UNIVERSIDAD DE GUADALAJARA

CENTRO UNIVERSITARIO DE CIENCIAS EXACTAS E INGENIERÍAS

DE ELECTRÓNICA Y COMPUTACIÓN

DEPARTAMENTO DE CIENCIAS COMPUTACIONALES

Ingeniería en computación

Administración de redes

SECCIÓN D-05

CLAVE I5907

Ejercicio de Firewall

Edgar Agustín Martínez Gonzalez

CÓDIGO: 220286695

27/10/2022

CALIFICACIÓN: \_\_ / 8

PROF. ANAYA OLIVEROS JORGE

OBSERVACIONES:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Contenido**

Objetivo General……………..……..………………………………………………………….…..2

Objetivo Particular……………………………………………….………………………….……...2

Introducción…………………………………………………………………………………………2

Ejercicio de firewall ........ .............……….……………….……………...………………….……5

Conclusión…………….…………………………………………………………………….………8

Glosario……………………………….…………………….……………...…………………….…8

Referencias………………………………………….………………….………………………..…8

**Objetivo General**

Simular un escenario en el que una red interna exponga solamente un servidor http hacia la red externa y que todos los demás equipos en dicha red sean inalcanzables

**Objetivos Particulares**

* Comprender el funcionamiento de un firewall
* Conocer y aplicar las listas de control de acceso
* Aprender a montar un servidor http en packet tracer

**Introducción**

**Firewall**

Un firewall es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

Los firewalls han constituido una primera línea de defensa en seguridad de la red durante más de 25 años. Establecen una barrera entre las redes internas protegidas y controladas en las que se puede confiar y redes externas que no son de confianza, como Internet.

Un firewall puede ser hardware, software o ambos.

**Tipos de firewall**

**Filtro de paquetes**

Este es el tipo de firewall más antiguo, pero tiene la ventaja de no afectar al rendimiento general del sistema. Puedes pensar en un firewall de filtrado de paquetes como un punto de control que se emplea en un router o switch de tráfico.

El filtro de paquetes evaluará, valga la redundancia, los paquetes de datos que llegan a través de tu router. Normalmente, este filtro puede evaluar la dirección IP de origen, la dirección IP de destino, el tipo de paquete, el puerto de origen y el puerto de destino.

No inspecciona el contenido real del paquete, solo la información general a nivel superficial. En función de la configuración del firewall, puedes filtrar para permitir o no los paquetes procedentes de direcciones IP específicas o de puertos concretos.

Este tipo de firewall es relativamente simple, por lo que es fácil de evadir si eres un atacante decidido. Es mejor utilizar este tipo de firewall junto con otra arquitectura de firewall más fuerte.

**Puerta de enlace a nivel-circuito.**

Al igual que el filtro anterior, una puerta de enlace a nivel-circuito tiene un sistema de aprobación o rechazo del tráfico. Funcionan evaluando el protocolo de control de transmisión (TCP por sus siglas en inglés). Esta evaluación determina si el paquete proviene de una sesión legítima.

**Actuando como servidor proxy**

Se cree que este es el tipo de firewall más seguro porque no permite el contacto directo de la red. El servidor de seguridad proxy tiene la capacidad de examinar todo el paquete de red en lugar de detalles a nivel superficial como la dirección IP y el número de puerto. Al verificar la información del paquete, este firewall puede asegurarse que no tenga ningún contenido malicioso.

Un inconveniente de un firewall proxy es que realiza una conexión adicional para cada paquete que entra y sale, lo que puede causar un retraso en el rendimiento del sistema y puede ser un punto débil durante un ataque externo.

**Firewall de aplicaciones web**

Una puerta de enlace de aplicaciones es similar a un servidor proxy. A continuación, se muestra un ejemplo de cómo funciona:

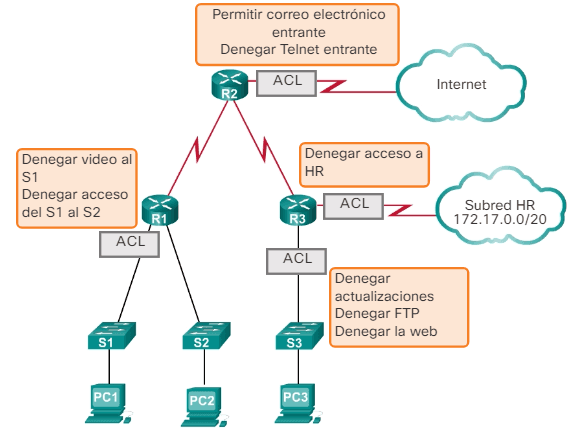
El usuario de la computadora “A” crea una conexión con la puerta de enlace de la aplicación. Luego, la puerta de enlace de la aplicación decide si el contacto entre los dispositivos debe aprobarse o no. Si se aprueba, se establece una conexión con la computadora externa “B”.

Toda la información pasa por dos conexiones: la computadora del usuario “A” a la puerta de enlace de la aplicación y la puerta de enlace de la aplicación a la computadora externa “B”.

La puerta de enlace de la aplicación verifica todo el tráfico antes de enviarlo. Al igual que un servidor proxy, la dirección IP de la puerta de enlace de la aplicación es la única que se ve desde el exterior, por lo que la red interna permanece oculta.

**Listas de control de acceso (ACL)**

Las ACL permiten controlar el flujo del tráfico en equipos de redes, tales como enrutadores y conmutadores. Su principal objetivo es filtrar tráfico: permitir o denegar el tráfico de red de acuerdo con alguna condición. Sin embargo, también tienen usos adicionales, como, por ejemplo, distinguir "tráfico interesante" (tráfico suficientemente importante como para activar o mantener una conexión) en RDSI (red digital de servicios integrados).



**Tipos de ACL**

• ACL estándar, donde solo tenemos que especificar una dirección de origen.

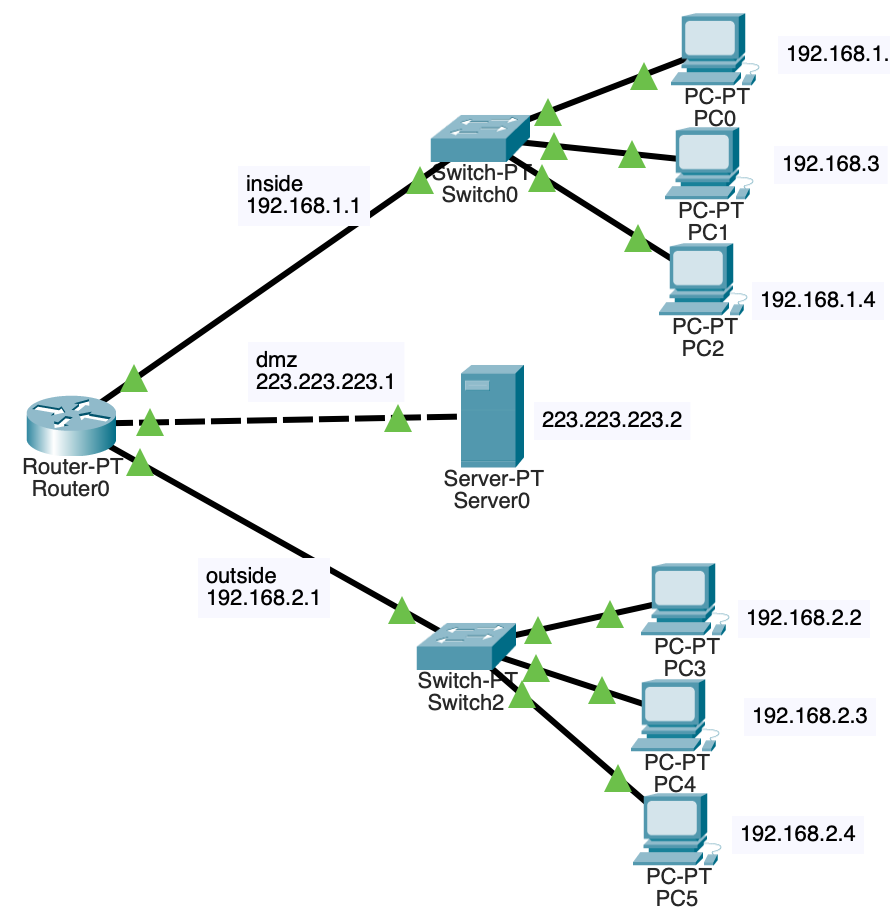
• ACL extendida, en cuya sintaxis aparece el protocolo y una dirección de origen y de destino.

• ACL con nombre, permite dar nombres en vez de números a las ACL estándar o extendidas.

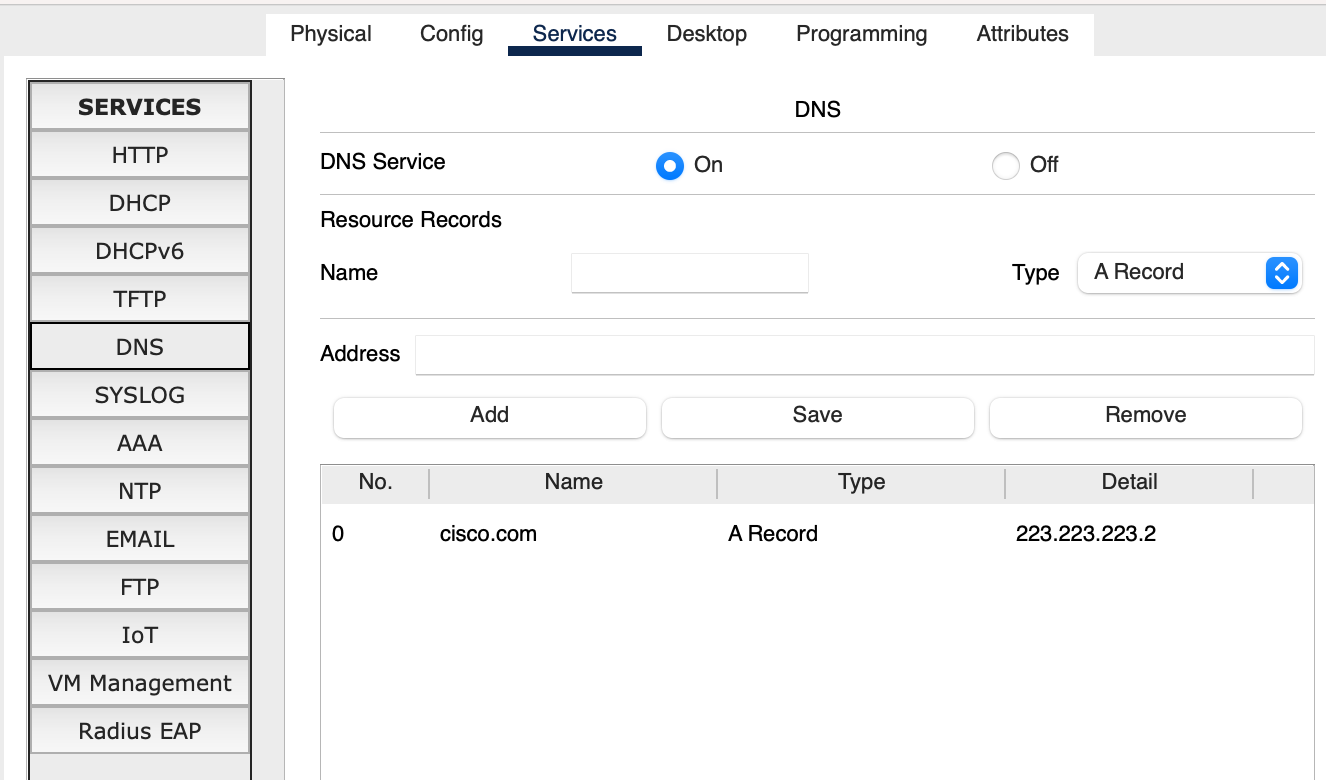
**Ejercicio de firewall**

Lo primero a hacer es crear la red y configurar los equipos con sus correspondientes ip, gateway y el dns como la ip del servidor que usaremos.

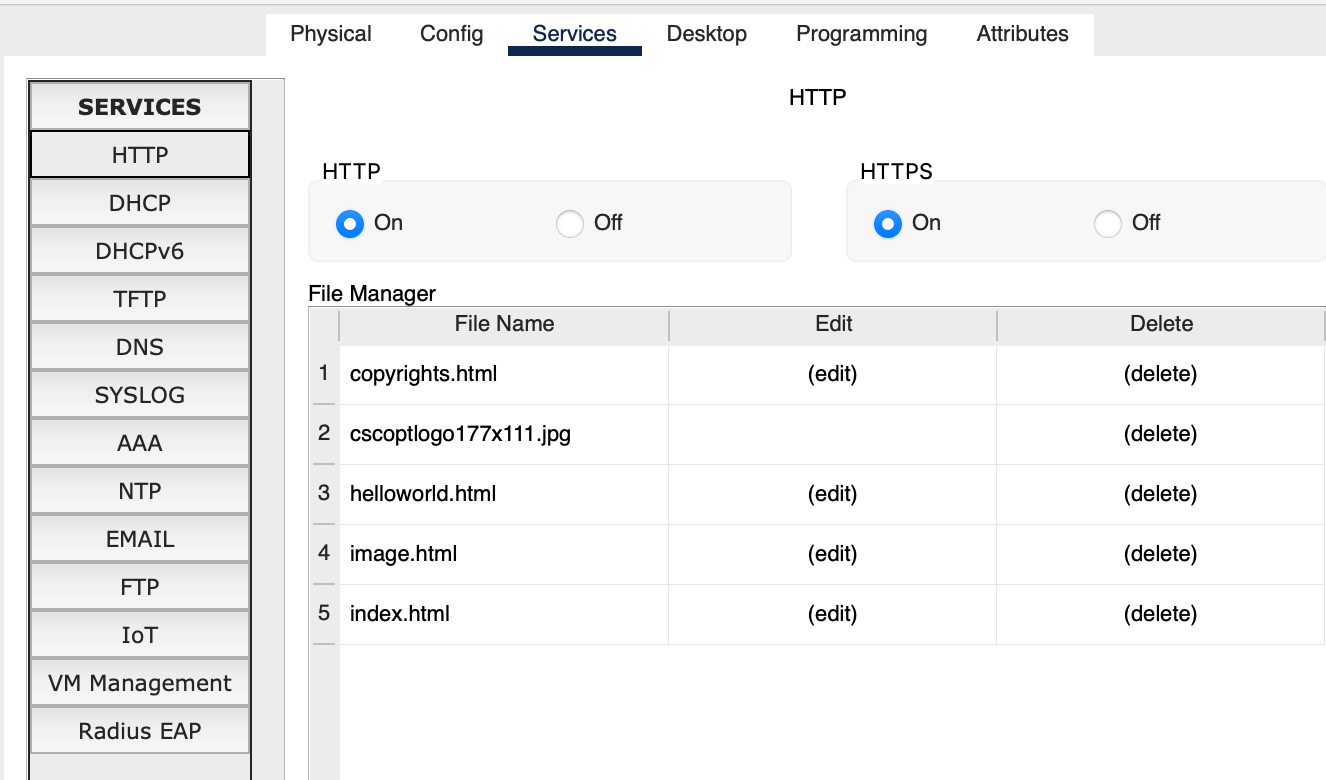
Como se puede observar se tienen 3 redes, inside y dmz representan las redes pertenecientes a nuestra organización y tienen completo acceso a comunicarse entre ellas. Outside representa todo el trafico exterior fuera del control de nuestra organización y unicamente se les permitirá la comunicación al dns y el servidor http



Para configurar el servidor como un dns deberemos activar dicha opcion y ademas definir una url que se asocie con la misma direccion de nuestro servidor.



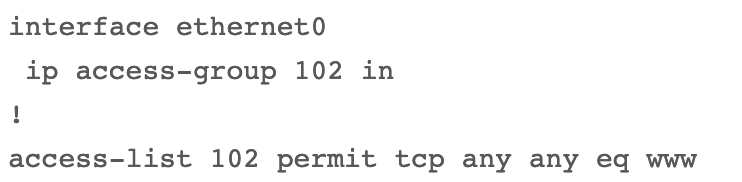
El servidor por default esta configurado con http e incluso incluye unas paginas prefabricadas por packet tracer por lo que no tendremos que agregar nada mas para que funcione como lo queremos



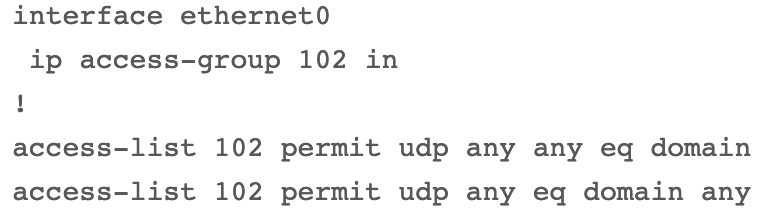
Lo siguiente que tenemos que hacer es configurar el router con los siguientes comandos para crear listas de control de acceso en la sección de cli y aplicando la lista de control de acceso que creamos a la interfaz que corresponde a la red exterior.



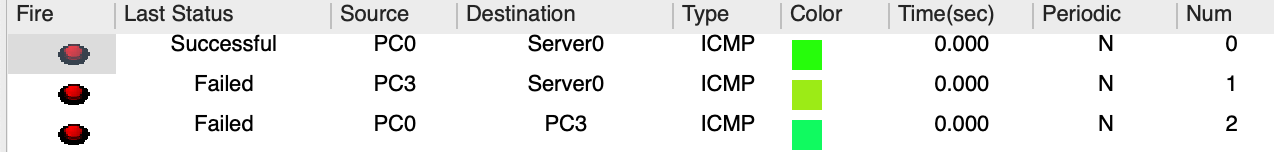
El primer comando permite que la red outside se comunique con nuestra red por medio de http



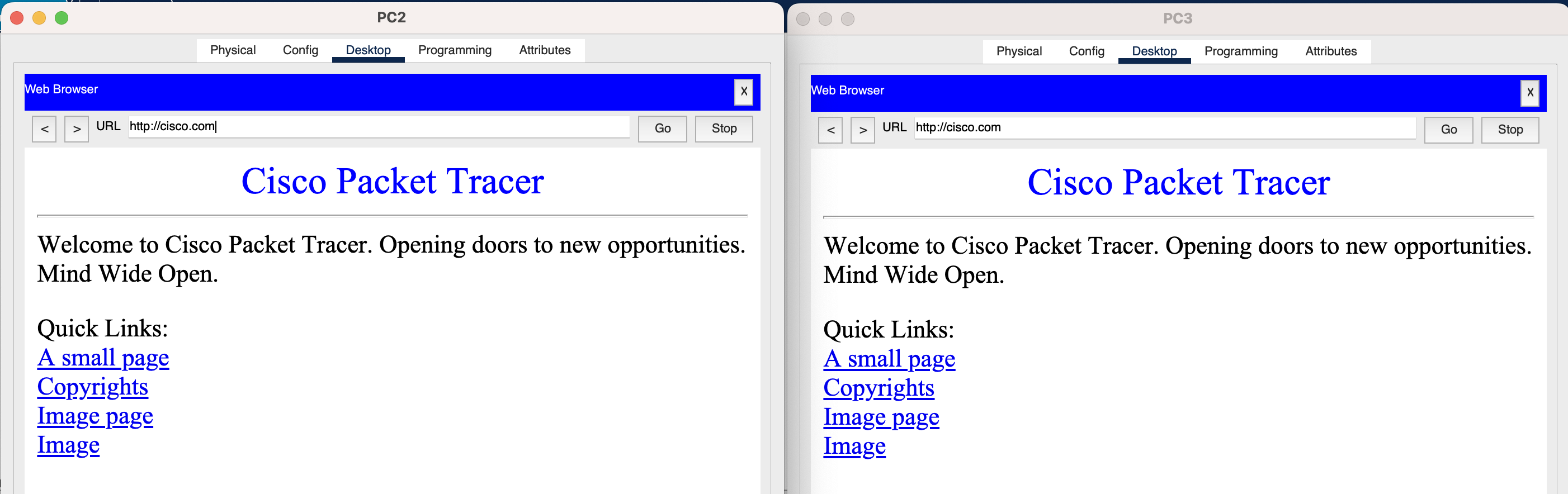
El segundo comando permite la comunicación necesaria para que los equipos de la red outside obtengan la información del dns



Ya configurado todo podemos observar que los equipos de la red inside y dmz se pueden comunicar entre ellos de cualquier forma mientras que los equipos de la red outside no pueden comunicarse por medio de icmp



Sin embargo los equipos de tanto la red inside como outside pueden ver la pagina web del servidor en la red dmz esto gracias a que en la red outside no denegamos los protocolos necesarios para acceder a la pagina



**Conclusión**

Un firewall es esencial cuando se tiene considerado recibir trafico externo fuera del contro de nuestra organizacion, pero existen muchos casos mas en los que es ventajoso configurar un firewall aunque sea por medio de software sin tener que gastar en un equipo mas.

**Glosario**

**Firewall .-** Es un dispositivo de seguridad de la red que monitorea el tráfico de red —entrante y saliente— y decide si permite o bloquea tráfico específico en función de un conjunto definido de reglas de seguridad.

**HTTP.-** El Protocolo de transferencia de hipertexto es el protocolo de comunicación que permite las transferencias de información a través de archivos en la World Wide Web.

**ACL.-** Una lista de control de acceso o ACL (del inglés, access control list) es un concepto de seguridad informática usado para fomentar la separación de privilegios. Es una forma de determinar los permisos de acceso apropiados a un determinado objeto, dependiendo de ciertos aspectos del proceso que hace el pedido.

**DNS.-** El sistema de nombres de dominio (Domain Name System o DNS, por sus siglas en inglés)​ es un sistema de nomenclatura jerárquico descentralizado para dispositivos conectados a redes IP como Internet o una red privada. Este sistema asocia información variada con nombres de dominio asignados a cada uno de los participantes. Su función más importante es «traducir» nombres inteligibles para las personas en identificadores binarios asociados con los equipos conectados a la red, esto con el propósito de poder localizar y direccionar estos equipos mundialmente

**Referencias**

Sportack, M. A., & Sportack, M. A. (2003). *Fundamentos de enrutamiento IP* (1. edición.). Madrid: Pearson Educación.

<https://www.cisco.com/c/es_mx/products/security/firewalls/what-is-a-firewall.html>

https://www.cisco.com/c/en/us/support/docs/ip/access-lists/26448-ACLsamples.html#anc17