deben tener metadatos, para no facilitar información sensible e interna de la organización.

- Procedimiento de actualizaciones del sistema. Entre los principios básicos de seguridad está la actualización de cada uno de sus componentes. Además, al ser servicios que están expuestos al exterior y suelen estar en publicados en los servicios DMZ, estos parches de seguridad deben solventarse en primera prioridad, ya que son accesibles para cualquier atacante. Es necesario mantener actualizados el software de todos los componentes del sistema: servidor web, servidor de base de datos, servidor de contenidos (CMS),...

- Se debe tener control de las interconexiones del servicio web con servicios externos, haciéndose siempre la interconexión por medios de cifrado seguros, y con autenticación. Este control es necesario, para que en caso de que los sistemas interconectados sufran un incidente no se pueda expandir a nuestra infraestructura. Se pueden aplicar los siguienets mecanismos de protección contra estos servicios externos:
    - Autenticación fuerte entre servicios: usuario/password, 2FA, certificados,...
    - Filtrado de conexión por IPs
    - Protocolos seguros de comunicación.

- De cara a mantener el servicio se debe disponer de un diagrama de arquitectura del sistema que aloja el servicio web, donde se incluirá un diagrama con los flujos de información entre los diferentes componentes (internos y externos) y protocolos utilizados en los diferentes flujos de información.

- Se realizarán auditorías de seguridad con una periodicidad regular (inferior a 6 meses) en el que se establezcan medidas correctoras sobre los fallos de seguridad encontrados. En la siguiente auditoría se debe indicar qué medias se han implementado para subsanar las deficiencias encontradas.

- Se establecerán requisitos más restrictivos para el acceso a las partes privadas de la web. Por ejemplo: los usuarios deben acceder con autenticación basada en 2FA y sólo pueden acceder desde determinados equipos.

- Deberá existir un método de cifrado de información que se almacena (cifrado en reposo) en el servicio.

- Eliminar todas las contraseñas y usuarios por defectos del software y de las herramientas que soportan el servicio.

- Se definirá los procedimientos de operativos de las web: recuperación de contraseñas, alta\baja\modificación de usuarios de la web, métodos de subida y descarga de ficheros,etc. Y estos procedimientos no serán vulnerables ataques.

2.4.- WAF.

WAF (cortafuegos de aplicaciones web)

Un WAF es un dispositivo de protección de la seguridad que está localizado entre los clientes y el servidor web; su objetivo principal es proteger el servidor web de ataques malware o de denegación de servicio.

Está dentro de la categoría de proxy firewall, siendo el intermediario entre el cliente web y el servidor para poder inspeccionar y analizar el contenido de los paquetes del servicio web.

Autoevaluación

Cual de las siguientes es una metodología de desarrollo seguro

- ○ OWASP
- ○ OSSTMM
- ○ Scrum

Correcto.

Incorrecto. Es una metodología de pentesting o pruebas de seguridad

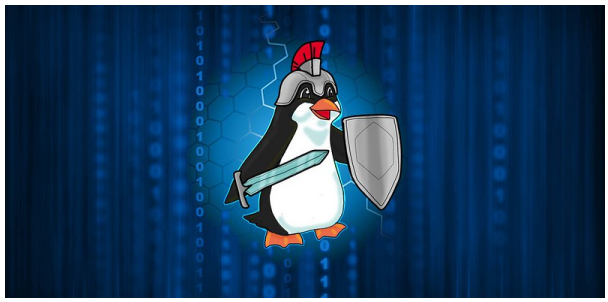
Incorrecto. Es una metodología ágil para el desarrollo. No tiene por qué tener en cuenta la seguridad.

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto

3.- Segmentación de redes.

Caso práctico



Richard Patterson (CC BY)

La envasadora localizada en el pueblo de "Catarrejos" ha decidido unir la red que controla los robots de embotellado (red OT) con la red que ya tenía desplegada para gestión empresarial (red IT), donde los equipos de gestión e ingeniería realizan la labores de marketing, facturación, recursos humanos... El objetivo es poder tener datos de fabricación: número de litros que se embotellan, los índices minerales del agua, fallos de los robots,...en la red corporativa.

Esta red tiene un impacto alto en la operativa, ya que si se viera afectad algún fallo, incidente o ataque pararía la producción y repercutiría en pérdidas económicas.

¿Qué criterios de seguridad utilizarías para integrar esa red de fabricación, con la red corporativa?

Protege la fábrica

Uno de los criterios básicos es la segmentación de la red. Por lo que debe existir un control de flujos de información desde la red corporativa IT a la red OT.

Los accesos directos a la red de fabricación no deberían existir, y para acceder a la red de la fábrica siempre se debe acceder primero a la red IT, aplicando el criterio de defensa en profundidad.

Se deben establecer los usuarios que tienen acceso en la red IT, para segmentar la red de usuario que podrán acceder a la red OT.

Cada una de la capas de acceso deberá estar protegido por un dispositivo de protección perimetral.

La segmentación de redes desde el punto de vista de la seguridad permite:

- Proteger los activos por importancia y determinar las reglas de acceso de unos dispositivos a otros.
- Realizar una defensa en profundidad

- Segmentar los flujos de información y establecer la máxima seguridad para aquellos flujos críticos.
- Contener la propagación de la infección de los sistemas.
- Tener más información de lo que ocurre en el sistema. En base a la información de vigilancia suministrada por los dispositivos que realizan la segmentación.

La segmentación se puede realizar por capas:

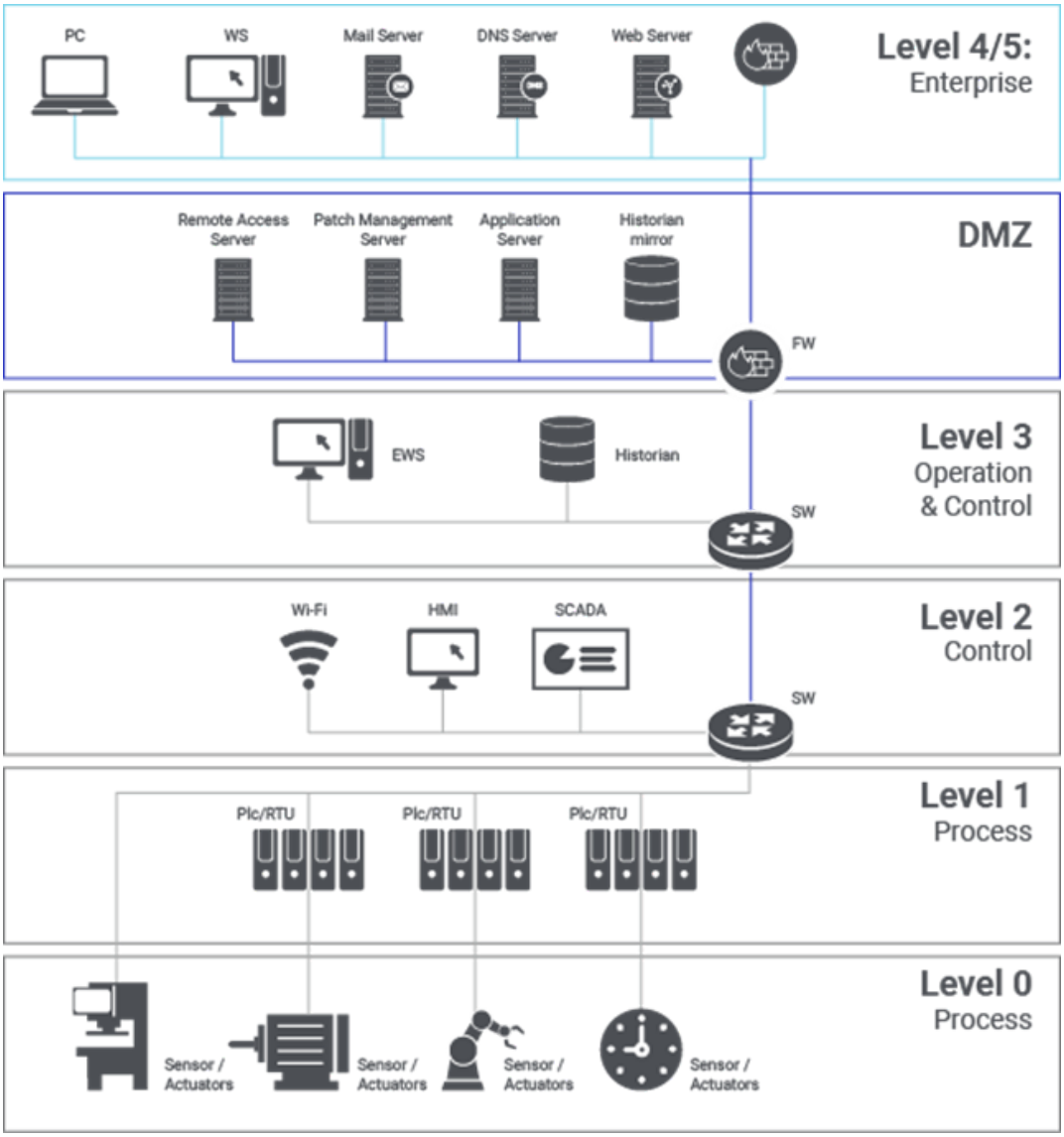
- En la capa de enlace (capa 2). Mediante la creación de VLANs. Controlada y gestionada por switches.
- En la capa de red (capa 3). Mediante la creación de redes. Controlada y gestionada por routers y firewalls.

Esta segmentación está apoyada por dispositivos de red y de seguridad de red que permitirán controlar las comunicaciones.

Switches	Puerto sin uso deshabilitados – VLAN específica. Filtrado por MAC Activación auditoría. Envío auditoría a servidor externo. Cambio VLAN por defecto Arranque seguro Administración y operación separados Contraseñas cifradas
Router	Puerto sin uso deshabilitados – VLAN específica. Activación auditoría. Envío auditoría a servidor externo. Cambio VLAN por defecto para ciertos protocolos Arranque seguro Administración y operación separados Contraseñas cifradas Eliminación de protocolos inseguros:

Héctor Fernández Bardal. *Medidas seguridad router y switch* (Dominio público)

Para las redes industriales existe un modelo de segmentación basado en capas y defensa en profundidad que es modelo IEC 62443 que hace referencia al modelo Purdue.



Zscaler (Dominio público)

Más información sobre los modelos de arquitectura OT de ciberseguridad IEC 62443.

Autoevaluación

¿Cuál de las siguientes respuestas es un beneficio de la segmentación de redes desde el punto de vista de la seguridad?

- ○ Control de flujos
- ○ Separar los equipos por departamentos
- ○ Conocer el número de equipos de la empresa

Correcto. El control de flujos a través de reglas, y la visualización de flujos a través de la monitorización. Son beneficios preventivos y reactivos respectivamente.

Incorrecto. Puede ser un criterio organizativo, pero sin más información no se considera de seguridad

Incorrecto. Ayudará a controlar los activos, fundamental para la seguridad, pero no es el objetivo principal de la segmentación

Solución

1. Opción correcta
2. Incorrecto
3. Incorrecto

4.- Subnetting.

Caso práctico

En la red de Ministerios de Hacienda existen interconexiones con otros organismos que facilitan los datos de entrada al sistema. Esta conexiones se producen entre dos dispositivos únicamente, por lo que ningún equipo más podrá pertenecer a esta red con el fin de evitar ataques MiM (man in the middle), y tener controlados y restringidos los accesos.

Malwarebytes (Dominio público)

Subnetting

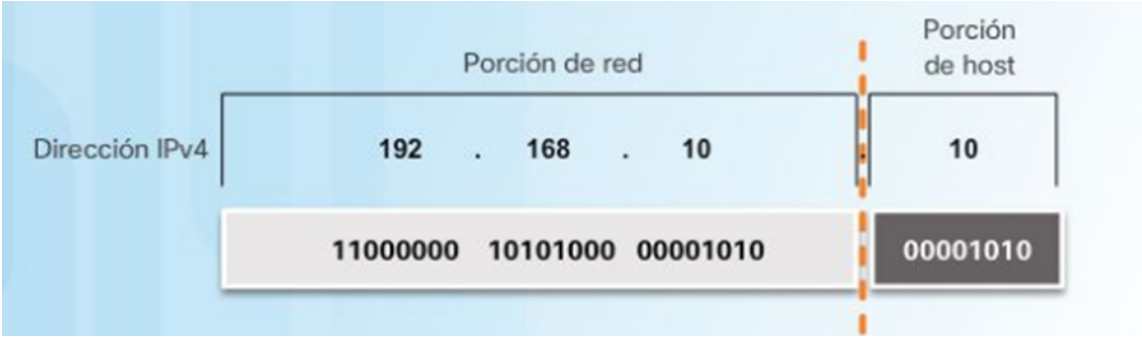
Una dirección IP está formada por conjunto de cuatro números llamados octetos. El valor de cada octeto será entre 0-255. Este número se calcula en base al direccionamiento y a la división de la red en subredes. Desde el punto de vista e la seguridad es necesario saber que las direcciones IP pueden cambiar de un dispositivo a otro, pero no pueden coincidir dos IPs dentro de una red. La IP constituye un identificador de control de los dispositivos.

Desde el punto de vista de la seguridad se deben tener en cuenta la segregación de redes en redes más pequeñas en base a:

- Separación de redes de usuarios y servicios
- Crear controles de seguridad en el paso de unas redes a otras.

- Establecer controles de conexiones para los usuarios con privilegios de administración.
- Permitir un control y gestión de la configuración de manera más eficiente.

Dentro de una red y el protocolo IP, el identificador que permite localizar a un dispositivo es la IP, que está dividida en 2 datos: la red y el equipo, proporcionando control y seguridad.



Kevin Linares (Dominio público)

Los principios que permiten realizar la segmentación de las redes desde el punto de vista del diseño no es objeto de este curso. Adjuntamos un enlace con los principios de subnetting para IPv4.

Para conocer la seguridad del subnetting es necesario conocer los protocolos asociados y sus ataques más comunes:

- ARP
- ICMP
- TCP
- DHCP

Se pone de manifiesto el concepto de **segmentación activa**, con el objetivo de aplicar mecanismo de defensa activa en caso de incidentes de seguridad que permitan realizar de una manera automática las primeras medidas de protección: aislamiento de zonas, reducción de superficie de ataque,…

Dentro del subnetting tenemos que poner especial atención en el bastionado a los equipos que realizan la segmentación:

Switches

Los switches son dispositivos de red que han sido diseñados unir varios dispositivos: PCs, impresoras u otros dispositivos que utilicen Ethernet. Estos dispositivos se conectan a un puerto del switch que identifica al dispositivo. De esta manera, cuando reciben un paquete, en lugar de repetir ese paquete en cada puerto como lo haría un hub lo envían a un destino específico reduciendo el tráfico de red. Estas comunicaciones se producen dentro de lo que se denomina dominio de broadcast.

Routers

El objetivo de un enrutador es conectar redes y transferir datos entre ellas. El enrutamiento es un proceso de encaminar datos que viajan entre las diferentes redes, creando una ruta.

Firewall

Con el firewall determinamos la reglas que permiten las comunicaciones desde unas capas de la red a otras. También pueden tener capacidades de enrutamiento y segmentación.

5.- Redes Virtuales (VLANS).

Caso práctico

El CEO de una importante industria farmacéutica está preocupado por la seguridad de su información, porque han descubierto un importante hallazgo sobre un medicamento. Quiere que esta información esté protegida y necesita que los equipos estén conectados dentro del laboratorio. Pero que esa información quede "confinada" dentro de la red específica (VLAN) del laboratorio y por lo tanto no tengan conectividad con el resto de departamentos que sí tienen conexión a Internet.

Wikipedia (Dominio público)

Tendremos que diseñar una estructura de VLANs en el que la información no salga del laboratorio. Sólo habrá un equipo de control, que proporcionará la entrada y salida de información del laboratorio. Este equipo tendrá que tener un requisito hardware adiccional y será el punto más crítico de nuestra red de laboratorio.

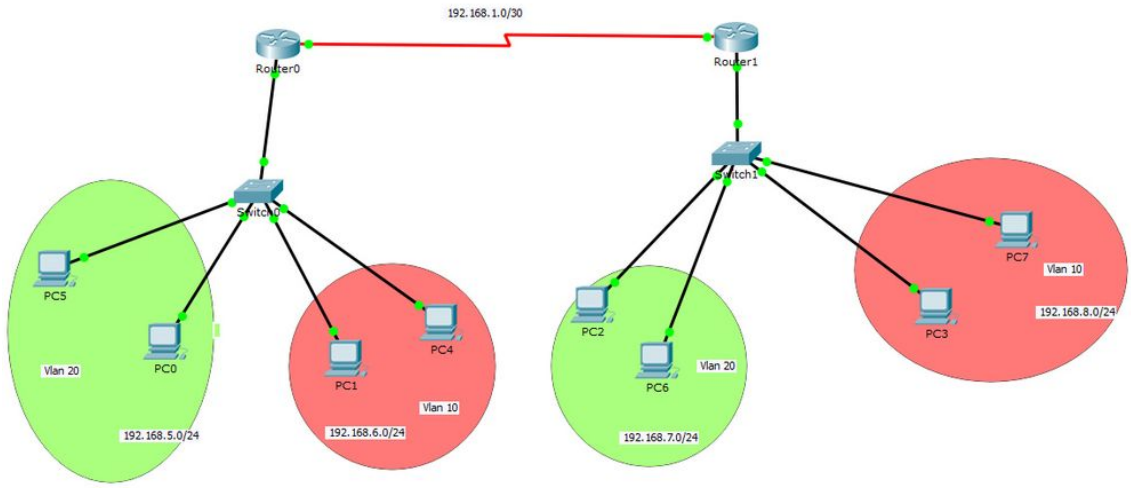
Protección VLAN

En la siguiente imagen se realiza una propuesta de VLANs asociadas con el laboratorio.

Redes Virtuales (VLAN)

Analizaremos los posibles ataques relativos a VLANs para poder realizar los mecanismos de seguridad que debemos aplicar a los dispositivos que las implementan que son los switch.

Las VLANs permiten que los dispositivos de una red se dividan virtualmente, pero beneficiándose de servicios de la red: internet, monitorización, servicios,… Esta separación de red aporta seguridad basada en las reglas que determinan cómo se comunican los dispositivos entre sí de dos redes diferentes.



Cisco. *VLANS* (Dominio público)

Es necesario analizar en los dispositivo que gestionan las vlan (switchs) los protocolo que tiene que asignadas VLANs por defecto (VLAN 1) para enviar mensajes cada cierto tiempo. En caso de no utilizarlos es necesario desactivarlos. Estos protocolo son:

- STP (Spaning Tree Protocol)
- GVRP
- LLDP

Como medidas de seguridad asociada a las VLAN se deben realizar las siguiente acciones :

- Desconectar los puertos que no esté en uso
- Establecer una VLAN específica para aquellos puertos que no esté en uso.
- Establecer seguridad en cada puerto asociado a una MAC.
- Realizar reglas de control de acceso entre las diferentes VLAN

Se recomienda la lectura de una guía de referencia de bastionado CCN sobre el bastionado de un switch hp.

Uno de los ataque más comunes asociado a no eliminar la VLAN 1 por defecto a los puertos de trunk es VLAN Hoping. Con la manipulación del protocolo de negociación automática de los puertos en modo "trunk" del protocolo DTP

podemos acceder a otra VLAN aunque no sea la de nuestro puerto, en el siguiente video demostrativo se puede ver el ataque.

Autoevaluación

Cual no es una medida de bastionado de un switch

- ○ Cifrado de las contraseñas almacenadas en el equipo
- ○ Tener actualizado el firmware
- ○ Crear al menos 5 VLANs

Incorrecto. Albergar contraseñas en claro o con algoritmos débiles de cifrado en una mala práctica de seguridad

Incorrecto. La actualización de software es uno de los principios básicos de seguridad

Correcto. El número de VLANs estará acorde a las necesidades del sistema, no se determina un número concreto. Pero no olvidar el principio fundamental de la segmentación

Solución

1. Incorrecto
2. Incorrecto
3. Opción correcta

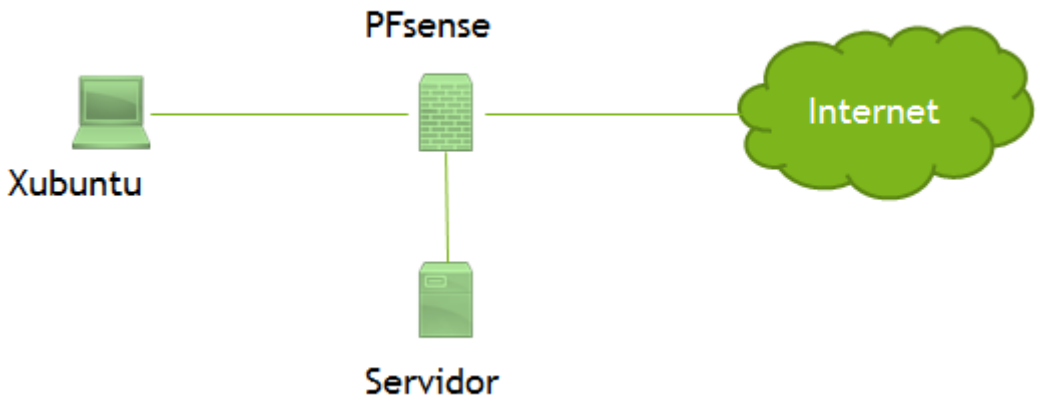
6.- DMZ.

Caso práctico

Vamos a revisar la reglas que tenemos que configurar en el firewall de la DMZ. En la DMZ sólo tenemos tenemos servidor web y queremos permitir los siguientes flujos de información :

- Habilitar NTP desde el servidor web hacia la red interna
- Habilitar DNS desde el servidor web hacia la red interna
- Permitir Web desde el exterior y red interna
- Bloquear tráfico a la red interna

Indica las reglas que deberíamos tener en el firewall. Podría explorar estas opciones en un pfsense.



Héctor Fernández Bardal. *DMZ con pfsense* (Dominio público)

Reglas

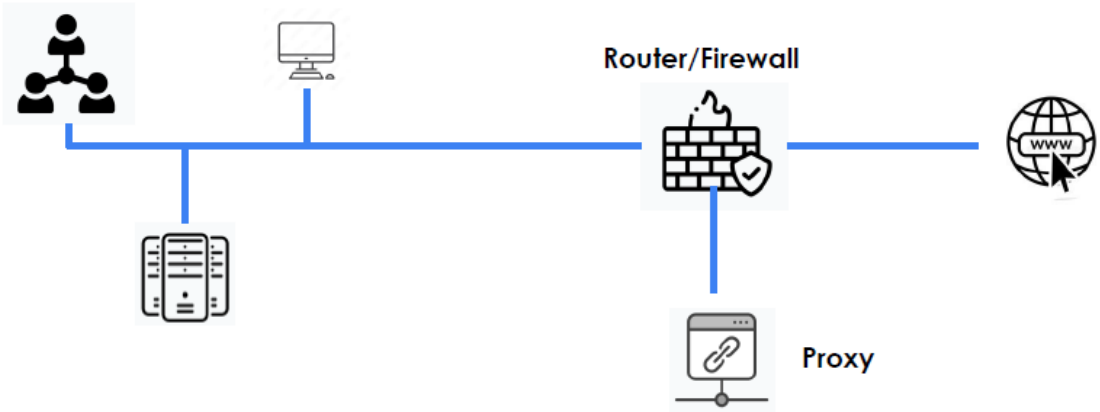
Allow TCP 80 from * (HTTP) to DMZ.Allow TCP 443 from * (HTTPS) to DMZ.Allow TCP/UDP 53 from DMZ to DNS server(s)Allow UDP 123 from DMZ to NT server.Deny any

La **DMZ** es la capa de nuestra red que contiene los servicios que están expuestos al exterior. Esta parte de la red está separada del resto de red corporativa ya que es la que está conectada a las redes que la compañía determina como no confiables (generalmente internet). Por lo que es la superficie de nuestra red que más probabilidad tiene de sufrir ataques o incidentes de seguridad. Por lo que el paradigma de **reducción de la "superficie de exposición"** debe hacerse en esta capa de manera especial. Además es necesario asegurar los flujos de información desde esta capa hacia el interior a través de un firewall. Estableciendo reglas que controlen los flujos de información de la DMZ a la red interna en el firewall que las separa.

Pueden existir en una arquitectura **varias DMZ** en las que se establezcan los niveles de seguridad de cada DMZ. El nivel de seguridad marcará las reglas del paso de información de una red de menor seguridad a otra de mayor seguridad. En esta guía de referencia del CCN sobre interconexiones se podemos ver los diferentes dispositivos de protección perimetral (DPP).

En un caso concreto la DMZ puede estar implementada por un firewall o por dos. En el caso de dos cortafuegos, uno de los firewalls permite la entrada de datos a la DMZ y el otro firewall permite la salida. En este modelo debe estar limitada la comunicación entre los dos firewalls.

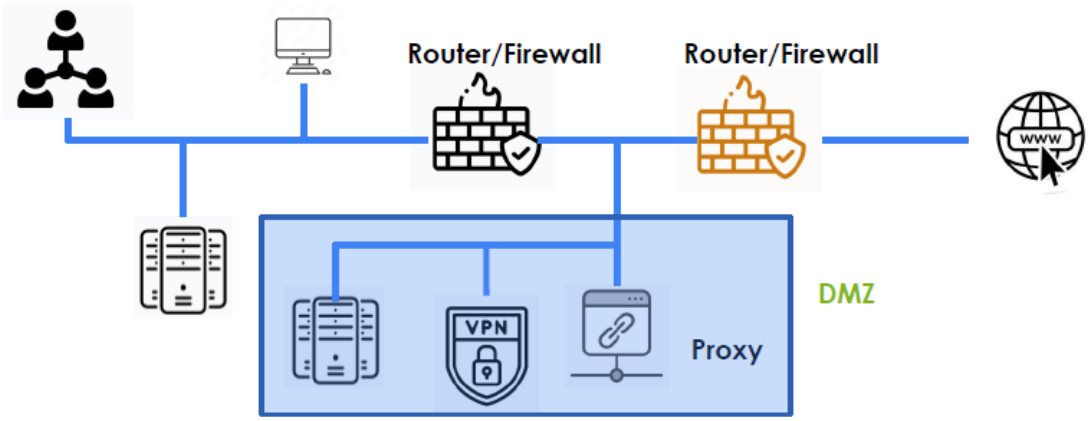
Con la arquitectura de dos firewall dificultamos los ataques, ya que es necesario comprometer ambos firewall, además el atacante no debe ser interceptado por las medidas de seguridad implementadas en la DMZ. Para elevar más la seguridad y que los firewalls no puedan ser atacados con el mismo vector de ataque se deben utilizar firewalls de diferente fabricante, diferente software, diferente configuración, diferentes administradores de seguridad, etc.



Héctor Fernández Bardal (Dominio público)

Los servicios más comunes en la DMZ y que requieren de una configuración segura son:

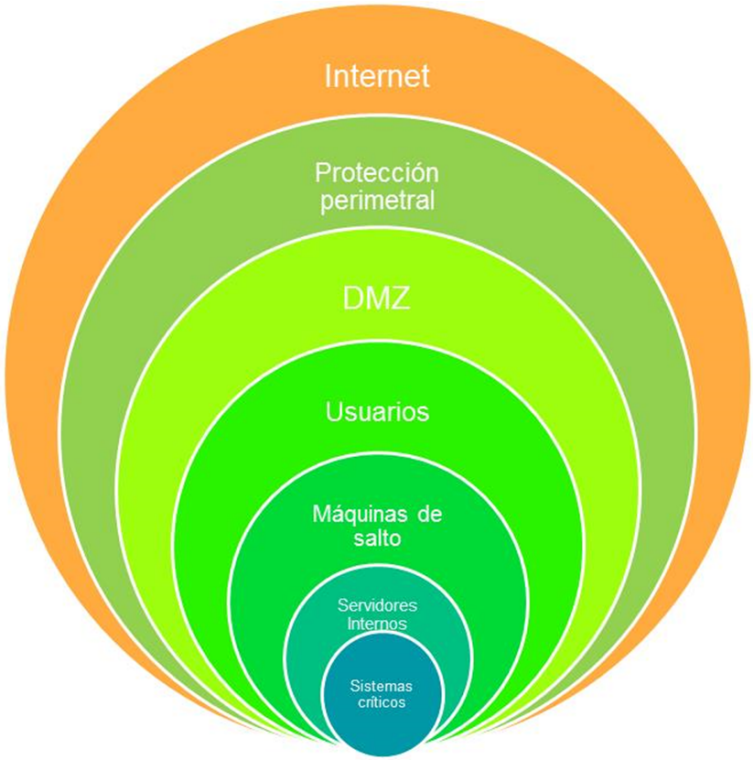
- Proxy: este dispositivo tiene la funcionalidad de filtrar todo el tráfico de entrada y salida. Los accesos al proxy deben ser autorizados por el firewall y todos los paquetes que viene de la red exterior e interior deben debe ser autorizados por el proxy. Los ataques al proxy son mitigados por el firewall.
- Servicios Web. HTTP/S
- Servicios de transferencia de archivos. SFTP/FTPS, SSH
- Servicios de resolución de nombres DNS.
- Concentrador de VPN



Héctor Fernández (Dominio público)

Por lo tanto la arquitectura segura de una DMZ tendrá las siguiente capas:

- **Sistemas de protección perimetrales:** Firewalls, AntiDoS, ProxyInverso, IPS, IDS, WAF … Asegurándose de que no es posible conectarse a un servicio de la DMZ si pasar por los dispositivos de seguridad que lo protegen.
- **Servicios propios de la DMZ.**
- **Servicios de protección de la red interna** a través de Firewalls internos. Estos firewalls deberían ser de diferente fabrican al firewall perimetral, lo que permite la **biodiversidad**. Así en caso de sufrir un ataque por vulneración de un fallo de seguridad en el firewall externo, no se pueda utilizar el mismo vector de ataque para promocionar a la red interna.



Héctor Fernández Bardal (Dominio público)

7.- Seguridad en entornos Cloud. Soluciones CASB.

Caso práctico

Los costes de mantenimiento de los servicios web de la compañía en los servidores del CPD se han disparado por la subida de la luz, servicios de vigilancia,... Hemos realizado una investigación y muchos desarrolladores de servicios web, prestan servicios en la nube con modelos SaaS, PaaS,...Por lo que hemos decidido que los servicios que actualmente prestamos sean migrados a la nube. El proveedor tiene tener en cuenta los requisitos de seguridad para este servicio.

FRANCISCO JAVIER RUIZ (Dominio público)

Indica 4 medidas de seguridad que serían responsabilidad del proveedor del servicio.

Control del cloud

Control de acceso al cloud para usuarios administradores

Realización de copias de seguridad

Monitorización de eventos del servicio

Gestión de usuarios

Autenticación. Valoración de implantación de doble factor de autenticación.

Gestión de contraseñas

.....

Seguridad en entornos Cloud. Soluciones CASB

Ante la difusión del perímetro de seguridad de las compañías por la migración de muchos de sus servicios a la nube, es necesario establecer mecanismo de seguridad y de control de los usuarios durante la utilización de estos servicios.

El objetivo es poder configurar de manera segura estos servicios (SaaS, PaaS, IaaS) y tener una vigilancia controlada de los mismo y desde los dispositivos desde los que se accede.

El acceso a los servicios se puede controlar desde qué dispositivos se realiza, si desde dispositivos de la compañía (COBO), dispositivos externos personales/corporaratios (COPE), dispositivos personales (BYOD),..pero siempre controlados a través de un Mobile Device Management (MDM). Aunque muchas vecen se implementen sistemas intermedios virtuales, que pueden formar parte de los servicios en nube, para proteger el control de la configuración de los dispositivos desde los que se conectan al sistema a través de dispositivos virtuales (VDI/VGI).

Las herramientas CASB (Cloud Access Security Broker) tiene como objetivo controlar y gestionar el uso de los servicios alojados en la nube.

El objetivo de estos productos es regular el uso los SaaS, PaaS, de la organización. La gestión de estos productos incluye:

- Monitorización de seguridad. Sobretodo en el punto de intercambio entre el sistema y el servicio alojado en la nube.
- Prevenir la fuga de información.
- Gestión de usuarios y permisos de los mismos
- Gestión de incidentes.
- Copias de seguridad
- Mecanismos de recuperación de desastres
- Cumplir con la RGPD
- Integración con herramientas corporativas: AD, SIEM, DNS, Correo, Proxy, firewall, …

Cloudfare (Dominio público)

Los proveedores de estos servicios deben proteger:

- Control de las comunicaciones
- Definición de la gestión. Especial atención a la administración del servicio con cuentas privilegiadas, definiendo el acceso para usuarios privilegiados.
- Control de acceso
- Datos de configuración
- Control de la auditoría
- Actualizaciones de seguridad relativas a los componentes del servicio
- Información almacenada

Debido a que los servicios en la nube pueden estar deslocalizados a nivel internacional, hay que tener en cuenta la leyes que se aplican en función de dónde se encuentre físicamente alojado el servicio, por si pudiera tener una incompatibilidad con la reglas internas de la compañía.

Aunque la responsabilidad de muchas acciones de seguridad recaen en el proveedor, la gobernanza de la seguridad debe recaer sobre el cliente del servicio que debe establecer los requisitos de seguridad. La parte de los servicios corporativos alojados en la nube deber poder integrarse e interconectarse de manera segura con la partes que residen en sus instalaciones (on-premise).

Es necesario comprobar la fiabilidad del proveedor del servicio desde el punto de vista de la seguridad, con la aportación de certificados de auditorías de seguridad, certificados de seguridad de entidades reconocidas como SOC 2, PCI DSS,...También es de utilidad saber algunos de los aspectos relativos al plan director de seguridad del proovedor para saber cómo gestionan un incidente cuando se ven afectados sus clientes.

Mitre ya ha definido una matriz de TTP específica para los servicios en nube. Dentro del apartado de las medidas de protección ("mitigations"), se puede ver las medidas que se definen para cada una de las técnicas.

Referencia útil sobre la configuración segura herramientas CASB del CCN.