El punto general es que en este tipo de casos la ACL se enfoque especialmente en empresas donde quieran evitar tráfico no deseado en sus páginas y dentro de su empresa. Esto es particularmente relevante en situaciones donde el exceso de accesos pueda comprometer la estabilidad de los sistemas informáticos o donde sea crucial mantener una alta disponibilidad y rendimiento de los servicios en línea. Además, mediante el uso estratégico de listas de control de acceso, las organizaciones pueden asegurarse de que solo los usuarios autorizados tengan acceso a recursos críticos, minimizando así los riesgos asociados a la seguridad de la información.

Al implementar estas políticas, no solo se protegen contra posibles ataques cibernéticos, sino que también se optimizan los recursos al evitar el consumo innecesario de ancho de banda. Esto es vital para empresas que manejan grandes volúmenes de datos o que ofrecen servicios críticos en tiempo real. Así, la ACL se convierte en una herramienta esencial para la gestión eficiente del tráfico de red, permitiendo que la empresa opere de manera más fluida y segura.

En este contexto, las políticas de acceso pueden ser configuradas para identificar y bloquear automáticamente el tráfico que se considere potencialmente peligroso o innecesario. Por ejemplo, el tráfico de bots maliciosos, ataques de denegación de servicio (DDoS) y otros intentos de intrusión pueden ser efectivamente mitigados mediante el uso de ACLs que filtran las solicitudes basadas en IP, tipo de protocolo, y puertos específicos.

Además, esta estrategia de control de acceso no solo ayuda a reducir la carga en la infraestructura de red, sino que también contribuye a una mejor gestión de los recursos de TI. Al limitar el acceso solo a los usuarios legítimos y necesarios, se asegura que los sistemas críticos funcionen sin interrupciones, lo que es de suma importancia en entornos corporativos donde el tiempo de inactividad puede tener consecuencias financieras significativas.

La información se recopilo ante las actividad que se prevé que pase en el campo laboral aportado del curso de Cisco.

**Bitácora: Configuración de ACL estándar IPv4**

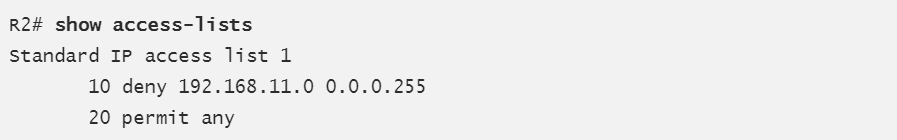
1. Abrimos la primera actividad que se encargó, y se hace el primer pasó, agregando un ACL estándar numerado en **R2**.



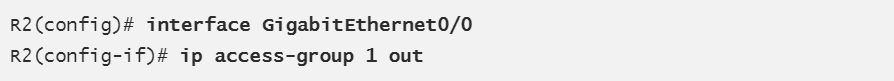
1. Se agrega el acceso para denegar todo el trafico que no coinciden con ninguna regla.



1. Antes de activar la lista de acceso, corroboramos la lista con el comando para filtrar el tráfico como se esperaba.



1. Se aplica la ACL en el tráfico saliente de la **interfaz GigabitEthernet0/0**.



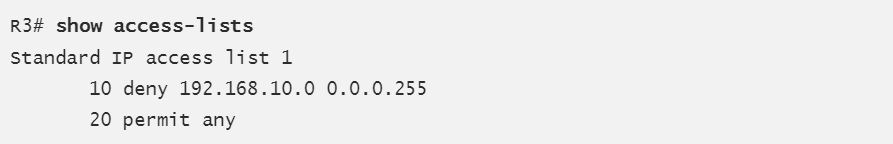
1. Ahora, se aplica una ACL estándar numerada en el **R3**, se crea con el número 1 que deniegue el acceso a la red 192.168.30.0/24 desde la red de la **PC1** (192.168.10.0/24).



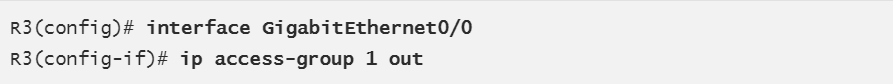
1. Se deniega de manera predeterminada todo el tráfico que no coincida con la regla.



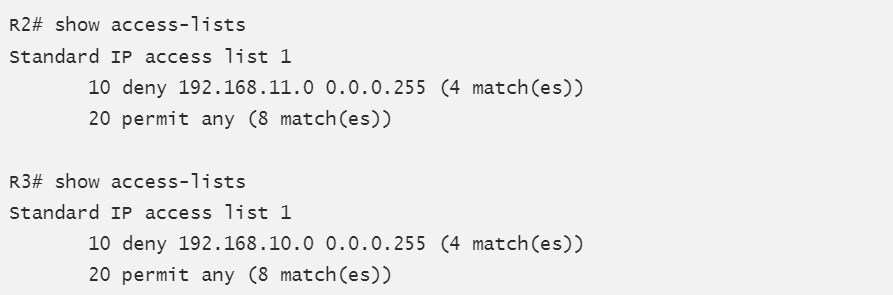
1. Se comprueba la lista antes de ejecutar el ACL.



1. Se coloca el ACL en el tráfico saliente de la **interfaz GigabitEthernet0/0**.



1. Aplicamos el comando **show run** en R2 y R3 para que se pueda aplicar la lista.
2. Se realizan los siguientes pings con los resultados que da:
   * Un ping de 192.168.10.10 a 192.168.11.10 se realiza correctamente.
   * Un ping de 192.168.10.10 a 192.168.20.254 se realiza correctamente.
   * Un ping de 192.168.11.10 a 192.168.20.254 falla.
   * Un ping de 192.168.10.10 a 192.168.30.10 falla.
   * Un ping de 192.168.11.10 a 192.168.30.10 se realiza correctamente.
   * Un ping de 192.168.30.10 a 192.168.20.254 se realiza correctamente.
3. Se detiene la lista para ejecutar el comando **show access-lists** de lo cuales muestra el numero de accesos que se han hecho tanto para el **R2** y **R3**.



1. En la segunda actividad, el punto es crear una ACL con nombre, lo cual configuramos el **R1** para eso con lo siguiente.



1. Utilizamos nuevamente el comando **show access-lists** para corroborar que estén correctas las direcciones IP.



1. Culminando lo anterior, nos dirigimos con el comando **interface FastEthernet0/1** y aplicamos el ACL.



1. Utilizamos el comando **show run** para ejecutar el ACL.
2. Las tres estaciones de trabajo deberían de poder hacer ping al **servidor web**, pero solo la **PC1** y el **servidor web** solo pueden hacer ping al **servidor de archivos**. Lo cual hacemos ping en todos los equipos y después validamos la lista para ver las peticiones que han hecho.

