Que es

Debe entenderse del perímetro de una red como el conjunto de sistemas que ofrecen servicios a la red externa (generalmente internet)

Al estar abiertos hacia el exterior, ofrece al atacante la exposición de vulnerabilidades que podrían ser explotadas

En informática, la seguridad perimetral es un metodo de defensa de las redes informáticas, que consiste instalar equipos de comunicaciones en los que se establece las políticas de seguridad necesarias para su optimo funcionamiento; estos equipos se los coloca entre la red externa y la red interna, permitiendo o denegando el acceso a los usuarios internos y externos a los diferentes servicios de la red…

Red sin red perimetral

Tendría las siguientes características negativas:

- Es una red plana, sin ninguna segmentación => una vez comprometido un nodo, se tiene acceso a toda la red.
- Se publican al exterior los servicios internos, sin intermediarios => la protección del nodo que exporta los servicios es la específica del nodo sin que posibles dispositivos intermediarios puedan añadir nuevas capas de defensa en profundidad (por ejemplo, un cortafuegos).
- No se activan los sistemas de monitorización de la red.
- No se establecen políticas de filtrado de tráfico, tanto de entrada como de salida
- No se verifica ni el malware ni el correo spam => responsabilidad reside en el usuario final

Funciones de la red perimetral

1. Rechazo de las conexiones desde clientes externos a servicios esencialmente sensibles, o que solo deben ser accedidos desde la red interna o a través de un intermediario de seguridad
2. Discrimina los diferentes tipos de tráfico, distinguiendo el tráfico que proviene de la LAN del que proviene de la red externa; estableciendo diferentes políticas para cada trafico
3. Selecciona el trafico procedente o dirigido a un determinado nodo de la red, por lo que también impide trafico que no provenga de donde deba provenir.
4. Proporciona un punto de conexión único con el exterior, el cual es controlable
5. Oculta servicios vulnerables para que no sean visibles desde la red externa
6. Oculta información sobre las características de la red interna como nombre de sistemas, topología de red, cuentas de usuario, etc.

Conceptos

Termino	Definición
Perímetro	Es la frontera fortificada de la red. La defensa del perímetro requiere la presencia de algunos elementos de fortificación como encaminadores, cortafuegos, IDS, VPN, DMZ (redes desmilitarizadas) y subredes controladas
Bastión	Es un servidor expuesto, que publica algún servicio a la red lo que le cataloga como de alto riesgo, pero que esta bien fortificado para resistir posibles ataques
Handering o fortificación	Es el conjunto ordenado y organizado de procedimientos por el que convertimos un servidor en un bastión suficientemente fortificado
Router de frontera	Es el Router más externo de la red, que esta en contacto directo con internet, debe filtrarse el trafico y ser capaz de soportar ataques
Cortafuegos	Dispositivo en el que se configuran reglas de filtrado que especifican que el trafico se aceptara y cual se denegara. Se ubica entre dos o más redes generando un único punto de análisis y operación. Frecuentemente, los routers de frontera tienen añadida una funcionalidad de cortafuegos.
Sistema de detección de intrusiones IDS	Es un sistema que despliega un conjunto de sensores estratégicamente situados en la red interna con objeto de detectar posibles ataques
Red privada virtual VPN	Es una tecnología que permite establecer sesiones de red protegidas a través de canales públicos o no seguros. Se contruyen mediante dispositivos ubicados en el perímetro que establecen sesiones cifradas entre distintas sedes por la red insegura. Típicamente internet
Red desmilitarizada DMZ	Es una porción de la red que aloja servicios que se hacen accesibles al exterior. En ellas se suelen situar los servidores que se publican en internet. Los nodos que componen un DMZ se sitúan delante del cortafuegos corporativo, de modo que están desprotegidos. Sin embargo, pueden contruirse arquitecturas de DMZ que proveen de alguna protección a los nodos que aloja para llegar a un consenso entre los servicios publicados y el riesgo de exposición.
Redes controladas, apantalladas o fuertemente protegidas	Son redes (o subredes) que se situan detrás del cortafuegos corporativo, a diferencia de las DMZ que se situan delante.

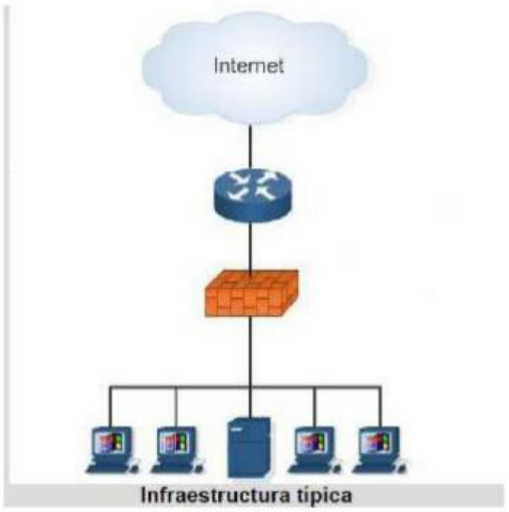
Defensa en profundidad en la red perimetral

Recordemos el concepto de seguridad en profundidad…

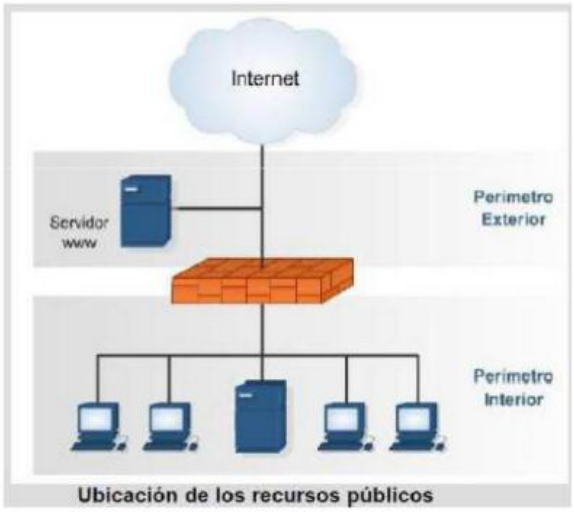
> " la defensa en profundidad es una estrategia consistente en introducir multiples capas de seguridad que permitan reducir la probabilidad de compromiso en caso de que una de las capas falle y en el peor de los casos minimizar el impacto."

Objetivos de la seguridad perimetral

- Seguridad de la red: asegurar un ambiente establece en términos de red y Pc´s. ya que la mayoría de las amenazas provienen de como interactúan los usuarios con internet
- Navegación segura: destinadas a proteger al usuario durante la navegación en internet, controlando los sitios a los que accede mediante listas negras/blancas (no permitidas/permitidas), sistemas de reputación y otros mecanismos.
- Internet libre: rentabilizar el recurso internet para el trabajo, dejándolo libre y con toda su capacidad y velocidad contratada.
- Detección de virus: pronta detección de equipos con brotes de virus y del uso de programas maliciosos
- Conexiones remotas: simplificar la conectividad segura hacia la red de oficinas y promoción de la movilidad vía VPN

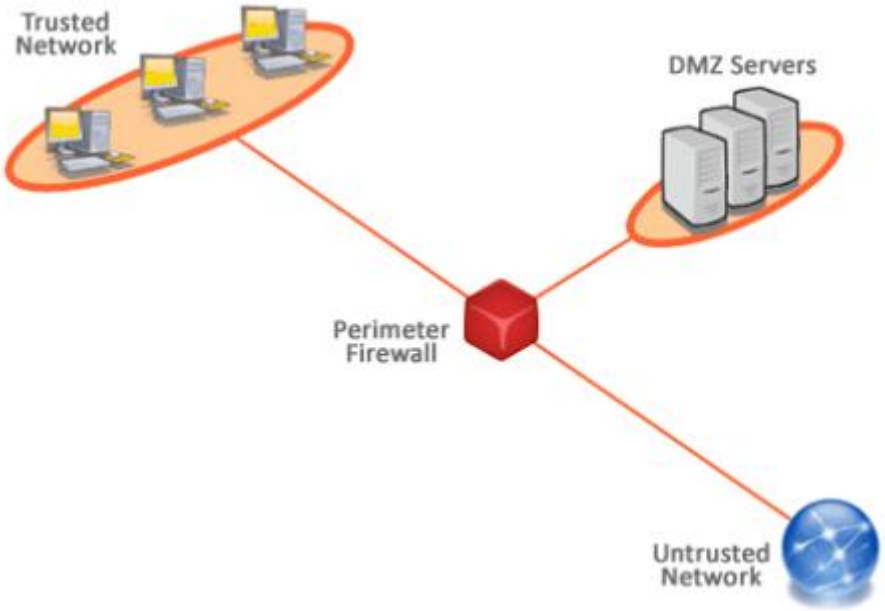


Infraestructura típica



Ubicación de los recursos públicos

Arquitectura débil



Una subred protegida es débil es aquella, que establece la protección de la red interna empleando una zona DMZ por detrás de un firewall de perímetro

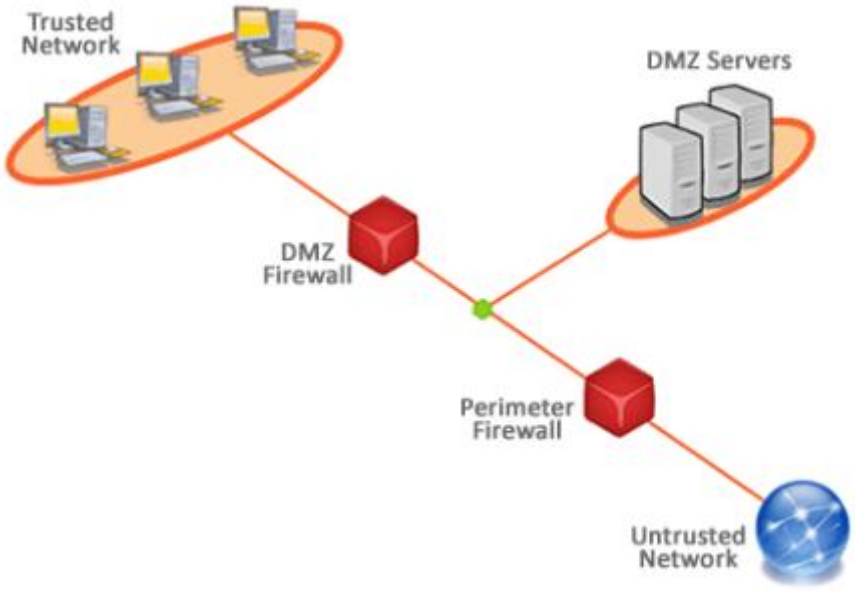
En esta disposición, el equipo que actúa como firewall debe tener al menos tres interfaces para poder conectar con la DMZ, el exterior y la red interna.

Un fallo en el cortafuegos puede desproteger a la red interna

La subred protegida aloja servicios que se pretenda sean accesibles desde internet, pero eso no implica que no deba ser segura. Los equipos que forman esta subred se denominan bastión, es un elemento mas adelantado que la red interna y esta mas en contacto con el peligro.

Los bastiones son equipos donde se han fortalecido tanto los S.O. como las aplicaciones para que sean lo mas seguro posibles. Estos equipos son el objetivo de todos los ataques puesto que son los que más contacto tienen con la red exterior

Arquitectura fuerte



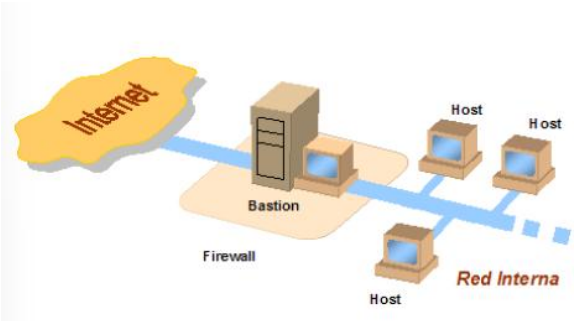
La subred protegida fuerte establece la protección de la red interna con una zona DMZ situada entre dos firewalls

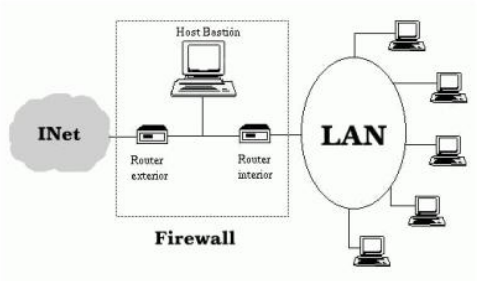
En esta disposición el cortafuegos externo (de acceso) bloquea y controla el trafico no deseado desde la red externa a DMZ. El cortafuegos interno (de contención) bloquea y controla el trafico no deseado de DMZ a red interna

Un fallo en el cortafuegos externo desprotege solamente la DMZ

Host bastión

Un host bastión es una aplicación que se localiza en un servidor con el fin de ofrecer seguridad a la red interna, por lo que ha sido especialmente configurado para la recepción de ataques, generalmente provee un solo servicio (como por ejemplo un servidor proxy).





Un host bastión es un equipo que esta completamente expuesto a los ataques. El sistema esta en el lado publico de la zona desmilitarizada (DMZ), protegidos por un firewall o un Router de filtrado (también considerados los hosts de bastión).

Debido a su exposición, se debe diseñar una configuración de seguridad muy solida en los mismos para reducir al mínimo las posibilidades de penetración.

Otros tipos de hosts bastión son la web, correo, DNS y servidores FTP. Cada host bastión desempeña una función específica, todos los servicios innecesarios, protocolos, programas y puertos de red están deshabilitados o eliminados.

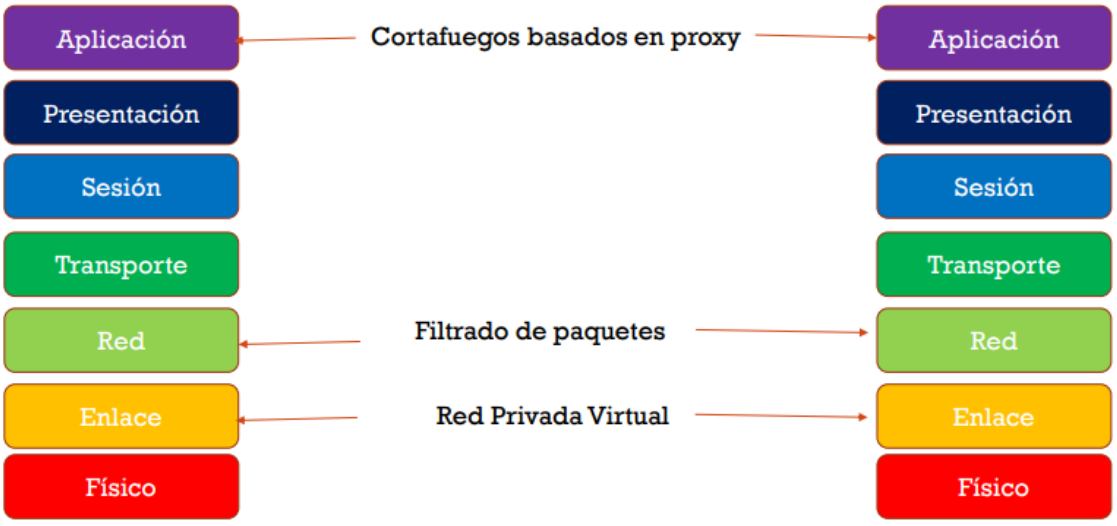
Algunos administradores de red también utilizan como chivos expiatorios estos sistemas son expuestos deliberamente a los hackers potenciales para analizar y realizar el seguimiento de los intentos de ataque. Esto se llama tarro de miel o honeypot

Cortafuegos

En la seguridad perimetral es común encontrar un Router que actúe como firewall o cortafuegos. Los conceptos de cortafuegos y Router son totalmente diferentes, pero ocurre que muchos routers incorporan un cortafuegos en su software y por ello no es necesario incorporar un cortafuegos adicional.

La palabra que mas se repite entre las opciones de firewall es “filtrar”. El cortafuegos más simple es un filtrado de paquetes, en el que los routers miran la dirección origen, la dirección destino y el puerto destino. Estos filtros aceptan o deniegan los paquetes permitiendo al Router eliminar o dejar pasar el paquete

Un ejemplo de este tipo de filtrado son las listas de control de acceso (ACL), son listados de restricciones o permisos que se aplican a un Router para controlar el trafico de entrada y de salida del mismo. Para crear una lista de control de acceso se emplea el comando Access-list.



Filtrado de paquetes estático

Es el modo de filtrado más básico de un cortafuegos y consiste en el rechazo o aceptación de paquetes en función de alguno o veros vampos que componen un paquete IP. Por ejemplo:

- La dirección IP de origen o de destino del paquete
- El nº de puerto a que se dirige el paquete o del que procede (recuerda que el nº de puerto identifica un servicio)
- Los campos de la cabecera del protocolo de capa superior (TCP, UDP).
- Los flags de cabecera (SYN, ACK, etc.)

Las decisiones de filtrado se toman en cada paquete que llega al Router siguiendo las reglas que se asocian a una lista de control de acceso (ACL)

El filtrado se puede realizar a la entrada, a la salida o a la entrada y salida del paquete.

Hay dos modos fundamentales de configuración de reglas en los cortafuegos:

- Política restrictiva o de lista blanca: se deniega por defecto todo el tráfico, salvo el que se acepta explícitamente. Por tanto, las ACL que se definen básicamente son de aceptación, aunque la última regla definida es la de denegación de todo lo que no haya sido explícitamente aceptado anteriormente.
- Política permisiva o de lista negra: se acepta todo el trafico salvo el que se deniegue explícitamente. En este caso las ACL son mayoritariamente de denegación, aunque la ultima regla es de aceptación de todo el trafico que no fue denegado anteriormente.

REGLA	ACCIÓN	IP ORIGEN	IP DESTINO	PROTOCOLO	PUERTO ORIGEN	PUERTO DESTINO
1	Aceptar	172.16.0.0/16	192.168.0.4	TCP	cualquiera	25
2	Aceptar	cualquiera	192.168.0.8	TCP	cualquiera	80
3	Aceptar	172.16.0.0/16	192.168.0.2	TCP	cualquiera	80
4	Denegar	cualquiera	cualquiera	cualquiera	cualquiera	cualquiera

Problemas

Las direcciones IP con fáciles de enmascarar, por lo que el cortafuegos puede ser engañado mediante la suplantación de direcciones IP contenidas en los campos de un paquete IP

Los servicios y aplicaciones pueden utilizar puertos no estandarizados y, por tanto, que no identifiquen inmediatamente al servicio que proveen

Algunos servicios tienen comportamientos especiales que no se pueden gestionar con un simple filtrado de paquetes IP, como por ejemplo el caso de FTP

Una vez que se llega al Router o cortafuego, la red interna está expuesta

No soporta autenticación de usuarios robustos, lo que debe ser confiado a protocolos de nivel superior.

Filtrado dinámico de paquetes

Este tipo de filtrado de reglas se crean y destruyen dinámicamente, según van apareciendo o desapareciendo las conexiones

Con este método, los paquetes de salida permitidos crean automáticamente reglas de filtrado para aceptar el trafico de respuesta al de salida.

No se permitirá la entrada a cualquier paquete desde la red externa, solo aquellos paquetes que contengan una respuesta a una conexión realizada previamente desde la red interna.

Ventaja

Las aplicaciones dentro de la red interna que esperan respuestas desde la red externa siempre la obtendrán puesto que el cortafuegos se encarga de ellos

Desventajas

La operación de filtrado se basa exclusivamente en la información de cabecera del paquete IP por lo que, por ejemplo, no se pueden filtrar por direcciones IP, por puertos u otros campos que no aparecen en la cabecera.

Generalmente, los dispositivos reales suelen combinar filtrado estático y filtrado dinámico

Introducción

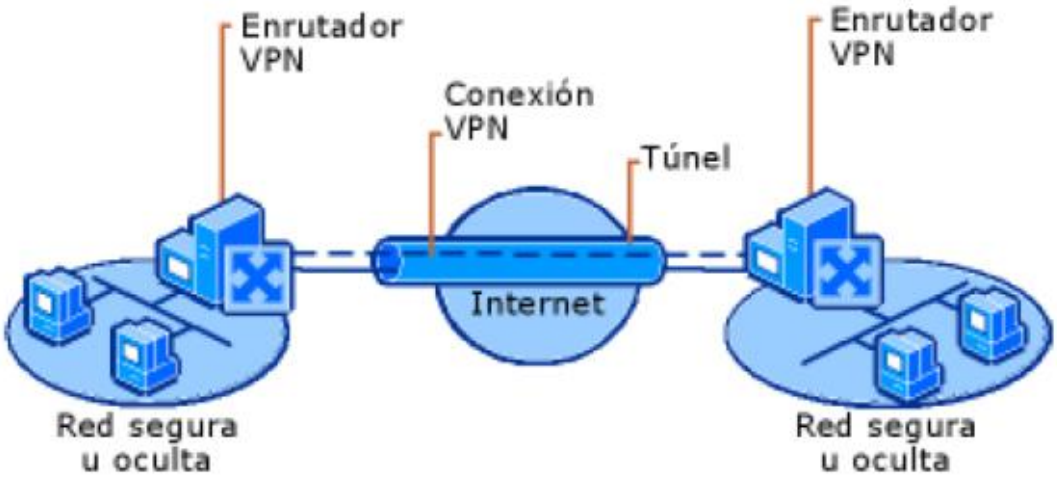
Otra de las grandes arquitecturas de seguridad, imprescindibles en cualquier organización de tamaño medio o grande, son las denominadas redes privadas virtuales (VPN en inglés, virtual private network)

En pocas palabras, una VPN establece un enlace de comunicaciones segura entre dos nodos, utilizando para ello un método de encapsulamiento del tráfico que utiliza criptografía simétrica. A este enlace se le llama normalmente tune cifrado VPN, o simplemente túnel VPN

Definición

Una red privada virtual (VPN) es una red creada artificialmente. Se dice que es virtual por que conecta dos redes “físicas” (redes de área local) a través de una conexión poco fiable (internet) y privada porque solo los equipos que pertenecen a una red de área local de uno de los lados de la VPN pueden “ver” los datos

El sistema VPN brinda una conexión segura a un bajo coste, sin embargo, no garantiza una calidad de servicio comparable con una línea dedicada, ya que la red física es publica y por lo tanto no esta garantizada.



Usos

Muchas veces, las empresas necesitan comunicarse por internet con filiales, clientes o incluso con el personal que puede estar alejado geográficamente. Sin embargo, los datos transmitidos a través de internet son mucho mas vulnerables que cuando viajan por una red interna de la organización, ya que la ruta tomada no esta definida por anticipado, es posible que, a lo largo de la línea, un usuario entrometido, escuche la red o incluso secuestre la señal.

La primera solución para satisfacer esta necesidad de comunicación segura implica conectar redes remotas.

Sin embargo, como la mayoría de las compañías no pueden conectar dos redes de área local remotas con una línea dedicada, a veces es necesario usar internet como medio de transmisión con un protocolo de túnel, que significa que los datos se encapsulan antes de ser enviados de manera cifrada

Funcionamiento

Una red privada virtual se basa en un protocolo denominado protocolo de túnel, es decir, un protocolo que cifra los datos que se transmiten desde un lado de la VPN hacia el otro

La palabra “túnel” se usa para simbolizar el hecho que los datos estén cifrados desde el momento que entran a la VPN hasta que salen de ella y, por lo tanto, son incomprensibles para cualquiera que no se encuentre en uno de los extremos de la VPN

En una VPN de dos equipos, el cliente de VPN es la parte que cifra y descifra los datos del lado del usuario y el servidor VPN (comúnmente llamado servidor de acceso remoto) es el elemento que descifra los datos del lado de la organización

De esta manera, cuando un usuario necesita acceder a la red privada virtual, su solicitud se transmite sin cifrar al sistema de pasarela, que se conecta con la red remota, mediante la infraestructura de red publica como intermediaria; luego transmite la solicitud de manera cifrada. El equipo remoto le proporciona los datos al servidor VPN en su red y este envía la respuesta cifrada. Cuando el cliente de VPN del usuario recibe los datos, los descifra y finalmente los envía al usuario

Ventajas

Reducen los costes de explotación al utilizar líneas publicas en vez de alquilarlas para realizar conexiones punto a punto

Incrementan la seguridad (confidencialidad, integridad, autenticación y no repudio)

No son difíciles de desplegar

Desventajas

Se necesita una mayor potencia de calculo ya que la operación de cifrado consume recursos

Requieren tener internet disponible, ya que es la red básica de transporte sobre la que establece el túnel

Tienen algunos problemas de implementación como, por ejemplo, la convivencia con el protocolo NAT

Necesita control y supervisión adicionales, lo que exige la atención del administrador

Requiere la instalación de un IDS para la detección de fallos en la seguridad

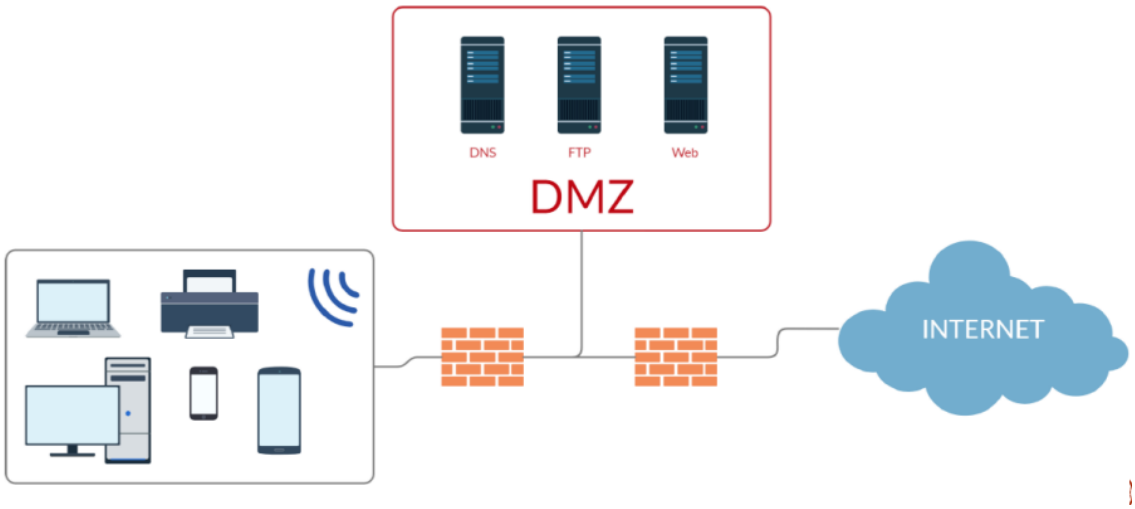
Que es una red DMZ

una DMZ o zona desmilitarizada es una red local que se ubica entre la red interna de una organización y una red externa, generalmente internet.

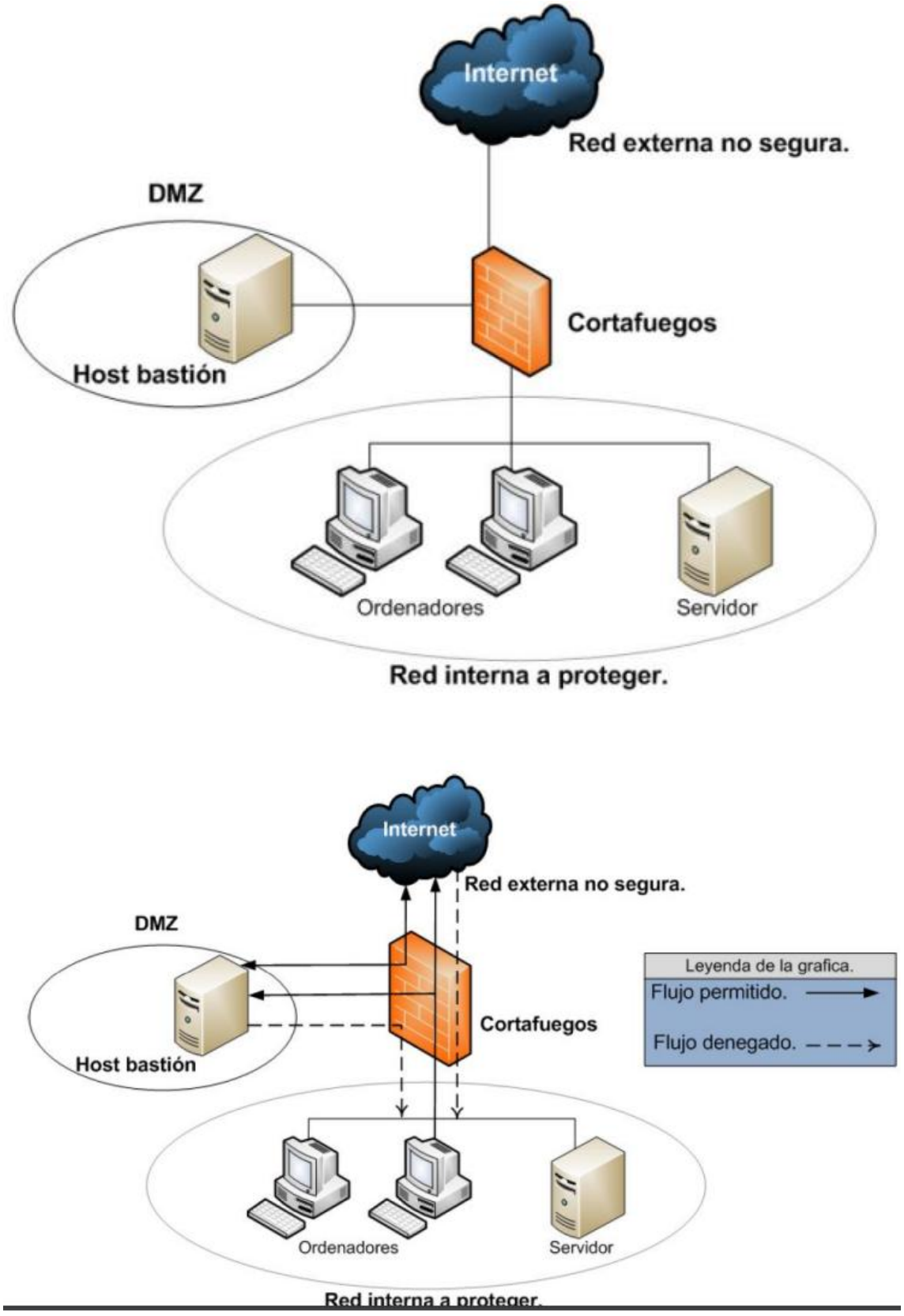
El objetivo de una DMZ es que las conexiones desde la red interna y la red externa a la DMZ estén permitidas, mientras que las conexiones desde la DMZ solo se permitan a la red externa, es decir: los equipos locales (host) en la DMZ no pueden conectar con la red interna.

Para cualquiera de la red externa que quiera conectarse ilegalmente a la red interna, la zona desmilitarizada se convierte en un callejón sin salida

La DMZ se usa habitualmente para ubicar servidores que es necesario que sean accedidos desde fuera, como servidores de email, web y DNS



Esquema básico red con DMZ: flujo del trafico



Importancia del diseño para redes DMZ

El concepto de las redes DMZ ha surgido por la necesidad de crear una mayor y efectiva separación entre los equipos que ofrecen servicios hacia el exterior (host bastión) y los equipos que contienen información confidencial que no debería ser expuesta hacia el exterior

La red DMZ es un componente crítico y a la hora de hacer el diseño de seguridad de una red informática actual, por lo que debe ser flexible para lograr altos niveles de seguridad

Se deben tener en cuenta las vulnerabilidades de los protocolos de comunicación existentes, que se pretenden utilizar dentro de la red.

Es de vital importancia la correcta ubicación de los equipos y servidores, en función de los servicios que prestaran del nivel de protección que estos requieren

Protocolos de comunicación dentro DMZ

Una de las ventajas de diseñar las redes DMZ con cortafuegos, es la posibilidad de controlar el flujo del trafico en función de los puertos de origen y destino o permitiendo/deshabilitando protocolos de comunicación

Algunos de esos protocolos pueden ser: FTP, TELNET, HTTP, SNMP, SSH, DNS…

IPSec y L2TP son protocolos de seguridad para proteger los datos

Características de los IDS

Debe funcionar continuamente sin supervisión humana. El sistema debe ser lo suficientemente fiable para poder ser ejecutado en background dentro del equipo que está siendo observado

Debe ser tolerable a fallos en el sentido de que debe ser capaz de sobrevivir a una caída del sistema.

Debe ser persistente a perturbaciones. El sistema puede monitorizarse a si mismo para asegurarse de que no ha sido perturbado.

Debe observar desviaciones sobre el comportamiento estándar.

Debe ser fácilmente adaptable al sistema ya instalado. Cada sistema tiene un patrón de funcionamiento diferente y el mecanismo de defensa debe adaptarse de manera sencilla a esos patrones

Debe hacer frente a los cambios de comportamiento del sistema según se añaden nuevas aplicaciones al mismo

Debe ser difícil de “engañar”.

Fortalezas de los IDS

Suministra información muy interesante sobre el trafico malicioso de la red

Genera poder de reacción para prevenir el daño

Ayuda a identificar de donde provienen los ataques que se sufren

Funciona como “disuasor de intrusos”

Es una parte de la infraestructura para la estrategia global de defensa.

La posibilidad de detectar intrusiones desconocidas e imprevistas. Pueden incluso contribuir (parcialmente) al descubrimiento automático de esos nuevos ataques

Son menos dependientes de los mecanismos específicos de cada sistema operativo

Menor coste de implementación y mantenimiento al ubicarse en puntos estratégicos de la red

Dificulta el trabajo del intruso de eliminar sus huellas

Debilidades y limitaciones de los IDS

Se producen falsas alarmas

No es sustituto para un buen firewall, una auditoria de seguridad regular y una fuerte y estricta política de seguridad

La alta tasa de falsas alarmas dado que no es posible cubrir todo el ámbito del comportamiento de un sistema de información durante la fase de aprendizaje

El comportamiento puede cambiar con el tiempo, haciendo necesario un entrenamiento periódico del perfil, lo que da lugar a lo no disponibilidad del sistema o la generación de falsas alarmas adicionales

El sistema puede sufrir ataques durante la fase de aprendizaje, con lo que el perfil de comportamiento contendrá un comportamiento intrusivo el cual no será considerado anómalo