UT3. IMPLANTACIÓN DE SEGURIDAD PERIMETRAL

Módulo: Seguridad y Alta Disponibilidad

Curso 2023/2024. 2º ASIR

CONTENIDOS

- Introducción
- Arquitecturas
- Host bastion
- Cortafuegos
- Redes privadas virtuales VPN
- Zonas desmilitarizadas DMZ
- Sistemas de detección de intrusos IDS
- Honeypots

INTRODUCCIÓN

QUÉ ES

- Debe entenderse el 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 <u>seguridad perimetral</u> es un método de defensa de las redes informáticas, que consiste instalar equipos de comunicaciones en los que se establece las políticas de seguridad necesarias para su óptimo 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 especifica 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 fina

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 tráfico.
3. Selecciona el tráfico procedente o dirigido a un determinado nodo de la red, por lo que también impide tráfico 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, topolgía de red, cuentas de usuario, etc.

CONCEPTOS

Término	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 está bien fortificado para resistir posibles ataques
Hardening 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 está en contacto directo con Internet. Debe filtrarse el tráfico y ser capaz de soportar ataques
Cortafuegos	Dispositivo en el que se configuran las reglas de filtrado que especifican qué trafico se aceptará y cuá se denegará. Se ubica entre dos o más redes generando un único punto de análisis y operación. Frecuentemente, los routers de frontera tienen añadida funcionalidad de cortafuegos.

CONCEPTOS

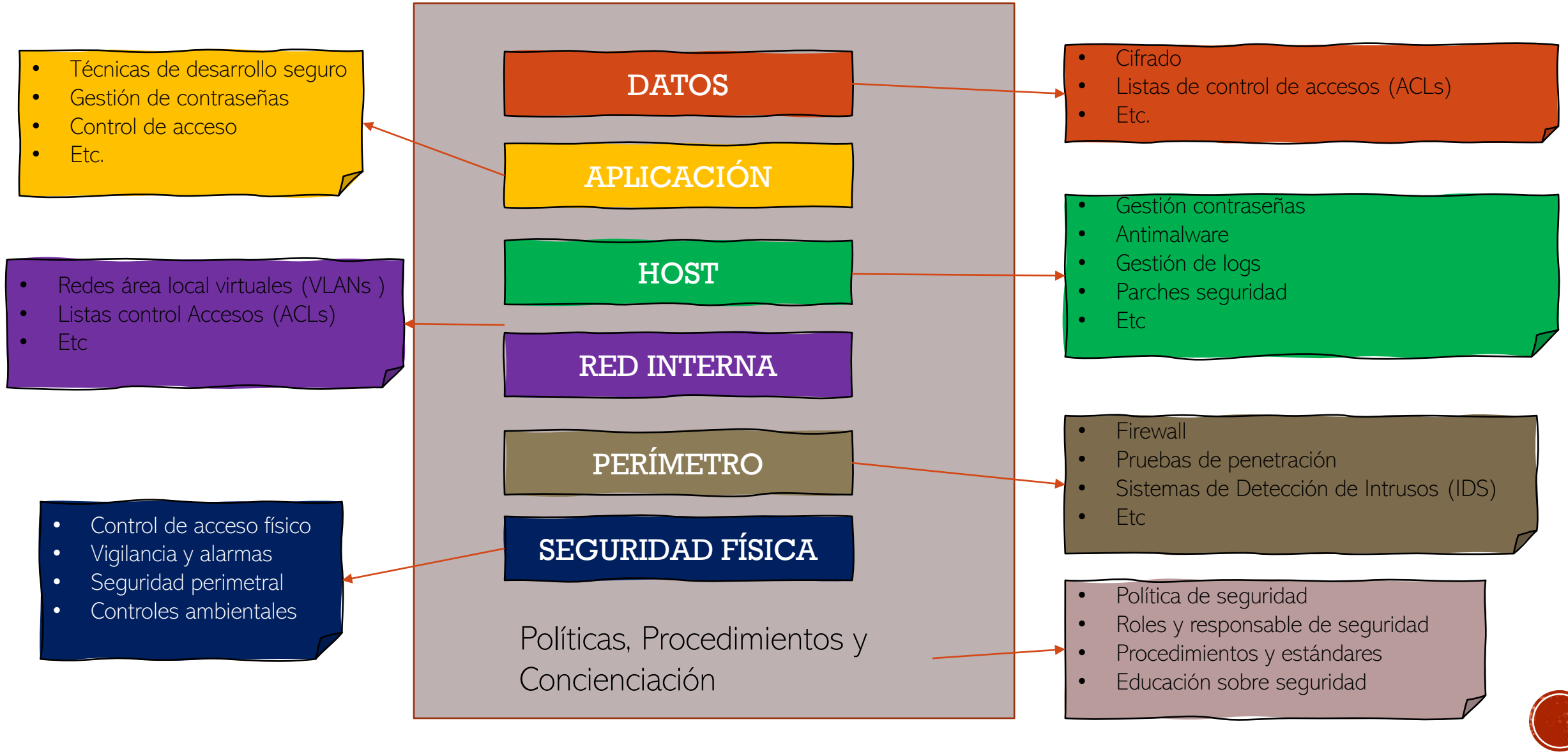
Término	Definición
Sistema de detección de intrusiones IDS	Es un sistema que despliega un conjunto de sensores estratégicamente situados en la red interna con objeto de detectar posibles ataques. Esta detección se realiza mediante el reconocimiento de ciertos patrones de información (firmas) o secuencias de acciones que son especificas de cada ataque.
Red privada virtual VPN	Es una tecnología que permite establecer sesiones de red protegidas a través de canales públicos o no seguros. Se construyen 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 construirse 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 sitúan detrás del cortafuegos corporativo, a diferencia de las DMZ que se sitúan 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 múltiples 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."

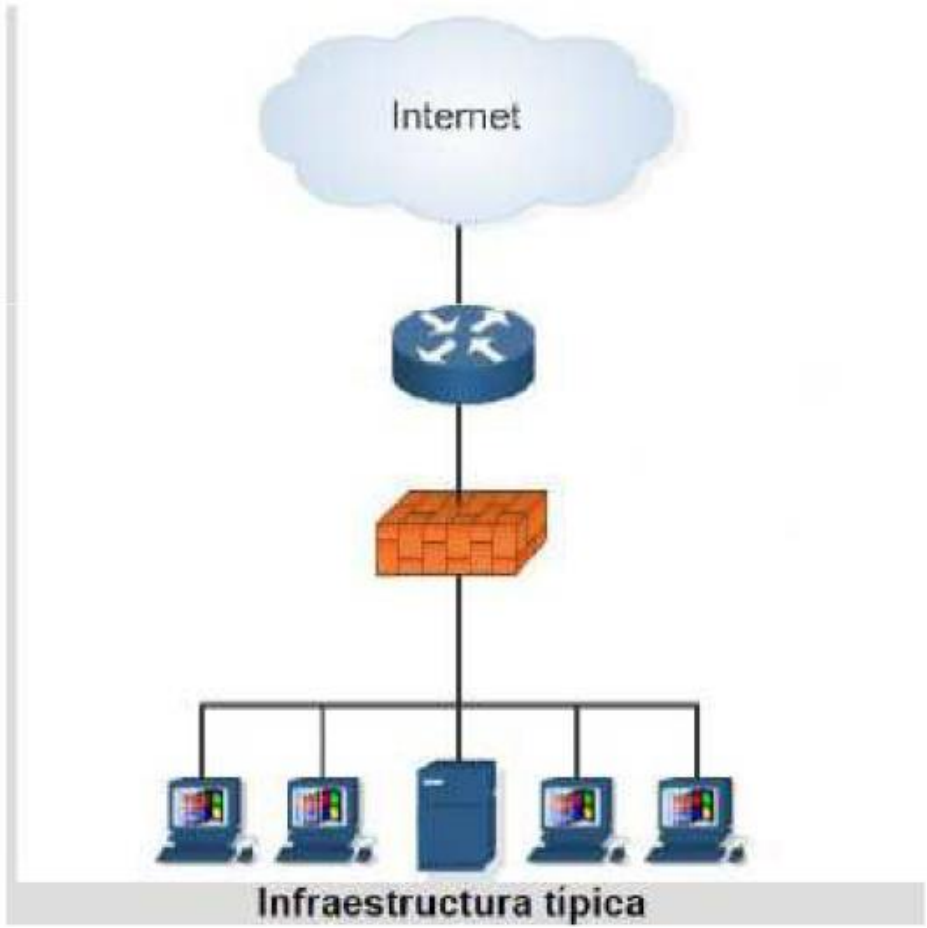
DEFENSA EN PROFUNDIDAD EN LA RED PERIMETRAL



OBJETIVOS DE LA SEGURIDAD PERIMETRAL

- **Seguridad de la Red:** Asegurar un ambiente estable en términos de red y Pc's. Ya que la mayoría de las amenazas provienen de cómo interactúan los usuarios con internet.
- **Navegación Segura:** Destinadas a proteger al usuario durante la navegación en Internet, controlando los sitios a los que se 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.

SEGURIDAD PERIMETRAL



Infraestructura típica

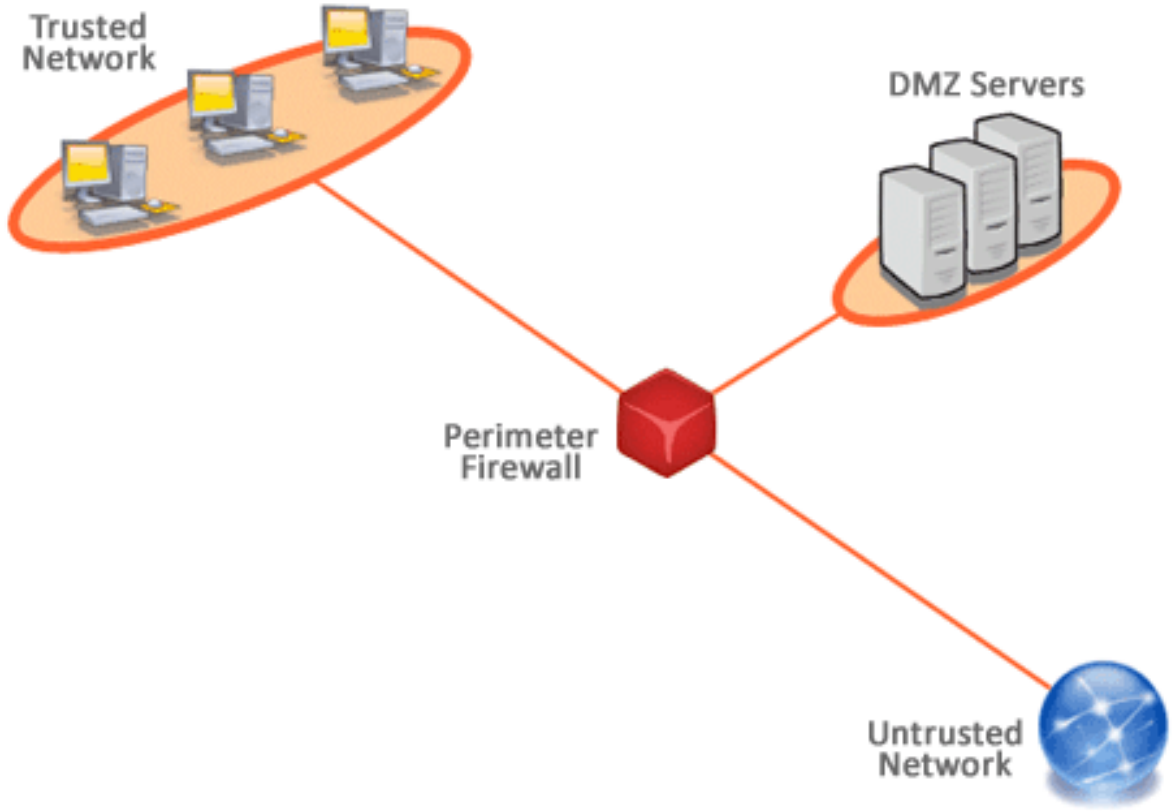
Ubicación de los recursos públicos

ARQUITECTURAS

ARQUITECTURA DÉBIL

- Una subred protegida 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.

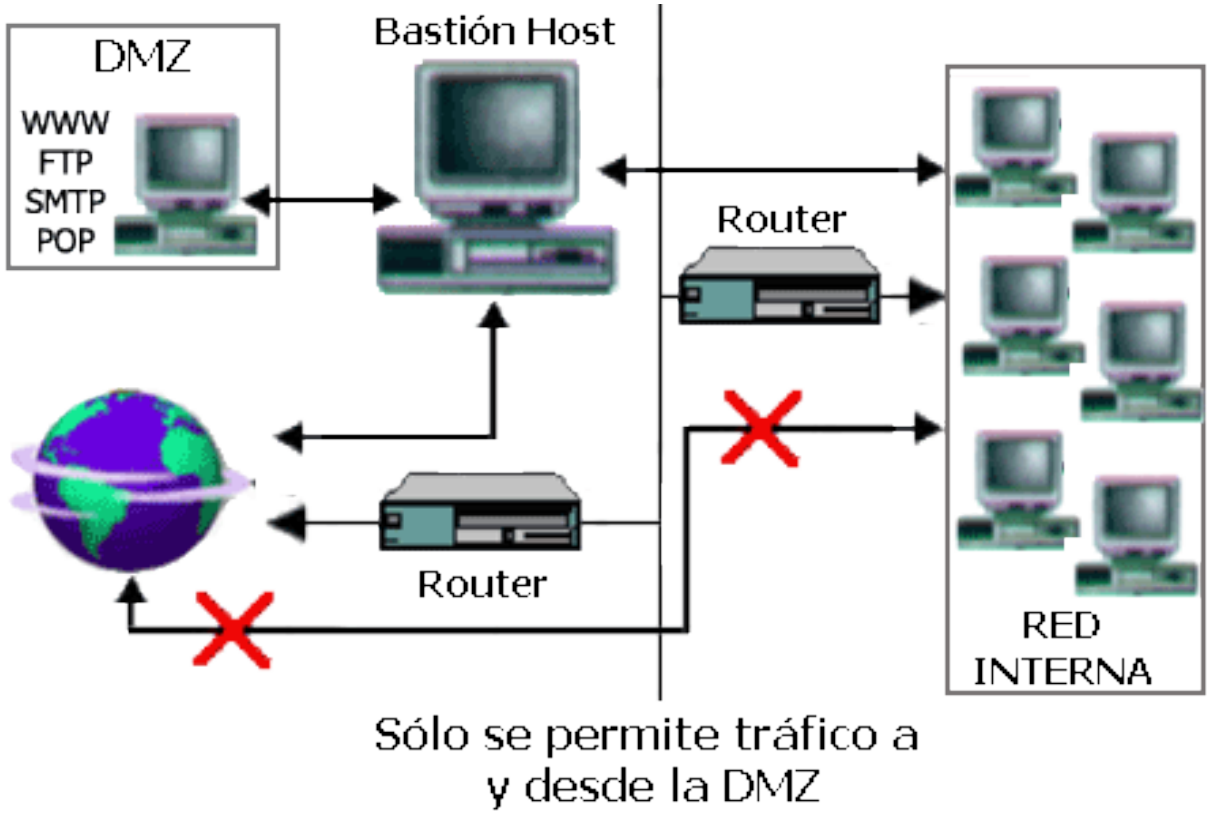
Un fallo en el cortafuegos puede desproteger a la red interna.



ARQUITECTURA DÉBIL

- 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 más adelantado que la red interna y está más en contacto con el peligro.

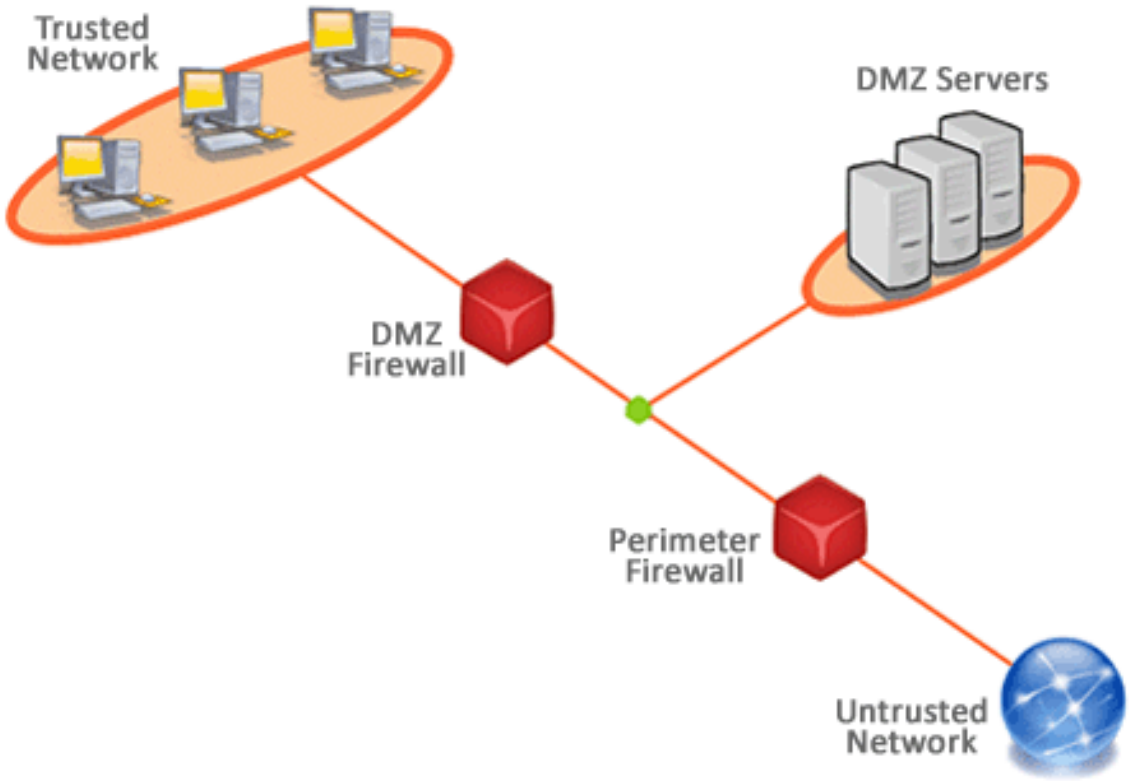
- Los bastiones son equipos donde se han fortalecido tanto los S.O. como las aplicaciones para que sean lo más seguro posibles. Estos equipos son el objetivo de todos los ataques puesto que son los que más contacto tienen con la red exterior.



ARQUITECTURA FUERTE

- La subred protegida fuerte establece la protección de la red interna con una zona DMZ situada entre dos firewall.
- En esta disposición el cortafuegos externo (de acceso) bloquea y controla el tráfico no deseado desde la red externa a DMZ. El cortafuegos interno (de contención) bloquea y controla el tráfico no deseado de DMZ a red interna.

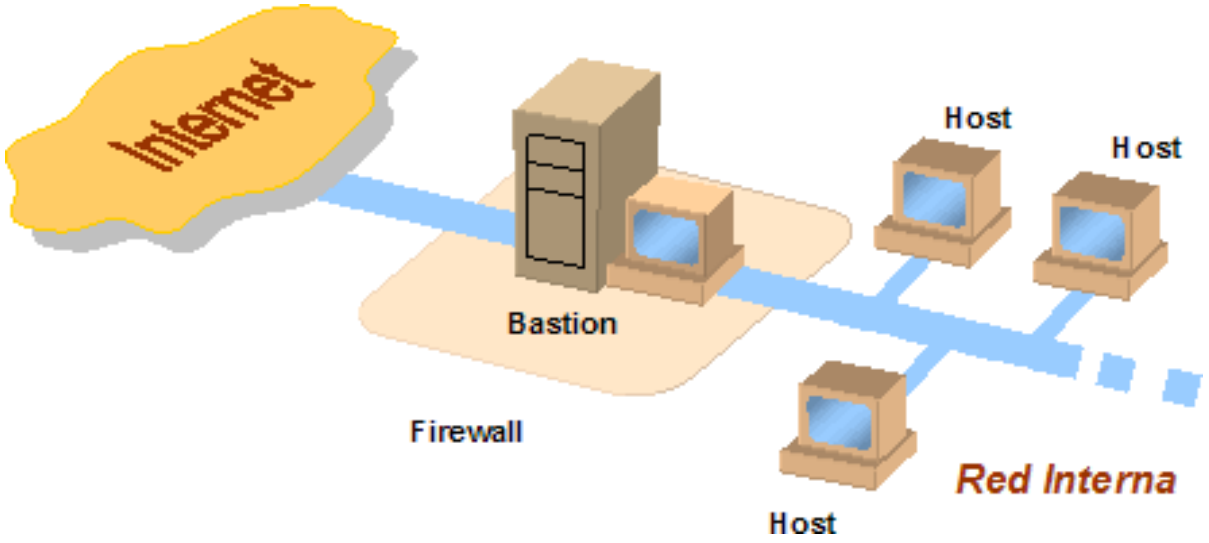
Un fallo en el cortafuegos externo desprotege solamente la DMZ.

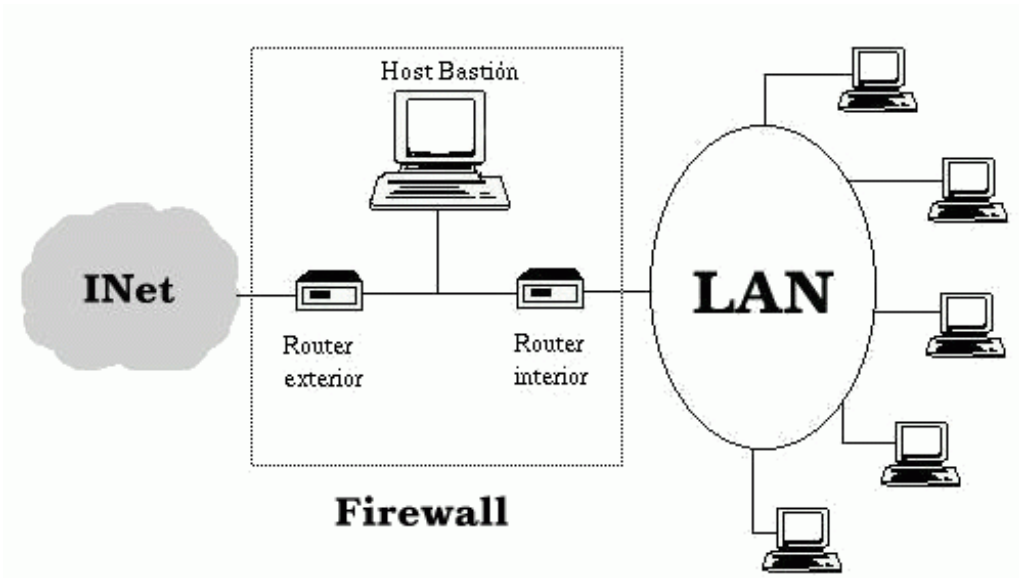


HOST BASTIÓN

DEFINICIÓN

- 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).





CARACTERÍSTICAS

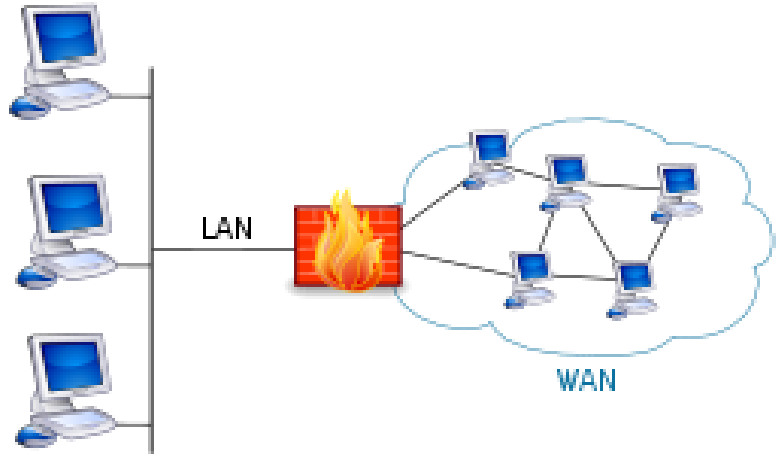
- Un host bastión es un equipo que **está totalmente expuesto a los ataques**. El sistema está en el lado público de la zona desmilitarizada (DMZ), protegidos por un firewall o un router de filtrado (también considerados los hosts de bastión).
- Debido a su exposición, se debe diseñar una configuración de seguridad muy sólida en los mismos para reducir al mínimo las posibilidades de penetración.
- Otros tipos de hosts de 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 que son expuestos deliberadamente a hackers potenciales para analizar y realizar el seguimiento de los intentos de ataque. Esto se llama tarro de miel o **honeypot**

CORTAFUEGOS

INTRODUCCIÓN

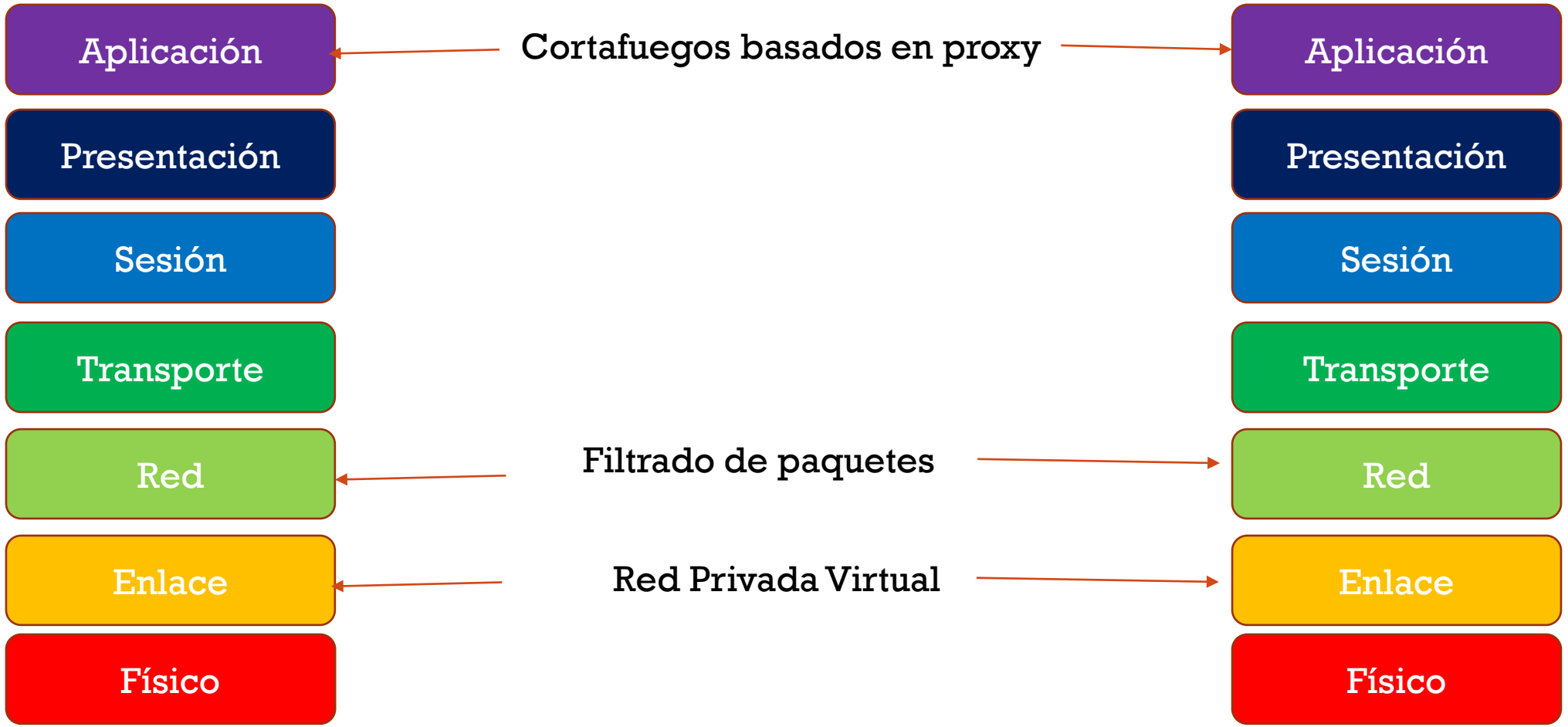
- En la seguridad perimetral es **común encontrar un router que actúe como firewall o cortafuegos**. Los conceptos de cortafuegos y router son totalmente diferentes, pero ocurre que muchos routers incorporan un cortafuegos en su software y por ello no es necesario incorporar un cortafuegos adicional.

- La palabra que más se repite entre las opciones del 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 tráfico de entrada y de salida del mismo. Para crear una lista de control de acceso se emplea el comando access-list.

INTRODUCCIÓN



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

FILTRADO DE PAQUETES ESTÁTICO

- 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 tráfico salvo el que se deniegue explícitamente. En este caso las ACL son mayoritariamente de denegación, aunque la última regla es de aceptación de todo el tráfico que no fue denegado anteriormente.

FILTRADO DE PAQUETES ESTÁTICO

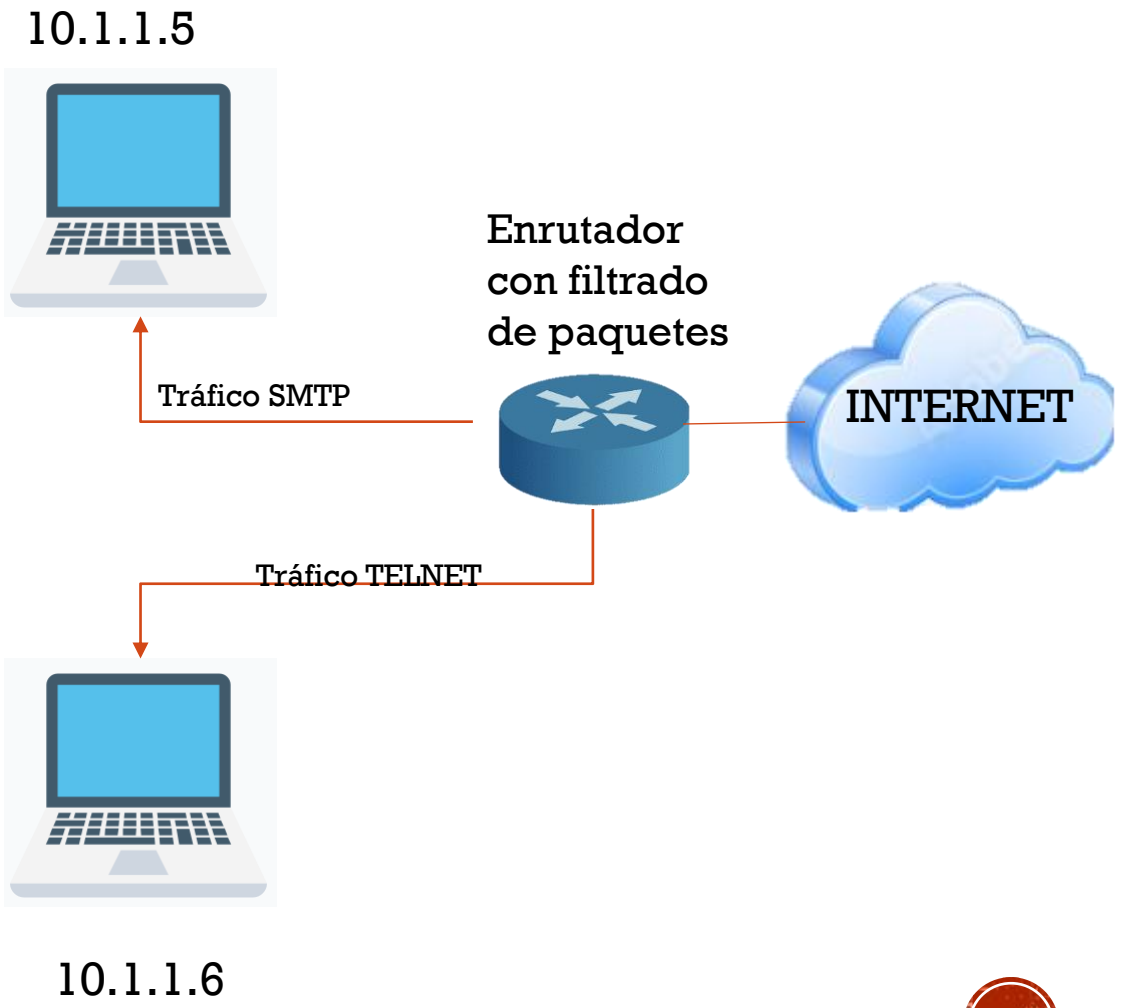
EJEMPLO POLÍTICA RESTRICTIVA

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

FILTRADO DE PAQUETES ESTÁTICO

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 tiene 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 tráfico 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.

FILTRADO DINÁMICO DE PAQUETES

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 puede 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

CORTAFUEGOS BASADOS EN PROXY

- Son los cortafuegos capaces de **operar en las capas superiores** de la arquitectura de red, por tanto son dependientes de la aplicación.
- Hay **dos tipos** de cortafuegos basados en proxy:
  - Pasarelas de nivel de aplicación
  - Pasarelas de nivel de circuito

CORTAFUEGOS BASADOS EN PROXY

PASARELAS DE NIVEL DE APLICACIÓN

El modo de operación de estas pasarelas es el siguiente:

1. El usuario solicita el servicio requerido a la pasarela identificada por una dirección IP y por un número de puerto de servicio, que representa la ubicación lógica del proxy que actuará como intermediario.
2. Opcionalmente, la pasarela solicita la identificación del sistema cliente con el que se pretende conectar.
3. El usuario responde a la petición de autenticación presentada por la pasarela por lo que autorizará o no a usarla como intermediario entre el cliente y el servidor remoto.
4. Si todo es correcto, la pasarela contacta con el sistema remoto y comienza un diálogo de intercambio de datos con él en representación del cliente. Es posible que el sistema final requiera de una autenticación para acceder al servicio. En este caso, la pasarela gestionará esta autenticación con la colaboración del usuario o utilizando la identidad con que el usuario se presentó a la pasarela.
5. En caso de que no disponga de un proxy adecuado para gestionar los paquetes de una determinada aplicación, estos son rechazados. Es decir, cada protocolo de aplicación requiere de una pasarela de aplicación especifica

CORTAFUEGOS BASADOS EN PROXY

VENTAJAS PASARELAS DE NIVEL DE APLICACIÓN

- Cada proxy se puede encargar de un determinado servicio, por tanto, hay control granular del tráfico, con configuraciones distintas para cada protocolo de nivel de aplicación
- Es posible la protección de antivirus y antimalware puesto que la acción de la pasarela puede proporcionar un valor añadido
- Se puede gestionar el control de accesos de cada servicio por separado
- Se pueden generar trazas e históricos de utilización de los servicios

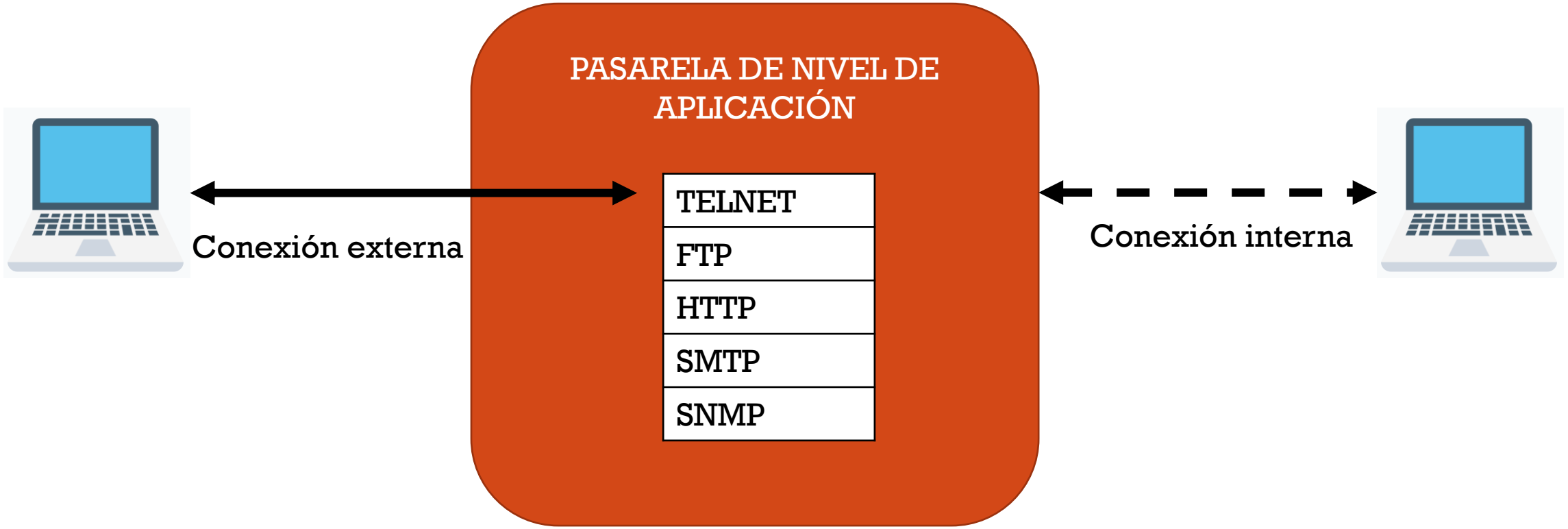
CORTAFUEGOS BASADOS EN PROXY

INCONVENIENTES PASARELAS DE NIVEL DE APLICACIÓN

- Se requiere que el cliente use aplicaciones específicamente diseñadas para ser utilizadas con estas pasarelas
- Exige la instalación de nuevos elementos de infraestructura en la red como son los servidores proxy para cada servicio.

CORTAFUEGOS BASADOS EN PROXY

EJEMPLO DE PASARELA DE NIVEL DE APLICACIÓN



CORTAFUEGOS BASADOS EN PROXY

PASARELAS DE NIVEL DE CIRCUITO

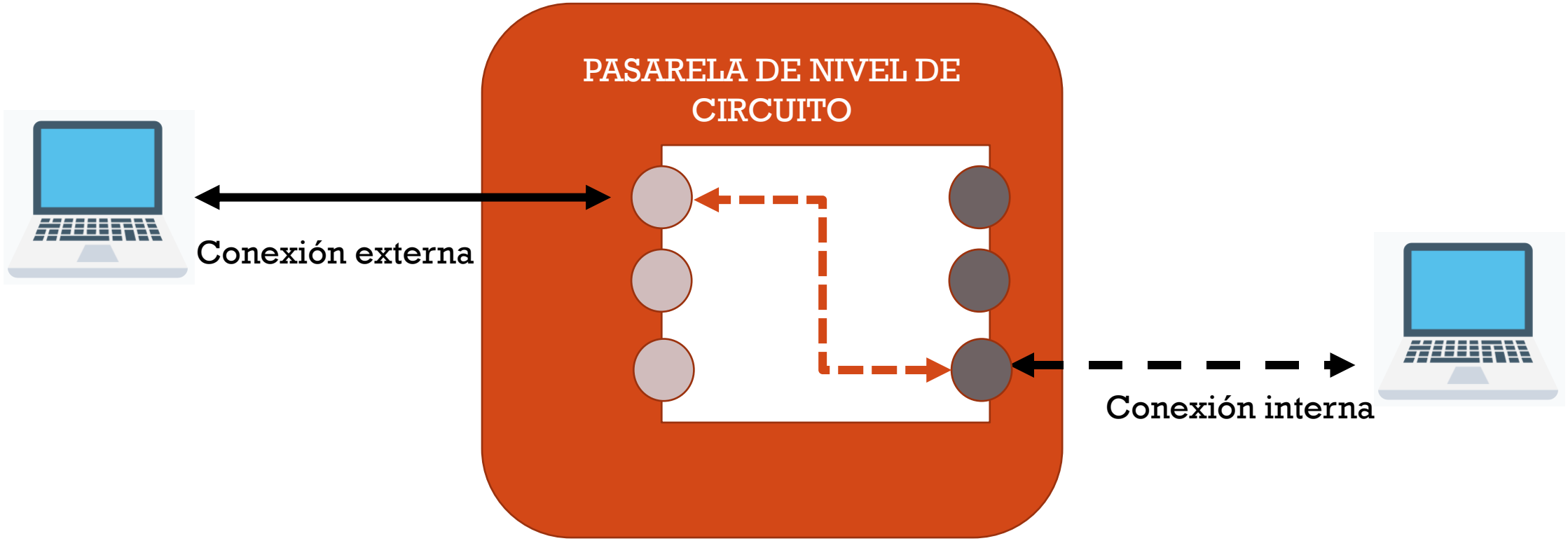
Estas son semejantes a las de aplicación, pero tienen algunas diferencias significativas que las hacen conceptualmente distintas.

Su modo de operación pasa por las siguientes fases:

1. Todos los servicios se solicitan a un único puerto por donde el proxy recoge las peticiones de sus clientes.
2. La pasarela opcionalmente autentica al usuario.
3. Si todo es correcto, el proxy conecta con el servicio solicitado.
4. Una vez que se valida la conexión (establecimiento del circuito), no se inspecciona el contenido de ningún paquete: la conexión se lleva a cabo entre fuente y destino como si circularan por un túnel

CORTAFUEGOS BASADOS EN PROXY

EJEMPLO DE PASARELA DE NIVEL DE CIRCUITO



CORTAFUEGOS BASADOS EN PROXY

PASARELAS DE NIVEL DE CIRCUITO

- En una pasarela e nivel de circuito se conecta el cliente con el servidor a través de una especia de túnel que se crea dentro de la pasarela que conecta una entrada específica con una salida especifica. Es decir, la pasarela copia la información de una de las conexiones en la ora, sin ningún valor añadido.
- Por tanto, hay una única conexión a diferencia de la pasarela de nivel de aplicación que creaba dos conexiones diferenciadas.

- En la práctica, en **instalaciones reales** se suelen utilizar **pasarelas de aplicación y de circuitos simultáneamente**.
  - **Pasarelas de circuito para conexiones salientes**, que siempre serán autorizadas una vez que el usuario se valide en la pasarela.
  - **Pasarelas de aplicación para las conexiones entrantes**, ya que estas conexiones pueden provenir de usuarios no confiables

REDES PRIVADAS VIRTUALES VPN

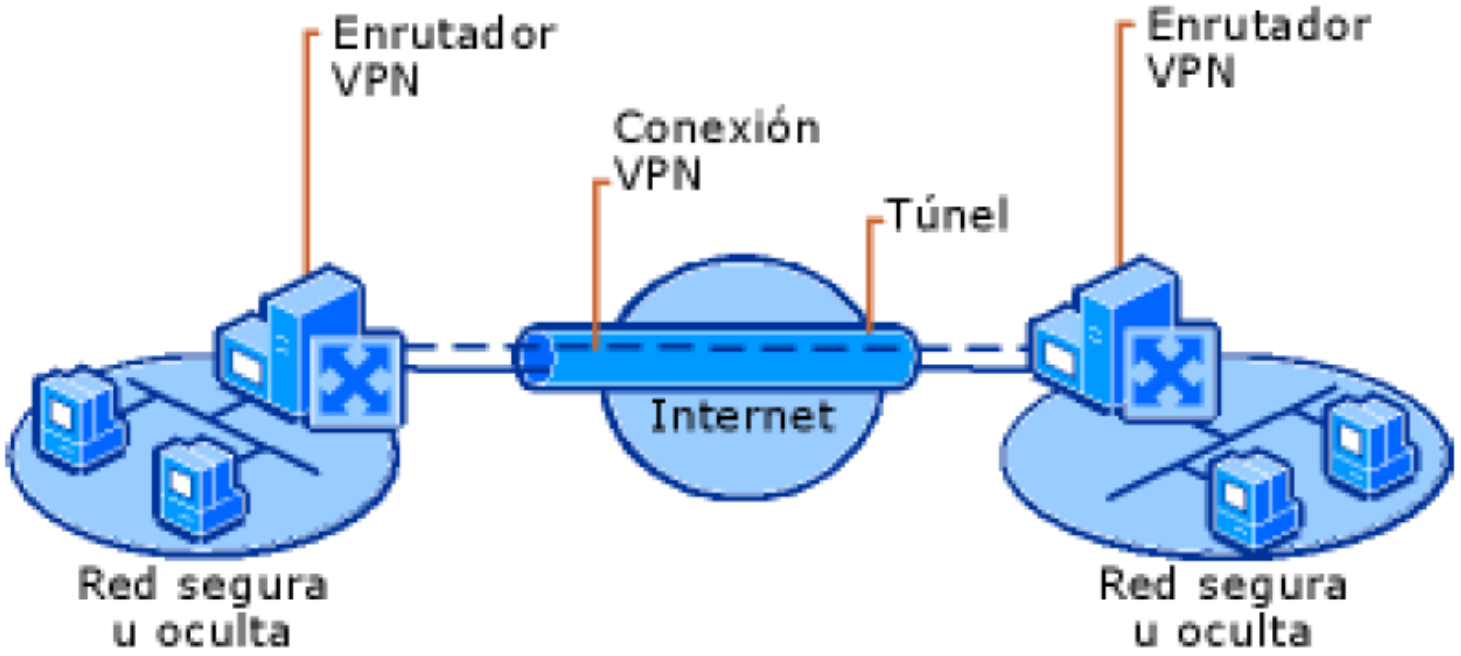
INTRODUCCIÓN

- 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, de 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 túnel cifrado VPN, o simplemente túnel VPN

DEFINICIÓN

- Una **Red privada virtual** (**VPN**) es una red creada artificialmente. Se dice que es **virtual** porque conecta dos redes "físicas" (redes de área local) a través de una conexión poco fiable (Internet) y **privada** porque sólo 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 pública y por lo tanto no está 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 más vulnerables que cuando viajan por una red interna de la organización, ya que la ruta tomada no está 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 mediante **líneas dedicadas**.
- 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 pública como intermediaria; luego transmite la solicitud de manera cifrada. El equipo remoto le proporciona los datos al servidor VPN en su red y éste 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 públicas en vez de alquiladas para realizar conexiones punto a punto.
- Incrementan la seguridad (confidencialidad, integridad, autenticacion y no repudio)
- No son difíciles de desplegar

DESVENTAJAS

- Se necesita una mayor potencia de cálculo ya que la operación de cifrado consume recursos
- Requieren tener Internet disponible, ya que es la red básica de transporte sobre la que se 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.

RECORDEMOS EL CONCEPTO DE NAT

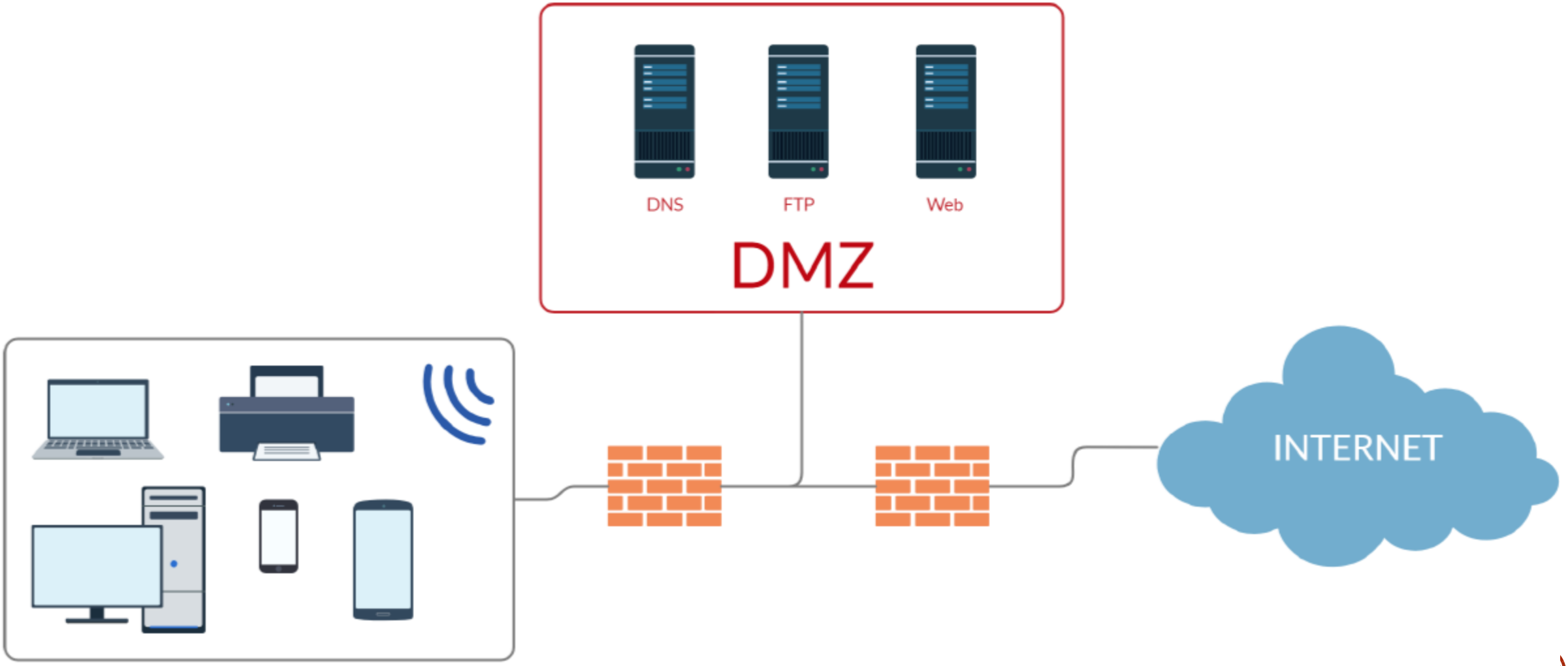
- El direccionamiento público es el esquema de direcciones IP que se utiliza en Internet. Cada dispositivo que se comunique a través de Internet, necesita tener una IP pública
- Un factor que aporta mayor seguridad es el uso de direccionamiento privado, tanto en las redes DMZ como en la red interna. Permite tener direcciones IP diferentes e incompatibles, para la red interna, las redes DMZ y la red externa. Siendo necesario el uso de routers para realizar una interconexión entre ellas por medio de traducciones de direcciones de red (NAT)
- Con esto se evita una comunicación directa entre las diferentes redes, poniendo más trabas al acceso no deseado hacia las redes protegidas.
- NAT (Network Address Translation) es un proceso utilizado por routers para realizar la comunicación de paquetes entre dos redes con direccionamento distinto e incompatible. Consiste en cambiar la información de la dirección IP en las cabeceras correspondientes de los paquetes.

ZONAS DESMILITARIZADAS DMZ

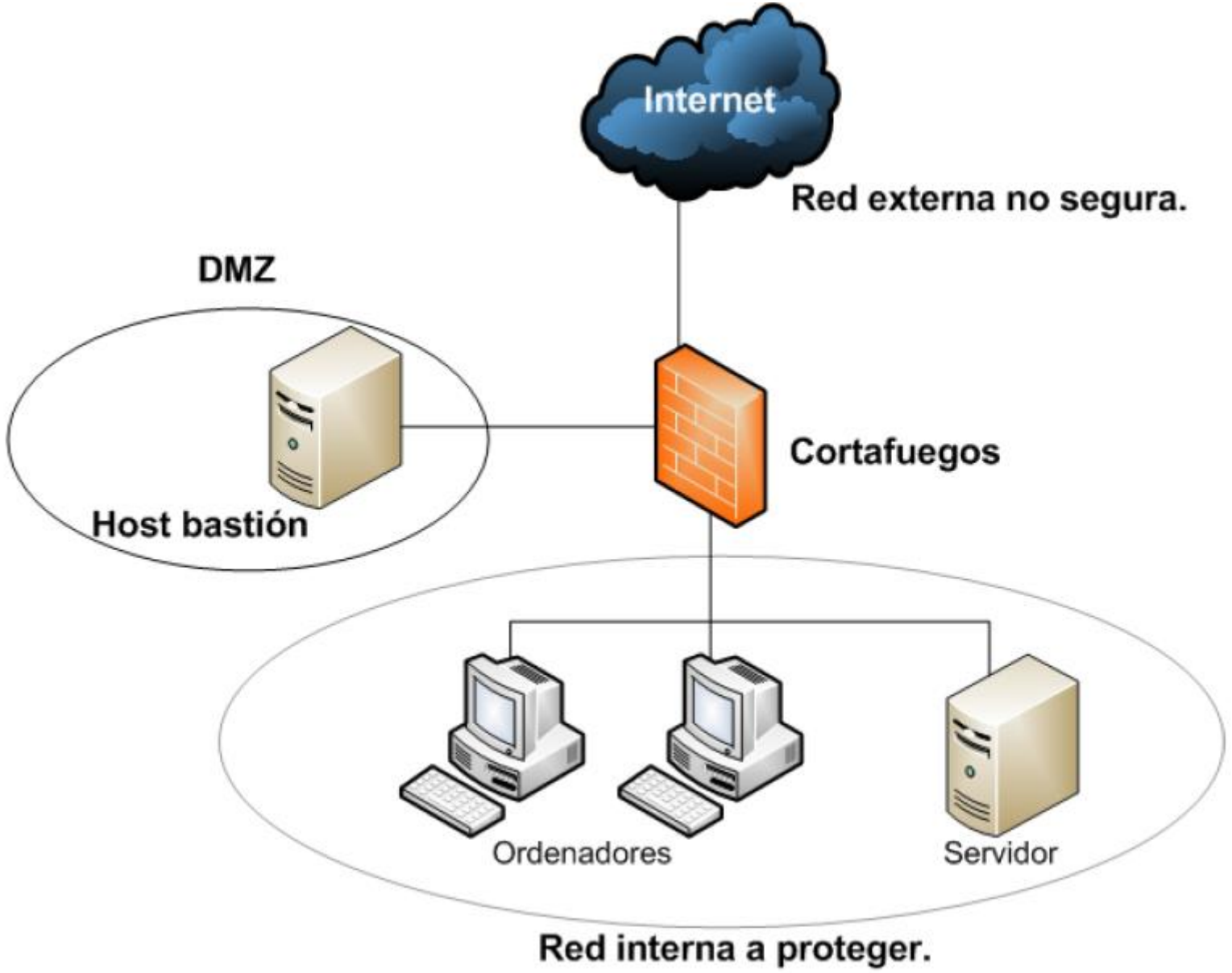
¿QUÉ ES UNA RED DMZ?

- 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.

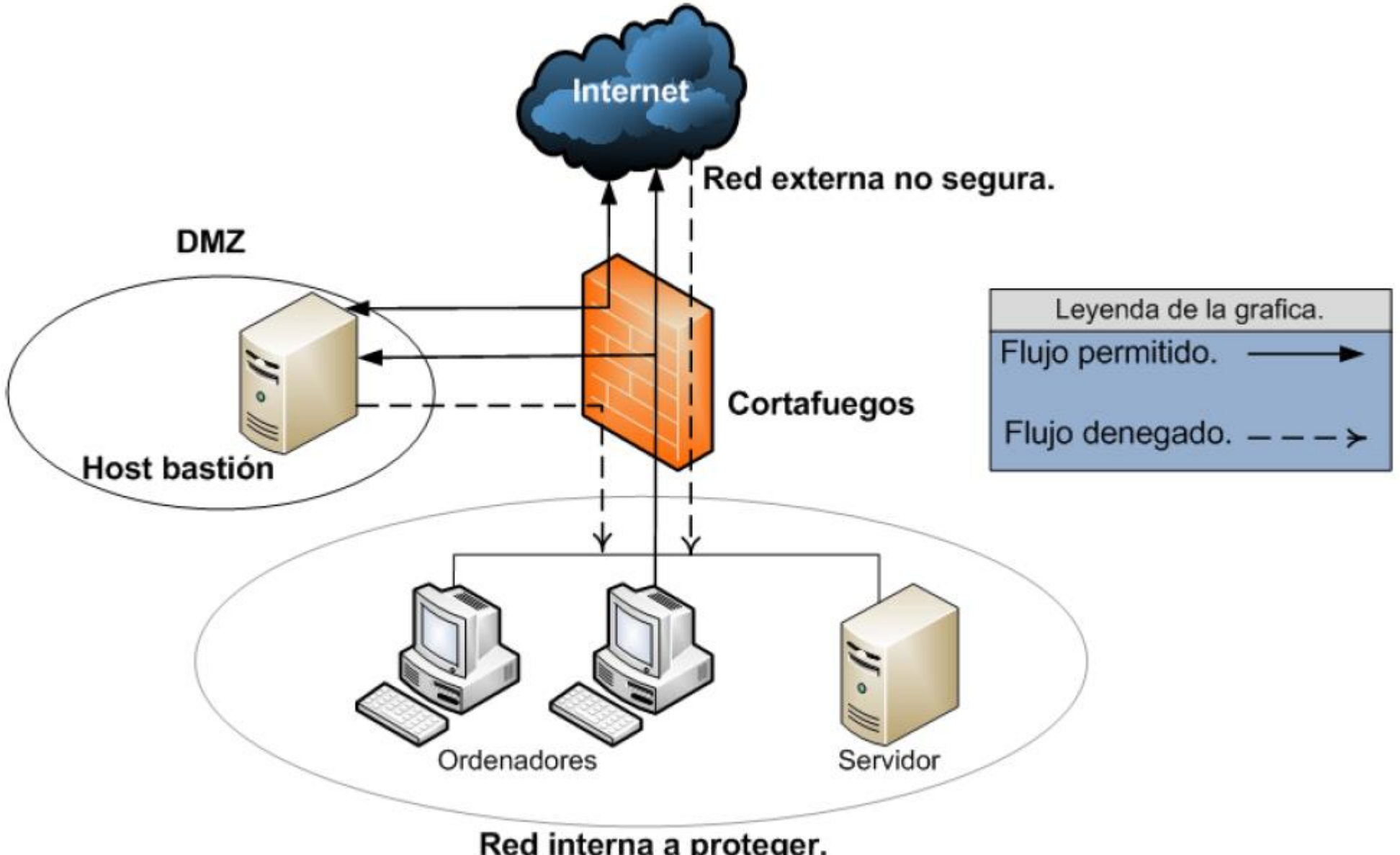
¿QUÉ ES UNA RED DMZ?



ESQUEMA BÁSICO RED CON DMZ



ESQUEMA BÁSICO RED CON DMZ: FLUJO DEL TRÁFICO



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** 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 y 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 tráfico en función de los puertos de origen y destino o permitiendo/deshabilitando protocolos de comunicación
- Algunos de estos protocolos pueden ser: FTP, TELNET, HTPP, SNMP, SSH, DNS…
- IPSec y L2TP son protocolos de seguridad para proteger los datos

PUERTOS EN LA DMZ

- En el diseño de la red DMZ se deben incorporar **reglas que bloqueen todo el tráfico** que no sea necesario para el funcionamiento de las comunicaciones requeridas.
- Esto se hace creando un conjunto de reglas para el **listado de control de acceso (ACL)**, que restringa o bloquee todos los puertos no utilizados por los protocolos permitidos para asegurar la denegación del trafico no deseado. Este conjunto de reglas son la parte esencial para la protección dentro de la DMZ
- ACL (Access Control List). Reglas en forma de sentencias que detallan puertos de servicio o nombres de dominio (de redes) que están disponibles en un terminal u otro dispositivo de capa de red, cada uno de ellos con una lista de terminales y/o redes que tienen permiso para usar el servicio.

SISTEMAS DE DETECCIÓN DE INTRUSIONES IDS

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 tolerante a fallos en el sentido de que debe ser capaz de sobrevivir a una caída del sistema.
- Debe ser resistente a perturbaciones. El sistema puede monitorizarse a sí mismo para asegurarse de que no ha sido perturbado.
- Debe imponer mínima sobrecarga sobre el sistema. Un sistema que ralentiza la máquina o red simplemente no será utilizado.
- 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 tráfico malicioso de la red.
- Genera poder de reacción para prevenir el daño.
- Ayuda a identificar de dónde 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

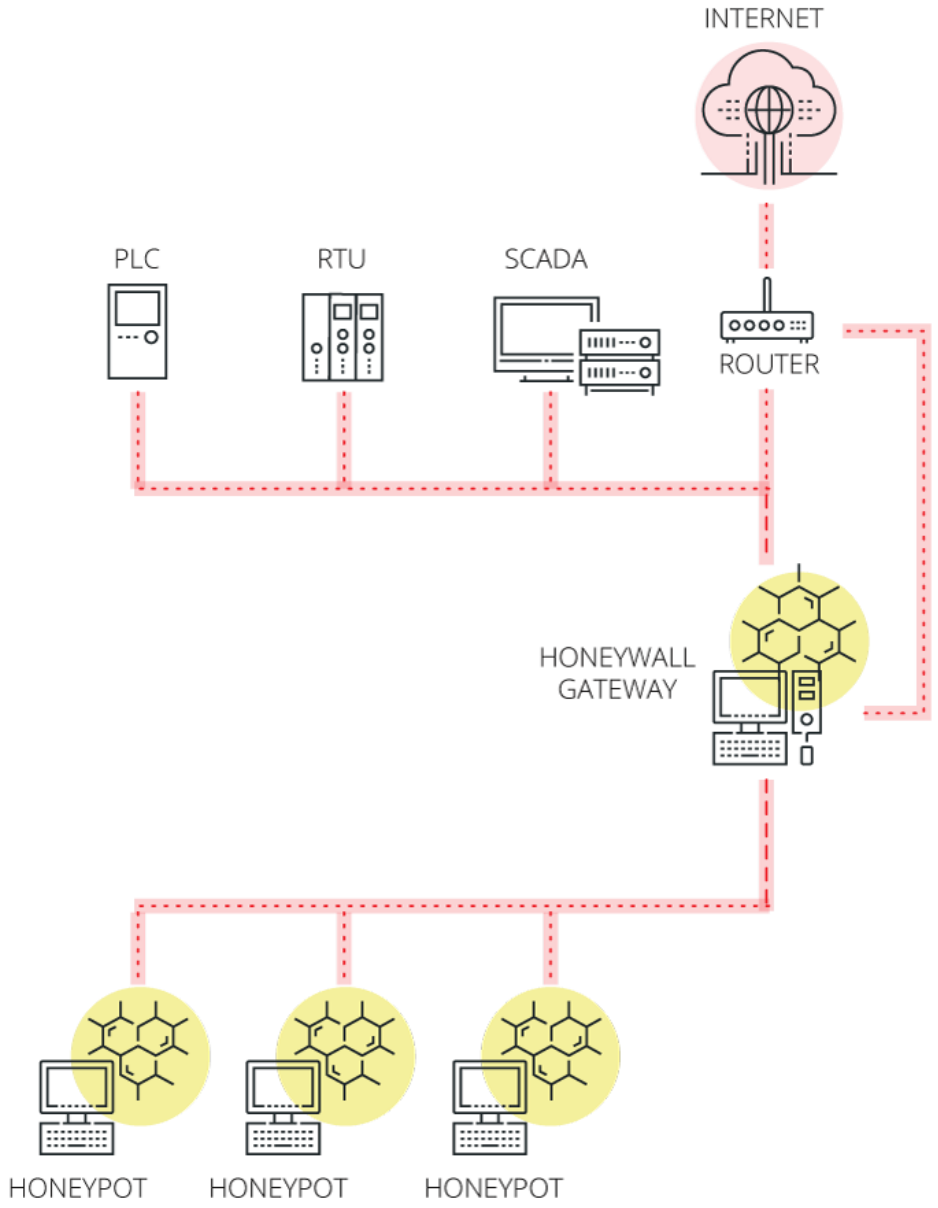
- Se producen falsas alarmas.
- No es sustituto para un buen Firewall, una auditoría de seguridad regular y una fuerte y estricta política de seguridad.
- La alta tasa de falsas alarmas dado que no es posible cubrir todo el ámbito del comportamiento de un sistema de información durante la fase de aprendizaje.
- El comportamiento puede cambiar con el tiempo, haciendo necesario un entrenamiento periódico del perfil, lo que da lugar a la 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.

HONEYPOTS

HONEYPOTS

- El tarro de miel o sistema de detección y engaño, es un sistema configurado expresamente con servicios de red ficticios, incluidas sus vulnerabilidades, para ser utilizado como objetivo de ataques y recoger la información de estos ataques para organizar la defensa.
- Es una trampa para atacantes.
- Hay dos tipos:
  - De investigación: Con más interacción al atacante, para registrar cuantos más datos mejor, y poder definir una mejor defensa.
  - De producción: Alberga funciones de detección y alerta. El fin es engañar al atacante, y que no conozca los servicios reales.
- Los servicios del honeypot no se hacen públicos, por tanto, si alguien accede a ellos, es señal de que es un ataque.

HONEYPOTS


INTERNET
PLC
RTU
SCADA
ROUTER
HONEYWALL
GATEWAY
HONEYPOT
HONEYPOT
HONEYPOT

¿POR QUÉ INSTALAR UN HONEYPOT SI YA HAY UN IDS?

- El honeypot es un complemento al IDS, ya que permite detectar ataques con patrones para los que todavía no hay una firma para el IDS.
- Si un atacante descubre una vulnerabilidad podría pasar desapercibido ante un IDS, si en el IDS no hay una firma para ese ataque por ser un ataque novedoso.
- En el momento en que el atacante intente acceder al honeypot, para explorar su contenido, generaría las alertas producidas por el acceso.
- Un honeypot también sirve para detectar la actividad de gusanos y demás malware que prueban automáticamente amplios rangos de sistemas de la red en su afán de explotar las vulnerabilidades que no has sido parcheadas.

VENTAJAS DE LOS HONEYPOT

- Los datos que ofrecen son mucho más selectivos puesto que siempre proceden de ataques, por lo que tienen muchos menos falsos positivos que los IDS.

- Requieren muy pocos recursos y capturan pocos datos, por lo que el análisis de los mismos es mucho más cómodo y sencillo.

- Son sistemas muy simples y no requieren ni actualizaciones ni un mantenimiento significativo.

INCONVENIENTES DE LOS HONEYPOT

- Solo ven la actividad en su contra, por tanto, si se producen otros ataques en la red, el honeypot no se enterará.

- Son sensibles a ataques de fingerprinting por lo que un atacante podría detectarlos como lo que son (honeypots) y engañar a los administradores para que pensaran que su red está siendo atacada. Es decir, el engañador (nosotros) es engañado.

- Pueden ser utilizados como plataforma para un verdadero ataque en nuestra red una vez comprometidos, por lo que las relaciones de red entre un honeypot y los verdaderos servicios debe estar sumamente cuidada y vigilada.

FUENTES

- Abad Domingo, Alfredo, “Seguridad y Alta Disponibilidad”, Ed. Garceta

UT3. IMPLANTACIÓN DE SEGURIDAD PERIMETRAL

Módulo: Seguridad y Alta Disponibilidad

Curso 2023/2024. 2º ASIR