ADMINISTRACIÓN Y CONFIGURACIÓN DE REDES (EIMT1019) - CURSO 2018-2019
BOLETÍN DE PROBLEMAS P7

SOLUCION

……

INTRODUCCIÓN.

Una de las herramientas que pueden utilizarse para aportar seguridad de una red es el uso de listas de control de acceso (ACL). En ellas se definen las reglas que pueden prevenir el tráfico de algunos paquetes a través de la red. Se pueden utilizar ACLs IP numeradas o estándares (se especifica IP de origen) o ACLs IP extendidas (se especifica varios parámetros, IP de origen y destino o puertos de origen y destino). En los siguientes ejercicios vamos a utilizar la configuración de red de la figura 1.

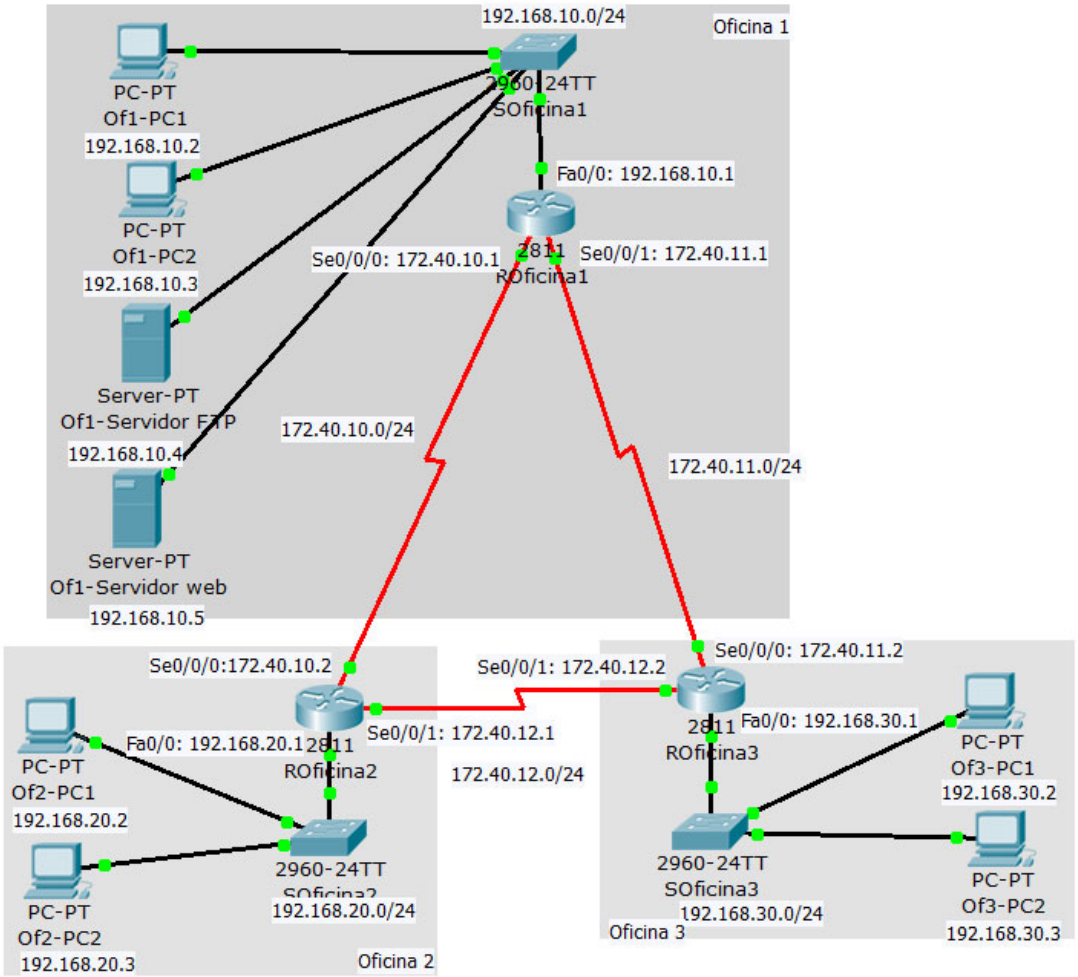

Figura 1. Configuración de la red.

LISTAS DE ACCESO ESTÁNDARES

EJERCICIO 1. Configuración de listas de control de acceso IP estándares.

Con la configuración inicial que aparece en la Figura 1, genera en el Router adecuado la ACL estándar necesaria para que ***el Of1-PC2 no pueda salir de Oficina 1 y el resto de tráfico esté permitido***.

1) Indica el router en donde crearás la lista y la interfaz o interfaces del mismo en donde aplicar la lista.

   Hay varias soluciones. Por ejemplo:

   -Roficina1 en los dos interfaces serie de salida (out)

   -o en Roficina1 en el interfaz Fa0/0 de entrada (in).

   -o otras soluciones serían en cualquiera de los interfaces hasta llegar al destino.

   Supongamos que lo aplicamos en Fa0/0 de entrada al interfaz (in).

2) Crear un comentario con la opción "*access-list 10 remark*" que indique en la ACL "**el Of1-PC2 no pueda salir de Oficina 1"**. Escribe también los comandos necesarios para genera la lista ACL con número 10 que cumplan los requisitos que el tráfico de PC Of1-PC2 no pueda salir de Oficina1 y el resto de tráfico está permitido.

   ROficina1(config)#

   access-list 10 remark Impide acceso al exterior de Of1-PC2

   access-list 10 deny host 192.168.10.3

   access-list 10 permit any

3) Indica los comandos para aplica la ACL en las interfaces que diste en el apartado 1). Indica primero el router (por ejemplo: "ROficinaX:") y después escribe los comandos para aplicar la lista en la o las interfaces adecuadas del router.

   En ROficina1:

   interface Fa 0/0

   ip access-group 10 in

   exit

4) ¿Crees que con la lista creada un PC de la Oficina 3 podrá acceder al Of1-PC2? Justifica tu respuesta.
   No, la vuelta del ping desde Of1-PC2 al PC de la oficina3 no funcionará debido a la lista.

LISTAS DE ACCESO EXTENDIDAS

EJERCICIO 2

Cuando necesitamos filtrar tráfico entre direcciones IP (o puertos de protocolos) de origen y destino será necesario el uso de listas de control de acceso extendidas.

Configuración de ACLs IP extendidas para denegar tráfico entre 2 host.

Con la configuración inicial que aparece en la Figura 1 genera las ACLs extendidas necesarias para que ***el pc Of1-PC2 no pueda acceder al pc Of3-PC1 y el resto de tráfico será permitido***. Veamos los pasos a seguir:

5) ¿Cuál será el Router adecuado para aplicarle las listas?

   Roficina1

6) Crear un comentario con la opción "*access-list 101 remark"* que indique en la ACL "**Of1-PC2 no pueda acceder a Of3-PC1**". Escribe también los comandos necesarios para genera la lista ACL con número 101 que cumplan los requisitos que el tráfico de Of1-PC2 no pueda acceder al pc Of3-PC1 y el resto de tráfico esté permitido.

   access-list 101 remark Of1-PC2 no puede acceder a Of3-PC1

   access-list 101 deny ip host 192.168.10.3 host 192.168.30.2

   access-list 101 permit ip any any

7) Indica los comandos para aplica la lista en la o las interfaces adecuadas del router que indicaste en 5).

   interface FastEthernet0/0

   ip access-group 101 in

   exit

EJERCICIO 3

Configuración de ACLs IP extendidas para denegar tráfico entre dos redes.

Con la configuración inicial que aparece en la Figura 1, genera en el Router adecuado las ACLs extendidas necesarias para que ***los hosts de Oficina 2 no puedan acceder a los host de Oficina 3 y el resto de tráfico esté permitido.*** Pasos a seguir:

8) ¿Cuál será el Router adecuado para aplicarle las listas?

   Roficina2

9) Crear un comentario con la opción "*access-list 102 remark*" que indique "***los hosts de Oficina 2 no pueden acceder a los host de Oficina 3 y el resto de tráfico está permitido***". Escribe también los comandos para crear la ACL con número 102 que cumpla los requisitos ***los hosts de Oficina 2 no puedan acceder a los host de Oficina 3 y el resto de tráfico esté permitido.***

   En Roficina2:

   access-list 102 remark host de Of2 no pueden acceder a host de Of3

   access-list 102 deny ip 192.168.20.0 0.0.0.255 192.168.30.0 0.0.0.255

   access-list 102 permit ip any any

10) Indica los comandos para aplica en la interfaz adecuada la lista de acceso creada.

    En Roficina2:

    interface FastEthernet0/0

    ip access-group 102 in

    exit

11) ¿Con está lista un PC de la oficina 3 podrá alcanzar a un PC de la oficina 2? Justifica tu respuesta.

    Podrá llegar pero no ira la vuelta

EJERCICIO 4

Configuración de listas de control de acceso IP extendidas para denegar tráfico especificando protocolos y puertos de origen y/o destino.

Con la configuración inicial que aparece en la Figura 1, queremos generar en el Router adecuado una ACL extendidas para que:

-el pc Of3-PC1 no pueda acceder al pc Of1-PC2,
- denegar el tráfico FTP de Of3-PC1 al servidor ftp en oficina1
-denegar el tráfico HTTP de Of3-PC2 al servidor web en oficina1
-que el resto de tráfico esté permitido.

12) Indica en que router e interfaces del mismo lo aplicarías y los comandos para hacerlo.

Roficina3

13) Escribe los comandos para generar la ACL 110 con los requisitos anteriores.

access-list 110 remark Of3-PC1 no puede acceder a Of1-Servidor ftp

access-list 110 remark Of3-PC2 no puede acceder a Of1-Servidor web

access-list 110 deny tcp host 192.168.30.2 host 192.168.10.4 eq ftp

access-list 110 deny tcp host 192.168.30.3 host 192.168.10.5 eq www

access-list 110 permit ip any any