Laboratorio 10: Cortafuegos en sistemas IOS

Objetivos:

- Aprender a utilizar listas de control de acceso (`ACL`) para configurar cortafuegos en sistemas IOS[1].

Topología de trabajo

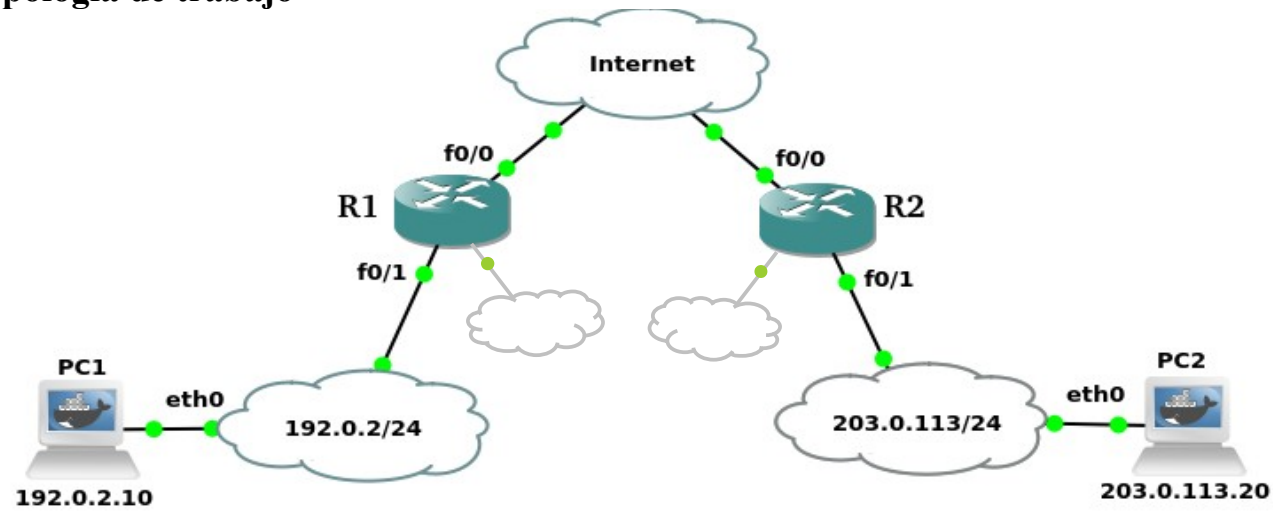

Figura 1 : Red utilizada

Tareas

Preparativos:

1. Para empezar, desde *e-gela*, descarga la configuración de la red, y descomprímela en el directorio `GNS3/projects`.
2. Lanza `GNS3`, abre la red descargada. Verifica el nombre de las interfaces, pon en marcha todas las máquinas y abre todas las consolas.
3. Para verificar que la red funciona correctamente, haz `ping` desde `PC1` a `PC2`, desde `R1` a `PC2`, y desde `R2` a `PC1`. Si no funciona, notifíquelo al docente.

Configuración básica en un cortafuegos en IOS: filtrar por dirección IP de origen.

4. Supongamos que en la red `203.0.113/24` se ha definido la siguiente política de seguridad:
   - **Solo se permite** el tráfico que proviene de la red `192.0.2/24`, enviado a cualquier máquina de nuestra red.

   a. ¿Qué tipo de lista `ACL` usarías para llevar a cabo este control, estándar o extendida?

   b. ¿En qué máquinas deberías configurar esta lista `ACL` para controlarlo?

   c. Haz la configuración necesaria. Usa el modo `ACL` numerada.

[1] https://www.ciscopress.com/articles/article.asp?p=3089353

d. Verifica la configuración realizada mediante los comandos '`sh ip interface`', '`sh access-list`' y '`sh run | include access-list`'

e. Comprueba que el cortafuegos definido está haciendo su trabajo. Para eso, (1) haz `ping` desde `PC1` a `PC2`, y (2) haz `ping` desde `R1` a `PC2`. Este segundo no tiene que funcionar

f. Con el comando '`sh access-list`', puedes ver las estadísticas asociadas a la lista. Y con '`clear access-list counters`', poner a cero los contadores.

5. Supongamos que en la red `192.0.2/24` se ha definido la siguiente política de seguridad:
   - **Solo se permite** el tráfico que proviene de la maquina `203.0.113.20`, enviado a cualquier máquina de nuestra red.

   a. Haz la configuración necesaria. Utiliza el modo `ACL` nombrada, y llama '`FILTRO-HOST`' a tu `ACL`

   b. Verifica la configuración realizada mediante los comandos '`sh ip interface`' y '`sh access-list`'

   c. Comprueba que el cortafuegos definido está haciendo su trabajo. Para eso, (1) haz `ping` desde `PC2` a `PC1`, y (2) haz `ping` desde `R2` a `PC1`. De nuevo, el segundo no tiene que funcionar.

   d. Cambia la lista `FILTRO-HOST`, para permitir también el tráfico proviniente de la interfaz `R2-f0/0`. Verifica la configuración realizada, y repite el anterior `ping` de `R2` a `PC1`

Filtros más específicos en IOS

6. Detén `R1` y `R2`, y luego inicia ambas máquinas y abre la consola. Verifica que puedes hacer, sin problemas, `ping` entre los dos PCs y desde `PC1` al encaminador. Además, intenta establecer una sesión `telnet` desde `PC1` con `PC2` (`telnet 203.0.113.20`). ¿Qué respuesta obtienes?
7. Supongamos que en la red `192.0.2/24` se ha definido la siguiente política de seguridad:
   - Se permite el tráfico generado en esta red que vaya a cualquier servidor HTTP externo.
   - Se permite realizar `telnet` desde la máquina `PC1` a la interfaz `R2-f0/0`
   - Todo el resto del tráfico no debe salir de la red a Internet.

   a. ¿Qué tipo de lista `ACL` usarías para realizar este control, estándar o extendido?

   b. Ejecuta los comandos requeridos para llevar a cabo la política anterior. Utiliza `ACL`s numeradas

   c. Verifica que has definido bien el filtrado, y también prueba su funcionamiento:

   Desde `PC1`:

   - Prueba a hacer `telnet` a `R2-f0/0`. Cuando consigas hacer la conexión, ejecuta después '`quit`' para cancelar la sesión.
   - Prueba a hacer `ping` a `PC2`. Idem `R2-f0/0`
   - Prueba a hacer el siguiente `telnet` : `telnet 198.51.100.2 80`

     Si va bien, se establecerá una sesión `telnet`, y el servidor web que está en `R2` está a la espera. Escribe lo siguiente:

     ```
     GET / HTTP/1.1
     ```

[línea en blanco]

- Repite la sesión `telnet` del ejercicio 6 a `PC2`. ¿Qué diferencia hay entre la negación de ahora y la que obtuviste antes?

8. Supongamos que en la red `203.0.113/24` se ha definido la siguiente política de seguridad:
   - **Solo se permite** tráfico web que va desde esta red a `R1-f0/0`

   a. Ejecuta los comandos requeridos para llevar a cabo la política anterior. Utiliza `ACL`s nombradas.
   b. Verifica que has definido bien el filtrado, y también prueba su funcionamiento

      Desde `PC2`:

      - Prueba a hacer el siguiente `telnet: telnet 198.51.100.1 80`
      - Si va bien, se establecerá una sesión `telnet`, y el servidor web que está en `R2` está a la espera. Escribe lo siguiente:

        ```
        GET / HTTP/1.1
        ```
        [línea en blanco]
      - Prueba un `ping` a `R1-f0/0`
      - Prueba un `ping` a `R2-f0/0`

   c. Modifica la asignación realizada, reasigna la `ACL` a la otra interfaz y en sentido contrario

      Desde `PC2`:

      - Prueba un `ping` a `R1-f0/0` ¿Por qué obtienes el mismo resultado?
      - Prueba un `ping` a `R2-f0/0` ¿Por qué obtienes un resultado distinto?
9. Supongamos que quieres permitir hacer `ping` entre las redes `192.0.2/24` y `203.0.113/24`
   a. Verifica que no funciona `ping` entre los dos `PC`s
   b. Cambia los cortafuegos configurados para lograrlo.
   c. Verifica que funciona `ping` entre los dos `PC`s

Referencias:

- https://ccnadesdecero.es/listas-control-acceso-ACL-router-cisco/
- https://ccnadesdecero.es/configuracion-ACL-ipv4-estandar/
- http://www.itesa.edu.mx/netacad/switching/course/module9/index.html#9.0.1.1
- http://ecovi.uagro.mx/ccna/ccna2/#7