Firewall

CORTAFUEGOS

Índice

¿Qué es el firewall?

Objetivos y funciones.

Tipos de cortafuegos: hardware y software.

Características:

- Filtrados a diferentes niveles. (Filter)
- Enrutamiento de paquetes. (NAT)
- Políticas de funcionamiento. (Permisión y denegación)

Ubicación.

- Nodo.
- Perimetral.
  - Dual Homed.
  - Screened Subnet (subred monitorizada - doble firewall).
  - Three Legged (Tres patas).

¿Qué es el firewall?

Sistema de seguridad perteneciente a un nodo o a una red.

Se encarga de inspeccionar el tráfico de red, permitiendo el tráfico o denegándolo en función de unas reglas preestablecidas.

Frontera de protección entre nuestros equipos y el exterior.

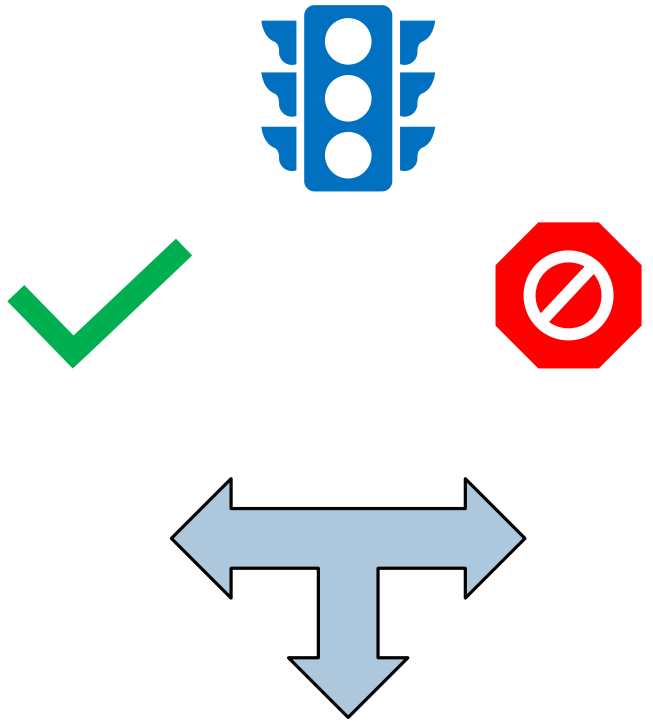
Objetivos y funciones.

Sus principales objetivos son:

- Proporcionar seguridad a la red interna.
- Mejorar el rendimiento de la red interna.
- Asegurar el tráfico adecuado y correcto de la red.

Sus funciones son:

- Permitir la comunicación.
- Denegar la comunicación, con respuesta o sin ella.
- Modificar el tráfico. Enrutamiento.



Tipos: hardware y software

Cortafuegos de tipo hardware:

- Dispositivos hardware diseñados específicamente
  - UTM (Unified Threat Management): Engloban funciones de firewall entre otras (proxy, VPN…)
  - Suelen usar un software propio o software libre, como iptables.

- Equipo o nodo, que puede ser real o virtual.

Tipos: hardware y software

Cortafuegos de tipo software:

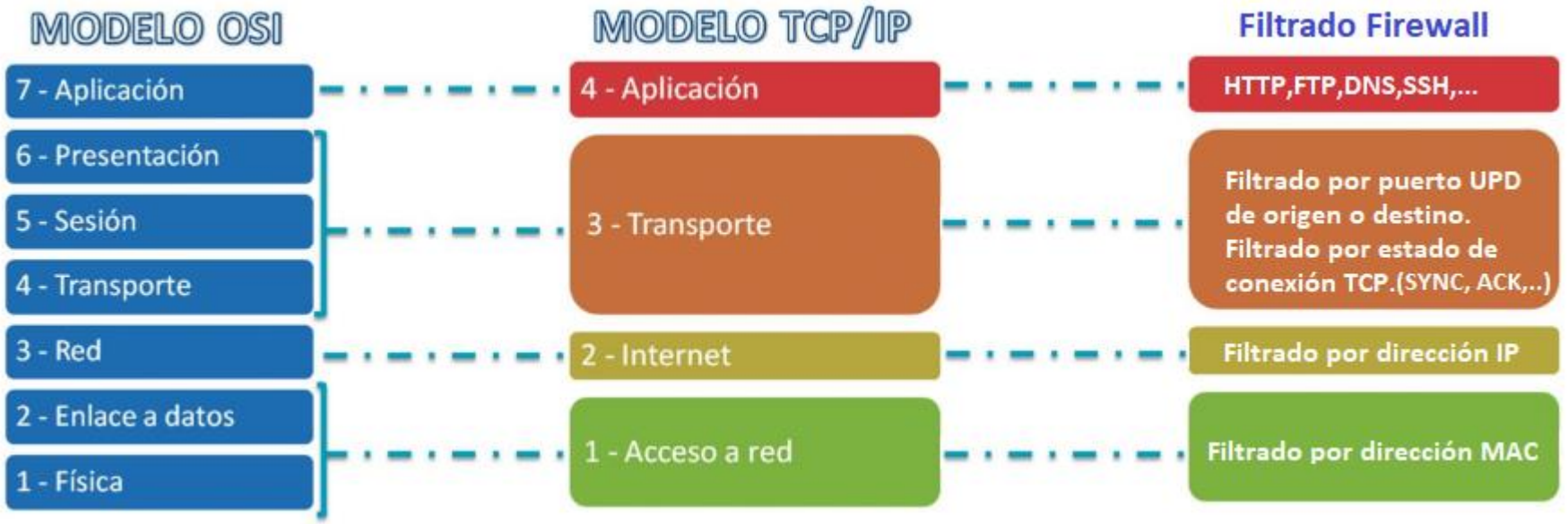
- Software antivirus completo.
- Software propio desarrollado por fabricantes de UTM.
- Software incorporado en sistemas operativos: firewall de Windows 10.
- Software libre: iptables de netfilter (hacen uso de ACL).

Norton LifeLock

netfilter
firewalling, NAT, and packet mangling for linux

Características

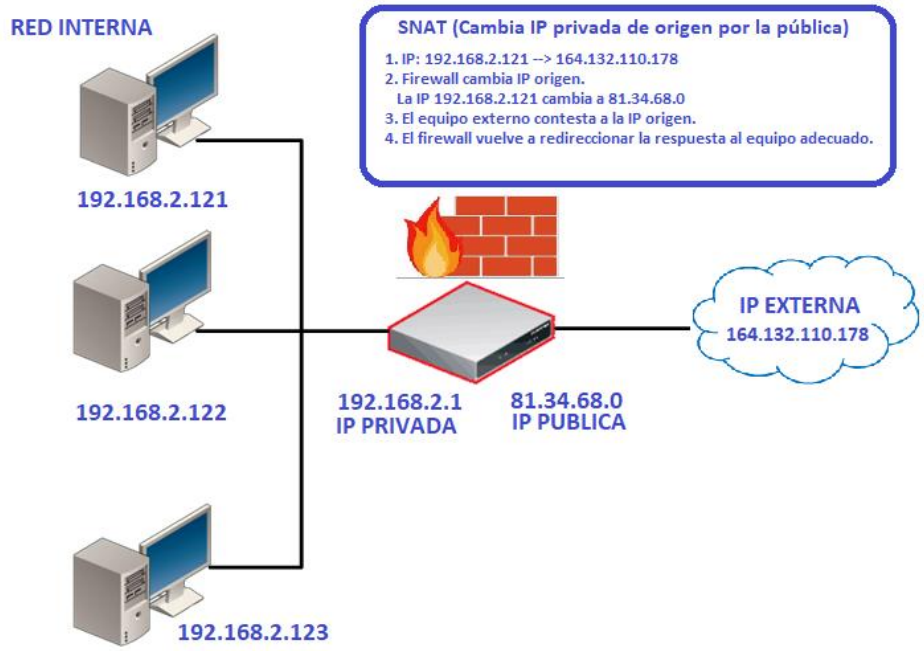
Filtrado a diferentes niveles:



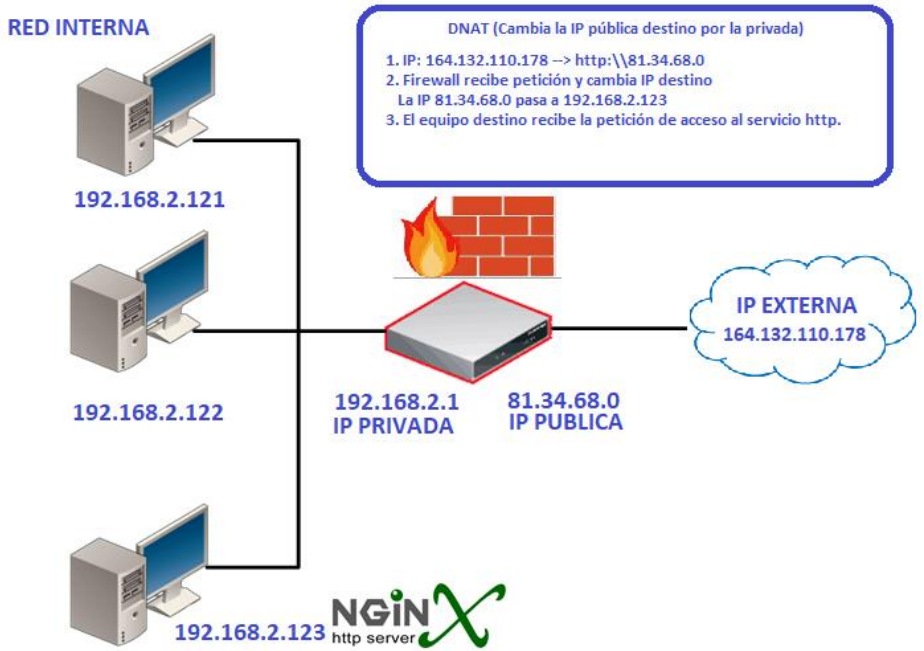
Características

Enrutamiento de paquetes NAT (Network Address Translation).

SOURCE NAT (SNAT)



DESTIONATION NAT (DNAT)



Características

Políticas de funcionamiento: Permisión y denegación

POLÍTICA DE PERMISIÓN (ACCEPT)

La política por defecto es ACCEPT.

- Se permite todo el tráfico.
- Fácil de implementar inicialmente.
- Es muy inseguro, ya que permite nuevas conexiones.
- Se incluyen las reglas de prohibición.

POLÍTICA DE DENEGACIÓN (DROP)

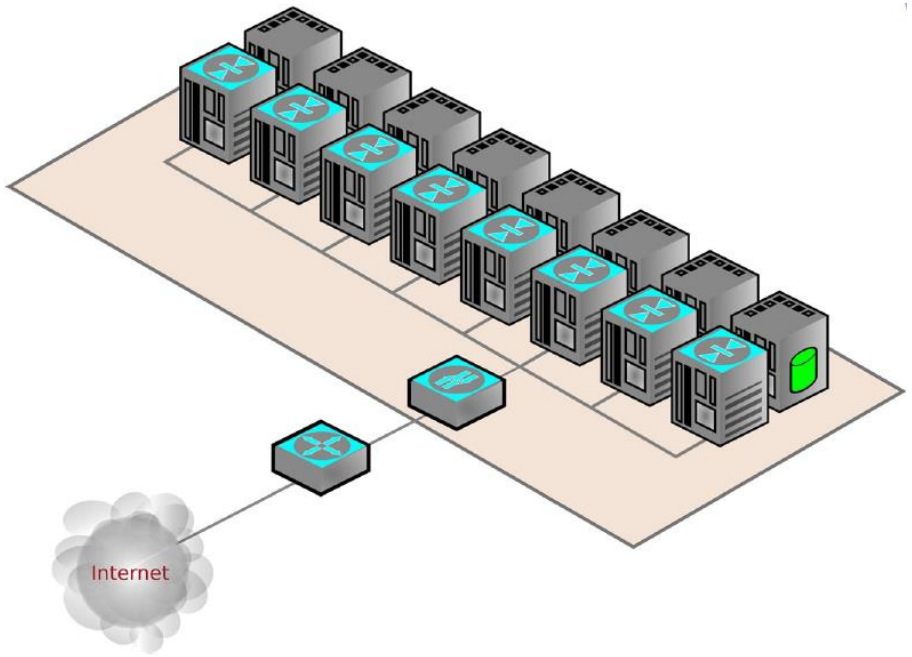
La política por defecto es DROP.

- Se deniega todo el tráfico.
- Difícil implementación inicial.
- Es muy seguro ya que restringe cualquier comunicación no deseada.
- Se van incluyendo reglas de permisión.

Ubicación

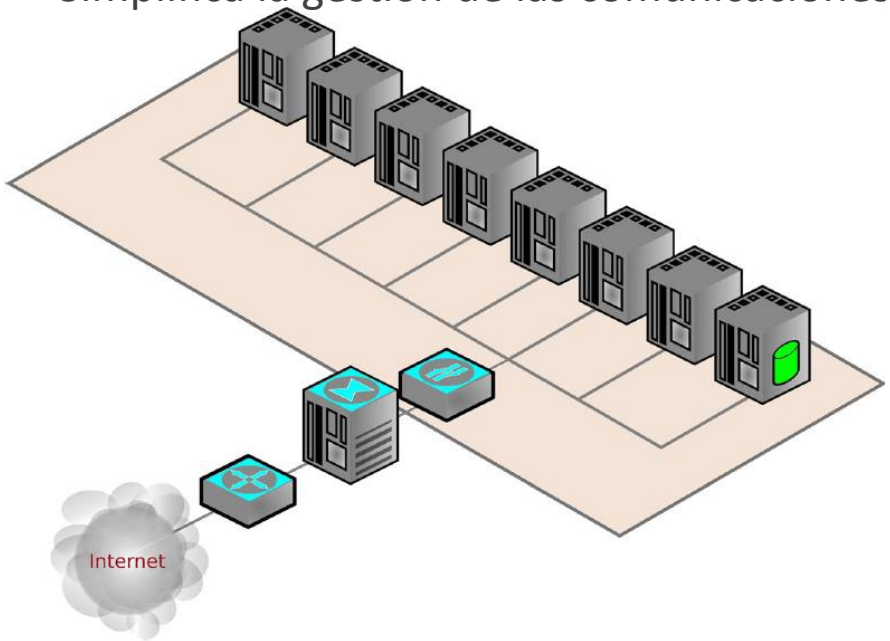
NODO

- Protege cada nodo de forma individual.
- Protege del tráfico interno y externo.



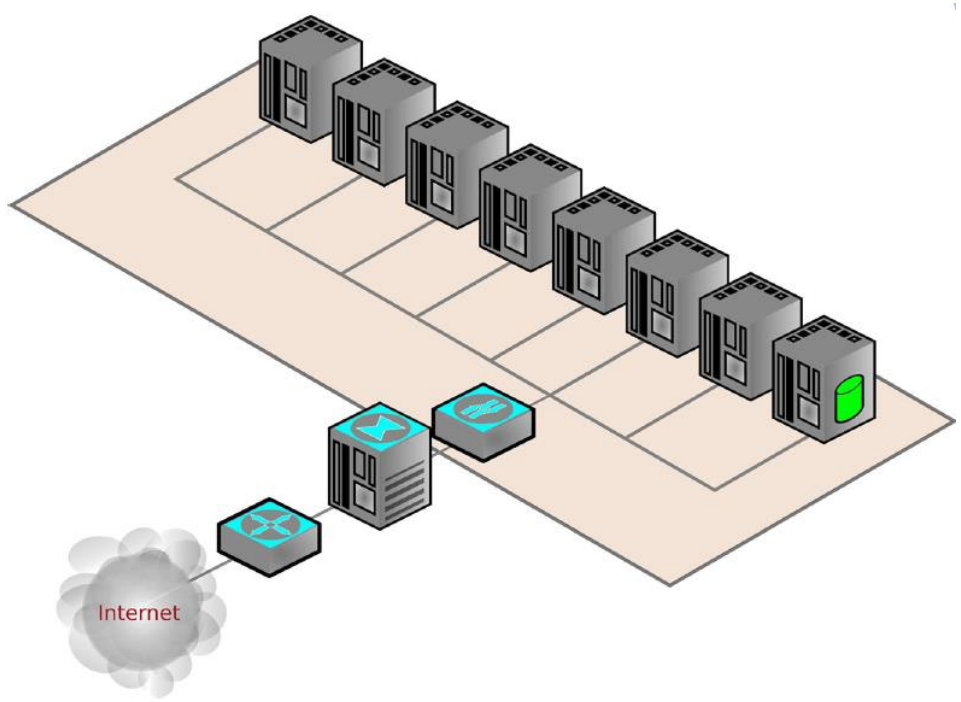
PERIMETRAL

- Protege la red con uno o varios nodos.
- Protege del tráfico interno y externo.
- Simplifica la gestión de las comunicaciones.



Ubicación perimetral

DUAL HOMED

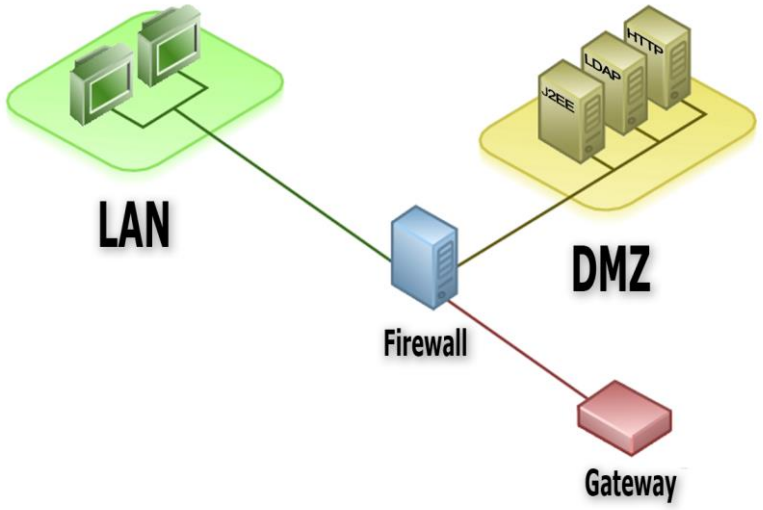


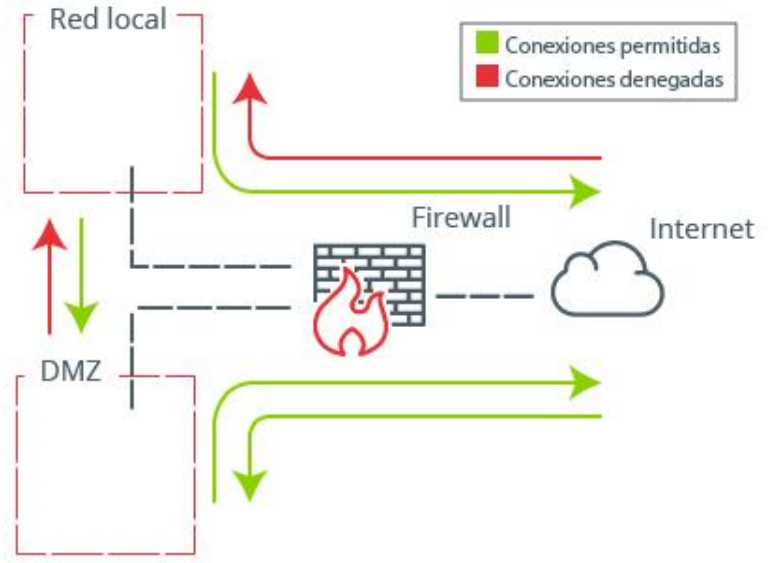
CARACTERÍSTICAS

- Firewall es un nodo con una fuerte y testada configuración.
- Está constantemente monitorizando el tráfico de red.
- Separa nuestra red de forma completa del exterior.
- Implementada en el sector empresarial.

Ubicación: Zona desmilitarizada (DMZ)

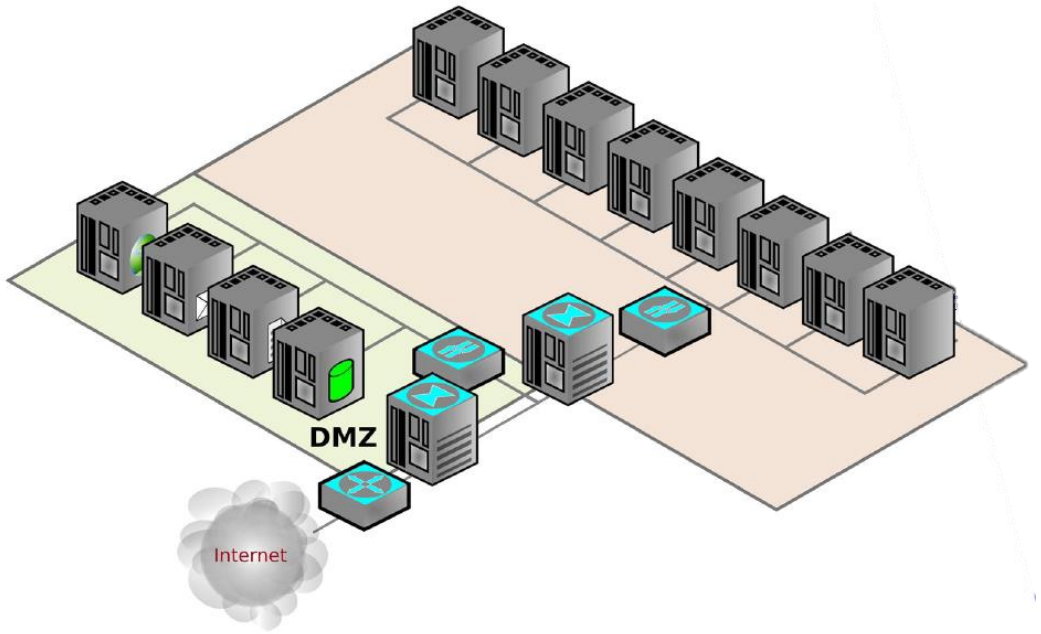
- La zona desmilitarizada o DMZ es una parte de nuestra red que alberga diferentes servidores que brindan sus servicios al exterior.
- La red privada tiene acceso a la zona DMZ.
- La zona DMZ no debe tener acceso a la red interna.
- La red pública puede acceder a los servicios ofrecidos por la DMZ (servicios de correos, web, etc.)





Ubicación perimetral

SCREENED SUBNET (SUBRED MONITORIZADA)

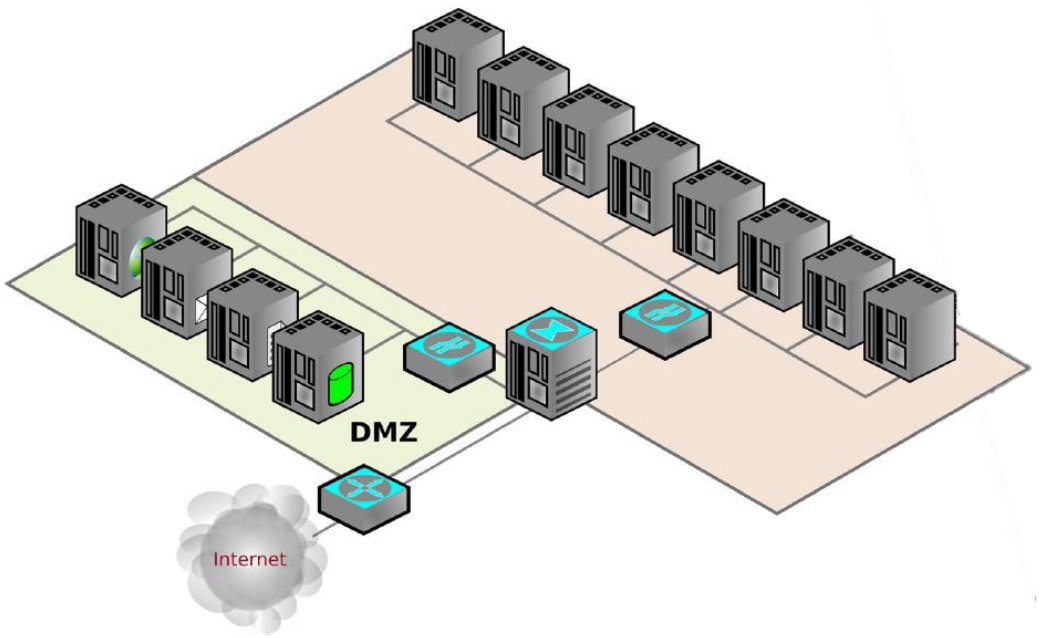


CARACTERÍSTICAS

- Se usa un doble firewall para protección.
- El primer firewall permite las comunicaciones a la DMZ y al segundo firewall.
- El segundo firewall protege a la red interna del exterior y de la DMZ.
- Configuración robusta y muy segura.
- Aplicada en grandes empresas.

Ubicación perimetral

THREE LEGGED (TRES PATAS)



CARACTERÍSTICAS

- Se suprime un firewall dejando solo uno.
- El firewall se encarga de gestionar el acceso a la red interna y a la DMZ de forma aislada.
- Es más insegura que la solución anterior.
- Es usada en pequeñas y medianas empresas.

!Gracias por vuestra atención!

JOSÉ ANTONIO SANTOS GÓMEZ

SEGURIDAD Y ALTA DISPONIBILIDAD – 2º ASIR.