SEGURIDAD EN NETWORKING

Unidad 2

Vulnerabilidades, procedimientos, acciones de mitigación y Controles de ISO 27001

ESCUELA DE INGENIERÍA Y CONSTRUCCIÓN

Director: Marcelo Lucero Yáñez

ELABORACIÓN

Experto disciplinar: Luis Ignacio Jaque

Diseñadora instruccional: Francisca Capponi

Editora instruccional: Francisca Aránguiz Jiménez

VALIDACIÓN

Experto disciplinar: Rodrigo Orellana Núñez

Jefa de Diseño Instruccional: Alejandra San Juan

EQUIPO DE DESARROLLO

Welearn

AÑO

2022

Tabla de contenidos

Aprendizaje esperado

Aplican listas de control de acceso de tipo IPv4 para implementaciones básicas de seguridad, según requerimientos de la empresa y estándares.

Introducción

Esta semana se realiza una revisión de las listas de acceso y de la configuración de ACL IPv4 estándar. junto con ello, se explica cómo configurar y solucionar problemas en las ACL IPv4 extendidas y ACL IPv6 en un router Cisco como parte de una solución de seguridad. Se incluyen consejos, consideraciones, recomendaciones y pautas generales sobre cómo utilizar las ACL.

Considerando la seguridad de las redes, el cómo y dónde se aplican las ACL IPv4 estándares nombradas y numeradas, al final de esta semana podrán responder a la pregunta ¿qué son las listas de acceso?

1. ACL IPv4 estándar y extendidas

Los dos tipos de ACL de IPv4 de Cisco son estándar y extendida.

Las ACL estándar se pueden utilizar para permitir o denegar el tráfico de direcciones IPv4 de origen únicamente. El destino del paquete y los puertos involucrados no se evalúan. En el ejemplo de la figura1, se permite todo el tráfico de la red 192.168.30.0/24. Debido a la instrucción implícita "*deny any*" al final, todo el tráfico, excepto el tráfico proveniente de la red 192.168.30.0/24, se bloquea con esta ACL. Las ACL estándar se crean en el modo de configuración global.

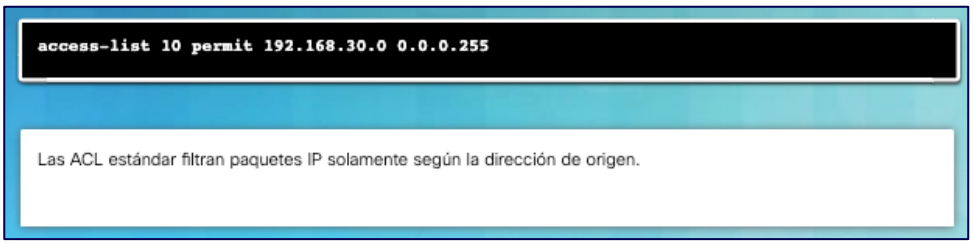


Figura 1: Listas ACL estándares.

Cisco Networking Academy (2022)

Las ACL extendidas filtran paquetes IPv4 según varios atributos:

- Tipo de protocolo
- Dirección IPv4 de origen
- Dirección IPv4 de destino
- Puertos TCP o UDP de origen
- Puertos TCP o UDP de destino
- Información optativa de tipo de protocolo para un control más preciso

En la figura2, la ACL103 permite el tráfico que se origina desde cualquier dirección en la red 192.168.30.0/24 hasta cualquier red IPv4 si el puerto de host de destino es 80 (HTTP). Las ACL extendidas se crean en el modo de configuración global.

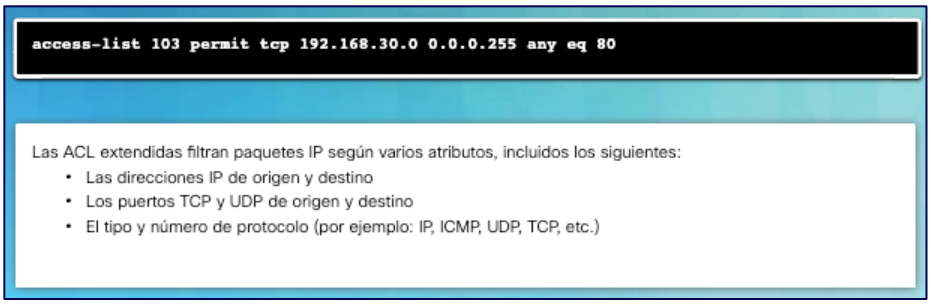


Figura 2: Listas ACL estándares.

Cisco Networking Academy (2022)

2. Listas ACL denominada y numeradas

Las ACL estándar y extendidas se pueden crear con un número o un nombre para identificar la ACL y su lista de instrucciones.

El uso de ACL numeradas es un método eficaz para determinar el tipo de ACL en redes más pequeñas con tráfico definido de forma más homogénea. Sin embargo, un número no proporciona información sobre el propósito de la ACL. Por este motivo, se puede usar un nombre para identificar una ACL de Cisco.

En la figura 3, se resumen las reglas que se deben seguir para designar las ACL numeradas y denominada.

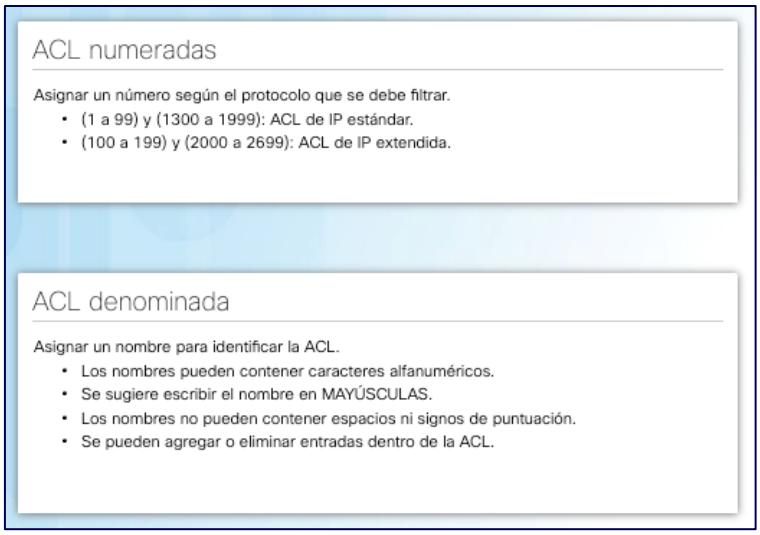


Figura 3: Numeración y denominación de las ACL.

Cisco Networking Academy (2022)

3. Dónde ubicar las ACL

Cada ACL se debe colocar donde tenga más impacto en la eficiencia. Como se muestra en la figura 4, las reglas básicas son las siguientes:

***Listas ACL extendidas*:** coloque las listas ACL extendidas lo más cerca posible del origen del tráfico que se filtrará. De esta manera, el tráfico no deseado se deniega cerca de la red de origen, sin que cruce la infraestructura de red.

***Listas ACL estándar*:** debido a que en las listas ACL estándar no se especifican las direcciones de destino, colóquelas tan cerca del destino como sea posible. Si una ACL estándar se ubicara en el origen del tráfico, la instrucción “permir” o “deny” se ejecutará según la dirección de origen determinada independientemente de adónde se dirige el tráfico.

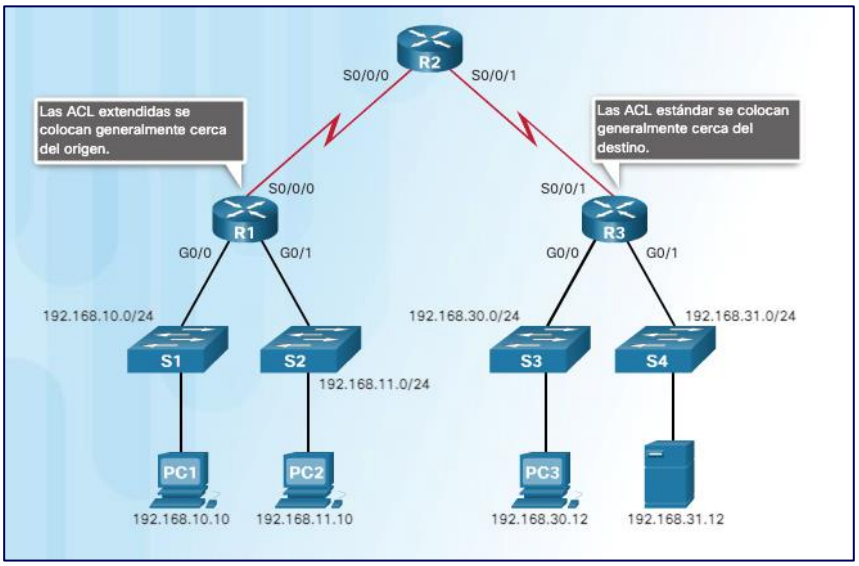


Figura 4: Ubicación de ACL.

Cisco Networking Academy (2022)

La ubicación de la ACL y, por lo tanto, el tipo de ACL que se utiliza también puede depender de diversos factores:

Alcance del control del administrador de la red: la colocación de la ACL puede depender de si el administrador de red controla tanto la red de origen como la de destino o no.

Ancho de banda de las redes involucradas: el filtrado del tráfico no deseado en el origen impide la transmisión de ese tráfico antes de que consuma ancho de banda en la ruta hacia un destino. Esto es de especial importancia en redes con un ancho de banda bajo.

Facilidad de configuración: si un administrador de red desea denegar el tráfico proveniente de varias redes, una opción es utilizar una única ACL estándar en el *router* más cercano al destino. La desventaja es que el tráfico de dichas redes utilizará ancho de banda de manera innecesaria. Se puede utilizar una ACL extendida en cada router donde se origina tráfico. Esto ahorra ancho de banda, ya que el tráfico se filtra en el origen, pero requiere la creación de ACL extendidas en varios *routers.*

3.1. Ejemplo de ubicación de una ACL estándar

En la figura 5, el administrador desea impedir que el tráfico que se origina en la red 192.168.10.0/24 llegue a la red 192.168.30.0/24.

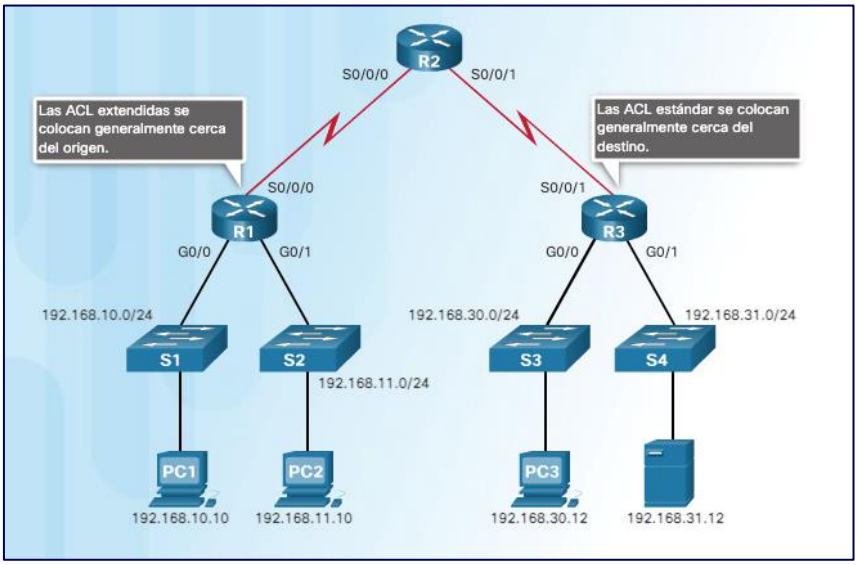


Figura 5: Ubicación de ACL estándar.

Cisco Networking Academy (2022)

Si la ACL estándar se coloca en la interfaz de salida del R1 (no se muestra en la figura), eso evitaría que el tráfico de la red 192.168.10.0/24 alcance cualquier red a la que se pueda llegar a través de la interfaz Serial 0/0/0 del R1.

De acuerdo con las pautas básicas de colocación de ACL estándar cerca del destino, en la ilustración se muestran dos interfaces posibles del R3 a las que aplicar la ACL estándar:

- ***Interfaz S0/0/1 del R3:*** la aplicación de una ACL estándar para impedir que el tráfico de 192.168.10.0/24 ingrese a la interfaz S0/0/1 evita que dicho tráfico llegue a 192.168.30.0/24 y al resto de las redes con las que se puede comunicar R3. Esto incluye la red 192.168.31.0/24. Dado que el objetivo de la ACL es filtrar el tráfico destinado solo a 192.168.30.0/24, no se debe aplicar una ACL estándar a esta interfaz.

- ***Interfaz G0/0 del R3***: al aplicar una ACL estándar al tráfico que sale por la interfaz G0/0, se filtran los paquetes que van de 192.168.10.0/24 a 192.168.30.0/24. Esto no afecta a las otras redes con las que se puede comunicar R3. Los paquetes de 192.168.10.0/24 aún pueden llegar a 192.168.31.0/24.

3.2. Ejemplo de ubicación de una ACL extendida

La regla básica para la colocación de una ACL extendida es colocarla lo más cerca posible del origen. Esto evita que el tráfico no deseado se envíe a través de varias redes y luego sea denegado cuando llegue a destino. Sin embargo, los administradores de red solo pueden colocar las listas ACL en los dispositivos que controlan. Por lo tanto, la colocación se debe determinar en el contexto de hasta dónde se extiende el control del administrador de red.

En la figura 6, el administrador de la empresa A, que incluye las redes 192.168.10.0/24 y 192.168.11.0/24 (conocidas como .10 y .11 en este ejemplo) desea controlar el tráfico hacia la empresa B. Específicamente, el administrador desea denegar el tráfico FTP y Telnet de la red .11 a la red 192.168.30.0/24 (.30, en este ejemplo) de la empresa B. Al mismo tiempo, se debe permitir que el resto del tráfico de la red .11 salga de la empresa A sin restricciones.

Existen varias formas de lograr estos objetivos. Una ACL extendida en el R3 que bloquee Telnet y FTP de la red.11 cumpliría el objetivo, pero el administrador no controla el R3. Además, esta solución también permite que el tráfico no deseado cruce toda la red y luego sea bloqueado en el destino. Esto afecta la eficacia general de la red.

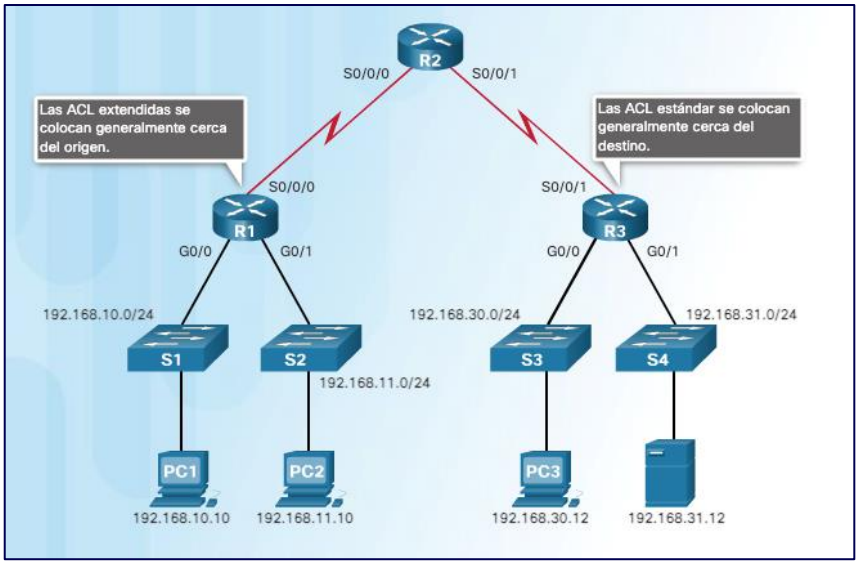


Figura 6: Ubicación de ACL extendida.

Cisco Networking Academy (2022)

Una mejor solución es colocar una ACL extendida en R1 que especifique tanto las direcciones de origen como las de destino (red .11 y red .30, respectivamente) y que aplique la regla “No se permite que el tráfico de Telnet y FTP de la red .11 vaya a la red .30”. La figura muestra dos interfaces en R1 en las que sería posible aplicar la ACL extendida:

- ***Interfaz S0/0/0 del R1 (de salida):*** una de las posibilidades es aplicar una ACL extendida de salida en la interfaz S0/0/0. Debido a que la ACL extendida puede examinar tanto la dirección de origen como la de destino, solo se deniegan los paquetes FTP y Telnet de 192.168.11.0/24, y el R1 reenvía el resto del tráfico de 192.168.11.0/24 y de otras redes. La desventaja de colocar la ACL extendida en esta interfaz es que la ACL debe procesar todo el tráfico que sale de S0/0/0, incluidos los paquetes de 192.168.10.0/24.

- ***Interfaz G0/1 del R1 (de entrada):*** la aplicación de una ACL extendida al tráfico que ingresa a la interfaz G0/1 implica que solamente los paquetes de la red 192.168.11.0/24 están sujetos al procesamiento de la ACL en R1. Debido a que el filtro se debe limitar solo a aquellos paquetes que salen de la red 192.168.11.0/24, la aplicación de una ACL extendida a G0/1 es la mejor solución.

4. Configurar ACL IPv4

La sintaxis completa del comando de ACL estándar es la siguiente:

Router(config)#access-listnúmero-cl{deny|permit|remark} origen[wildcard-origen] [log]

En la figura 7, se explica detalladamente la sintaxis para una ACL estándar.

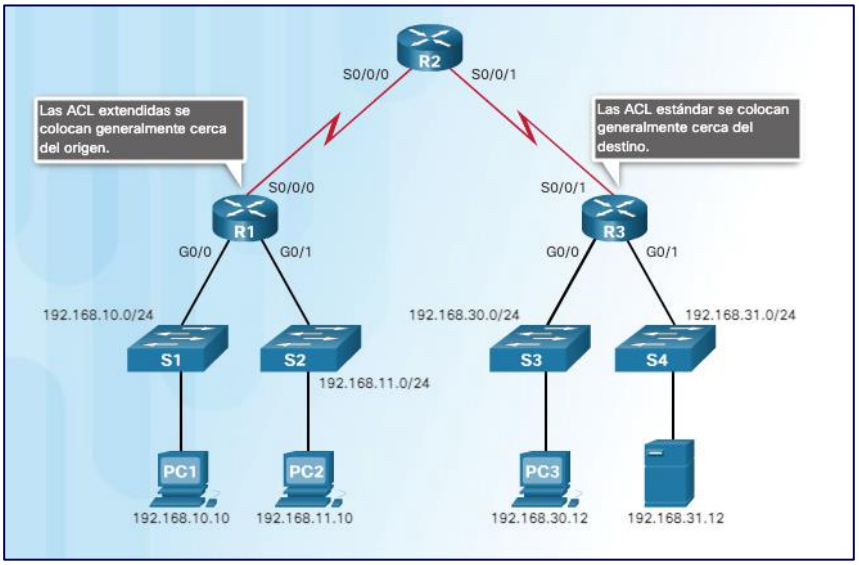


Figura 7: Sintaxis de comando de ACL estándar Access-list.

Cisco Networking Academy (2022)

Las ACE pueden permitir o denegar un solo host o un rango de direcciones host. Para crear una ACL numerada 10, que permita un host específico con la dirección IPv4 192.168.10.10, debe introducir lo siguiente:

R1(config)#*access-list 10 permit host 192.168.10.10*

Como se muestra en la figura 8, para crear una instrucción que permita un rango de direcciones IPv4 en una ACL numerada 10 que permite todas las direcciones IPv4 en la red 192.168.10.0/24, debe introducir lo siguiente:

R1(config)#*access-list 10 permit 192.168.10.0 0.0.0.255*

Figura 8: Eliminación de una ACL.

Cisco Networking Academy (2022)

Para eliminar la ACL, se utiliza el comando de configuración global **no access-list 10**. La ejecución del comando ***show access-list*** confirma que se eliminó la lista de acceso 10.

Como se muestra en la figura 9, se utiliza la palabra clave **remark** en los documentos, que facilita mucho comprender las listas de acceso. Cuando se revisa la ACL en la configuración mediante el comando ***show running-config***, también se muestra el comentario.

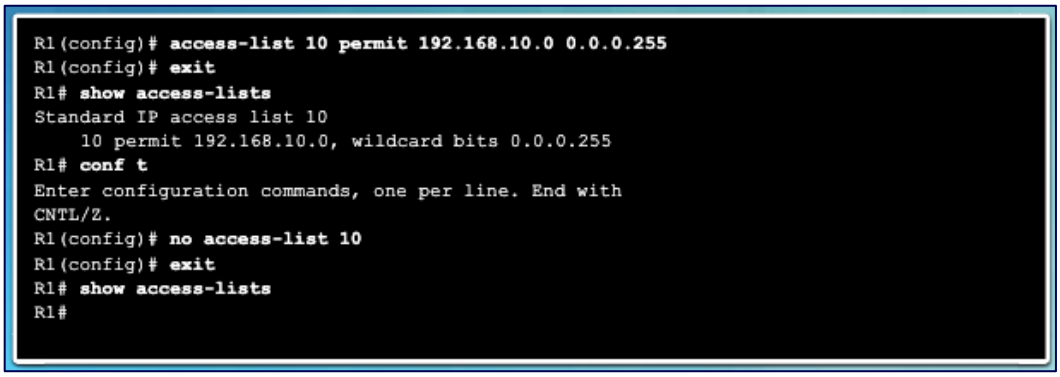


Figura 9: Uso de remark en una ACL.

Cisco Networking Academy (2022)

4.1. Aplicación de una ACL IPv4 estándar

Después de que se configura una ACL estándar IPv4, se vincula a una interfaz mediante el comando ***ip access-group*** en el modo de configuración de interfaz:

Router(config-if) # ***ip access-group*** {número-*acl* | *nombre-acl}* **{in** | **out}**

Para eliminar una ACL de una interfaz, primero introduzca el comando ***no ip access-group*** en la interfaz; luego, introduzca el comando global ***no access-list*** para eliminar toda la ACL.

La figura 10 muestra un ejemplo de una ACL diseñada para permitir una sola red. Solo el tráfico de la red 192.168.10.0/24 redes está permitido desde la interfaz serial 0/0/0.

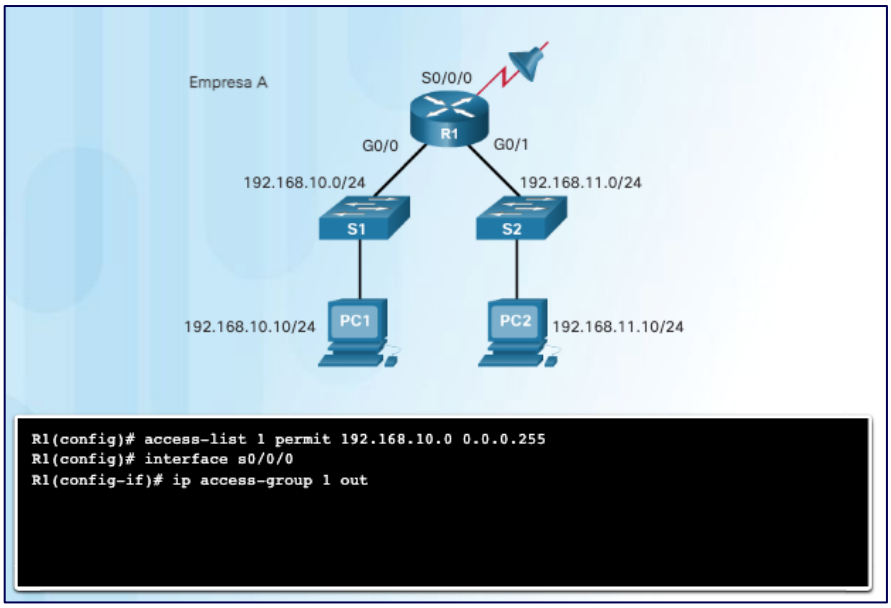


Figura 10: Admisión de una subred específica.

Cisco Networking Academy (2022)

4.2. Listas ACL IPv4 estándar denominada

En la figura 11, se muestran los pasos necesarios para crear una ACL estándar con nombre.

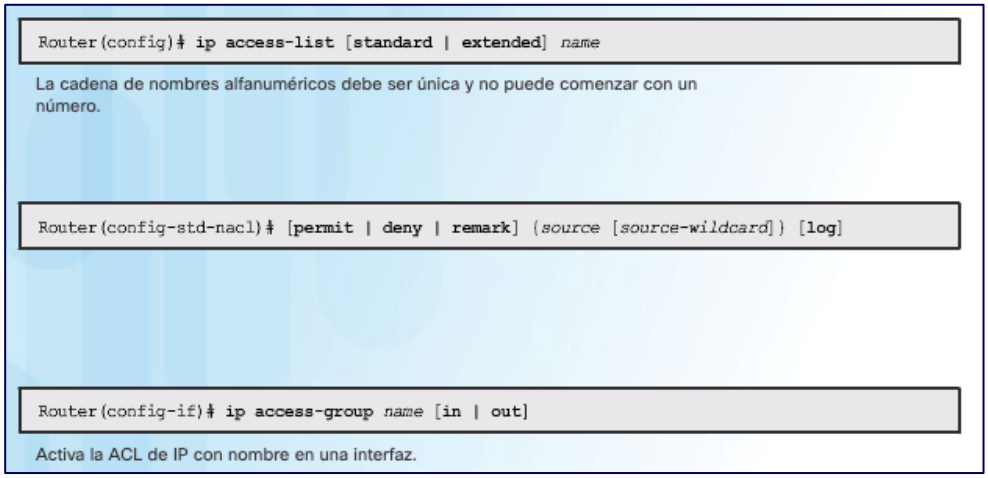


Figura 11: Ejemplo de ACL denominada.

Cisco Networking Academy (2022)

Paso 1: en el modo de configuración global, utilice el comando *ip access-list* para crear una ACL denominada. Los nombres de las ACL son alfanuméricos, distinguen mayúsculas de minúsculas y deben ser únicos. El comando de nombre *ip access-list standard* se usa para crear una con nombre estándar. Después de introducir el comando, el *router* se encuentra en el modo de configuración estándar (std) ACL denominada (nacl) como lo indica el segundo indicador en la Figura 11.

Paso 2: en el modo de configuración de ACL con nombre, utilice las instrucciones *permit o deny* a fin de especificar una o más condiciones para determinar si un paquete se reenvía o se descarta. Puede utilizar remark para agregar un comentario a la ACL.

Paso 3.: aplique la ACL a una interfaz con el comando *ip access-group*. nombre. Especifique si la ACL se debe aplicar a los paquetes cuando ingresan por la interfaz (in) o cuando salen de la interfaz (out).

La figura 12 muestra los comandos que se utilizan para configurar una ACL estándar denominada en el router R1, en la que la interfaz G0/0 deniega el acceso del host 192.168.11.10 a la red 192.168.10.0. La ACL se llama NO_ACCESS.

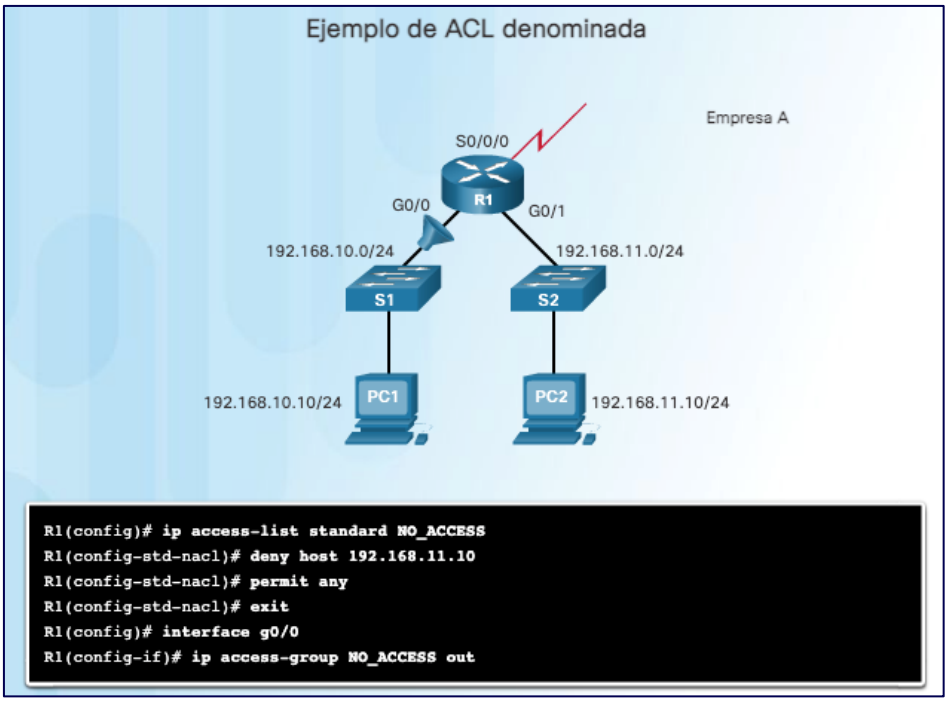


Figura 12: Ejemplo de ACL denominada.

Cisco Networking Academy (2022)

4.3. Verificación de listas ACL

Como se muestra en la figura 13, el comando ***show ip interface*** se utiliza para verificar la ACL en la interfaz. El resultado de este comando incluye el número o el nombre de la lista de acceso y el sentido en el que se aplicó la ACL. El resultado muestra que la lista de acceso 1 se aplica a la interfaz de salida S0/0/0 del router R1 y que la lista de acceso NO_ACCESS se aplica a la interfaz g0/0, también en sentido de salida.

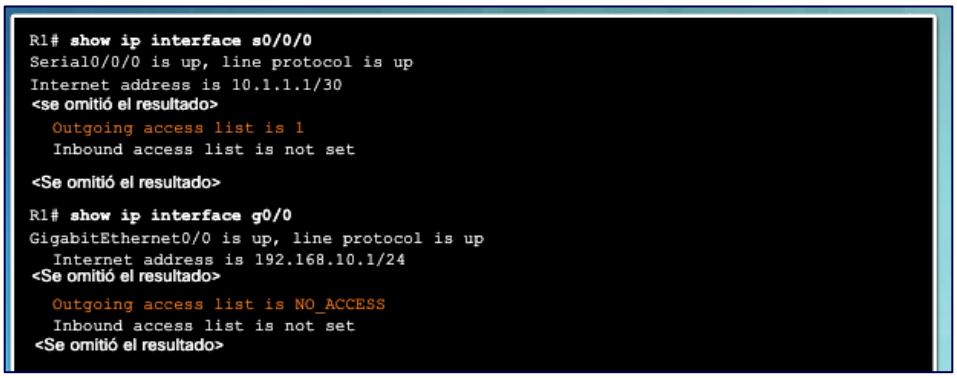


Figura 13: Verificación de interfaces de ACL estándar.

Cisco Networking Academy (2022)

En el ejemplo de la figura 14, se muestra el resultado de emitir el comando ***show access-lists*** en el router R1. Para ver una lista de acceso individual, utilice el comando ***show access-lists*** seguido del número o el nombre de la lista de acceso. Es posible que las instrucciones de NO_ACCESS se vean extrañas. Observe que el número de secuencia 15 se muestra antes que el número de secuencia 10. Esto se debe al proceso interno del router y se analizará más adelante en esta sección.

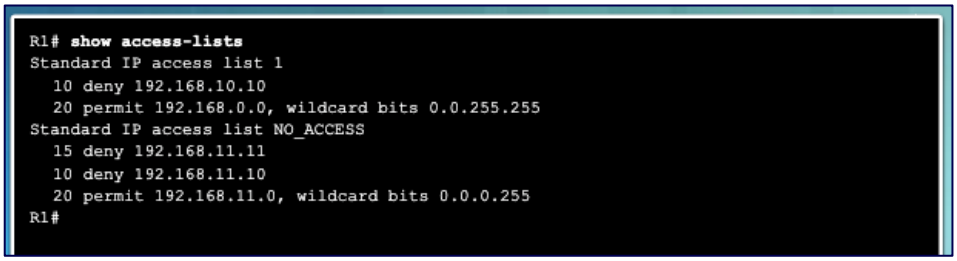


Figura 14: Verificación de instrucciones de ACL estándar.

Cisco Networking Academy (2022)

4.4. Listas ACL extendidas

Para un control más preciso del filtrado del tráfico, se pueden crear ACL de IPv4 extendidas. Las ACL extendidas se numeran del 100 al 199 y del 2000 a 2699, lo que da un total de 799 ACL extendidas numeradas posibles. Las ACL extendidas también pueden tener nombre.

Las ACL extendidas se utilizan con más frecuencia que las ACL estándar, porque proporcionan un mayor grado de control. Como se muestra en la figura 15, al igual que las ACL estándar, las ACL extendidas tienen la capacidad para revisar las direcciones de origen de los paquetes, pero también pueden revisar la dirección de destino, los protocolos y los números de puerto (o servicios). Esto proporciona una gama de criterios más amplia sobre la cual basar la ACL. Por ejemplo, una ACL extendida puede permitir el tráfico de correo electrónico de una red a un destino específico y, simultáneamente, denegar la transferencia de archivos y la navegación web.

4.5. Filtrado de puertos y servicios

Figura 15: Listas ACL extendidas.

Fuente: Cisco Networking Academy (2022)

La capacidad de filtrar por protocolos y números de puerto permite que los administradores de red creen ACL extendidas muy específicas. Se puede especificar una aplicación mediante la configuración del número o el nombre de un puerto bien conocido.

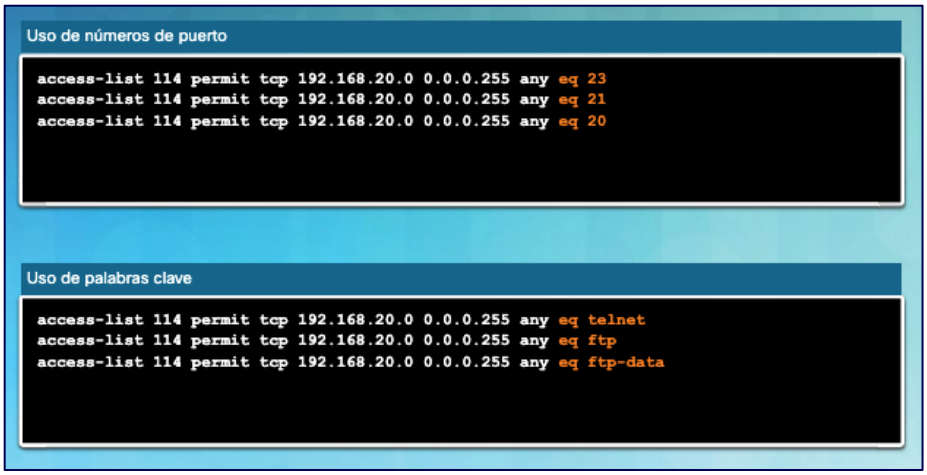


Figura 16: Ejemplos de ACL extendidas.

Fuente: Cisco Networking Academy (2022)

En la figura 16, se muestran algunos ejemplos de la forma en que un administrador especifica un número de puerto TCP o UDP colocándolo al final de la instrucción de la ACL extendida. Se pueden utilizar operaciones lógicas, por ejemplo, igual que (eq), distinto de (neq), mayor que (gt) y menor que (lt).

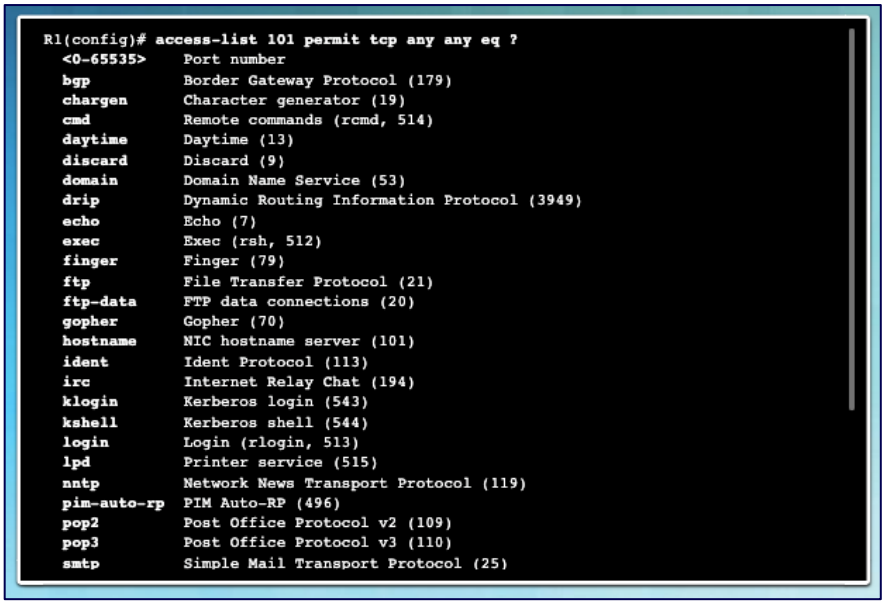


Figura 17: Generación de números de puerto.

Fuente: Cisco Networking Academy (2022)

En la figura 17, se muestra cómo visualizar una lista de números de puerto y de palabras clave que pueden utilizarse al generar una ACL mediante el siguiente comando:

R1(config)# ***access-list 101 permit tcp any any eq?***

4.6. Configurar las ACL extendidas

Los pasos del procedimiento para configurar ACL extendidas son los mismos que para las ACL estándar. Primero se configura la ACL extendida y, a continuación, se activa en una interfaz. Sin embargo, la sintaxis de los comandos y los parámetros son más complejos, a fin de admitir las funciones adicionales proporcionadas por las ACL extendidas.

Nota: La lógica interna aplicada al ordenamiento de las instrucciones de las ACL estándar no se aplica a las ACL extendidas. El orden en que se introducen las instrucciones durante la configuración es el orden en que se muestran y se procesan.

En la figura 18, se muestra la sintaxis frecuente de los comandos para las ACL de IPv4 extendidas. Observe que hay muchas palabras clave y parámetros para las ACL extendidas. No es necesario utilizar todas las palabras clave y todos los parámetros al configurar una ACL extendida. Recuerde que puede usar "**?**" para obtener ayuda al introducir comandos complejos.

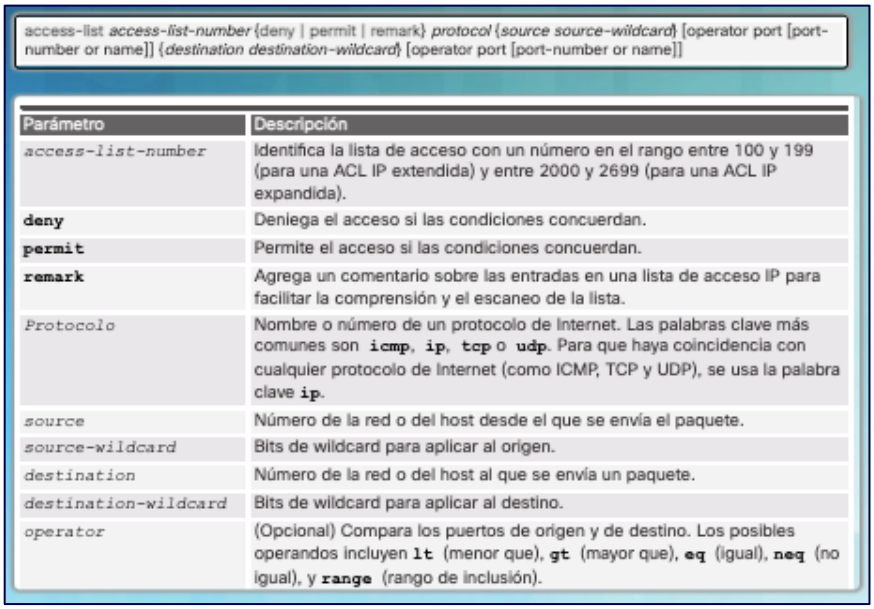


Figura 18: Configurar ACL extendidas.

Fuente: Cisco Networking Academy (2022)

En la figura 19, se muestra un ejemplo de una ACL extendida. En este ejemplo, el administrador de red configuró las ACL para restringir el acceso de red a fin de permitir la navegación de sitios web solo desde la LAN conectada a la interfaz G0/0 a cualquier red externa. La ACL 103 permite que el tráfico proveniente de cualquier dirección en la red 192.168.10.0 vaya a cualquier destino, sujeto a la limitación de que el tráfico utilice solo los puertos 80 (HTTP) y 443 (HTTPS).

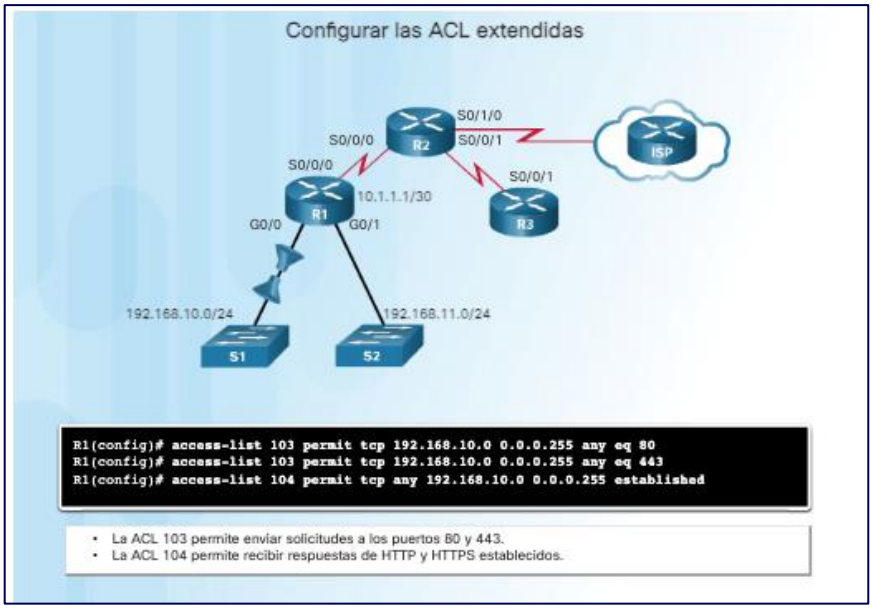


Figura 19: Configurar ACL extendidas.

Fuente: Cisco Networking Academy (2022)

La naturaleza de HTTP requiere que el tráfico fluya nuevamente hacia la red desde los sitios web a los que se accede mediante clientes internos. El administrador de red desea restringir ese tráfico de retorno a los intercambios HTTP de los sitios web solicitados y denegar el resto del tráfico. La ACL 104 logra esto mediante el bloqueo de todo el tráfico entrante, excepto las conexiones establecidas previamente. La instrucción “permit” en la ACL 104 permite el tráfico entrante con el parámetro ***established***.

El parámetro ***established*** permite que solo las respuestas al tráfico procedente de la red 192.168.10.0/24 vuelvan a esa red. Si el segmento TCP que regresa tiene los bits ACK o de restablecimiento (RST) establecidos, que indican que el paquete pertenece a una conexión existente, se produce una coincidencia. Sin el parámetro *established* en la instrucción de ACL, los clientes pueden enviar tráfico a un servidor web, pero no recibir el tráfico que vuelve de dicho servidor.

4.7. Aplicación de ACL extendidas a las interfaces

En el ejemplo anterior, el administrador de red configuró una ACL para permitir que los usuarios de la red 192.168.10.0/24 exploren sitios web seguros e inseguros. Aunque se configuró, la ACL no filtrará el tráfico hasta que se aplique a una interfaz. Para aplicar una ACL a una interfaz, primero debe considerar si el tráfico que se filtrará es entrante o saliente. Cuando un usuario de la LAN interna accede a un sitio web en Internet, hay tráfico que sale hacia Internet. Cuando un usuario interno recibe un correo electrónico de Internet, el tráfico ingresa al router local. Sin embargo, cuando se aplica una ACL a una interfaz, los términos “entrada” y “salida” tienen otros significados. Desde el punto de vista de una ACL, la entrada y salida son respecto de la interfaz del router.

En la topología de la figura 20, el R1 tiene tres interfaces: una interfaz serial, S0/0/0, y dos interfaces Gigabit Ethernet, G0/0 y G0/1. Recuerde que una ACL extendida comúnmente se debería aplicar cerca del origen. En esta topología, la interfaz más cercana al origen del tráfico de destino es la interfaz G0/0.

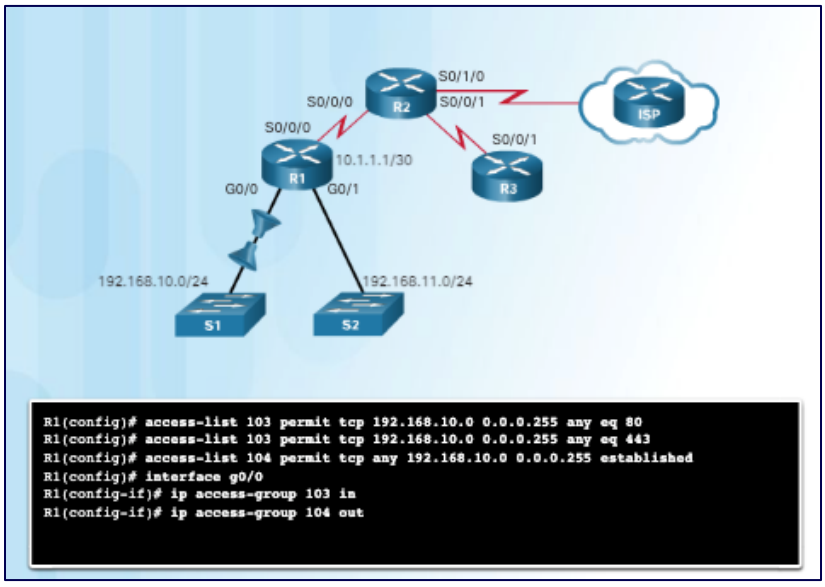


Figura 20: Cómo aplicar una ACL a una interfaz.

Fuente: Cisco Networking Academy (2022)

La solicitud de tráfico web de los usuarios en la LAN 192.168.10.0/24 entra a la interfaz G0/0. El tráfico de retorno de las conexiones establecidas a los usuarios en la LAN sale de la interfaz G0/0. En el ejemplo, se aplica la ACL a la interfaz G0/0 en ambos sentidos. La ACL de entrada, 103, revisa el tipo de tráfico. La ACL de salida, 104, revisa si hay tráfico de retorno de las conexiones establecidas. Esto restringe el acceso a Internet desde 192.168.10.0 para permitir solamente la navegación de sitios web.

Nota: las listas de acceso se podrían haber aplicado a la interfaz S0/0/0, pero en ese caso el proceso de ACL del *router* tendría que examinar todos los paquetes que ingresan al *router* y no solo el tráfico que va hacia 192.168.11.0 y que vuelve de esa red. Esto provocaría que el router realice un procesamiento innecesario.

4.8. Filtrado de tráfico con ACL extendidas

En el ejemplo que se muestra en la figura 21, se deniega el tráfico FTP de la subred 192.168.11.0 que va a la subred 192.168.10.0, pero se permite el resto del tráfico. Recuerde que FTP utiliza los puertos TCP 20 y 21, por lo tanto, la ACL requiere ambas palabras claves de nombre de puerto **ftp** y **ftp-data** o **eq 20** y **eq 21** para denegar el tráfico FTP.

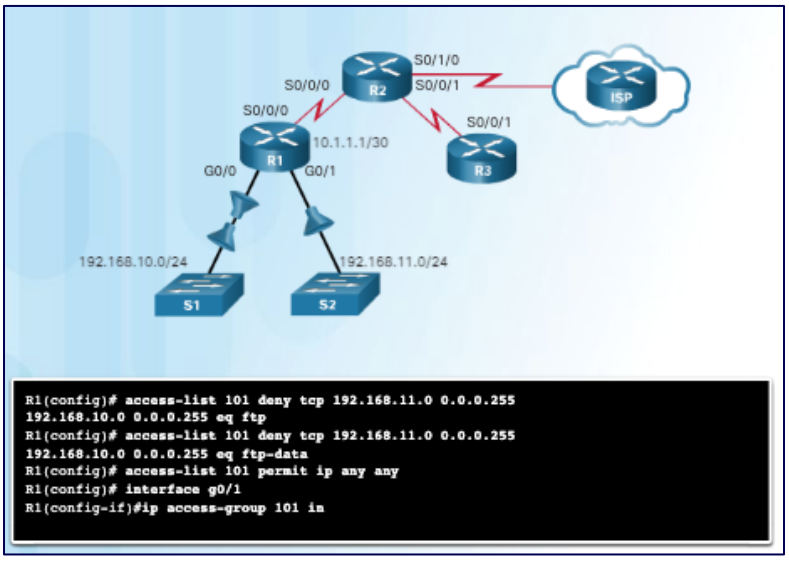


Figura 21: ACL extendida para denegar Telnet.

Fuente: Cisco Networking Academy (2022)

Si se utilizan números de puerto en vez de nombres de puerto, los comandos se deben escribir de la siguiente forma:

access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0 0.0.0.255 eq 20

access-list 101 deny tcp 192.168.11.0 0.0.0.255 192.168.10.0 0.0.0.255 eq 21

Para evitar que la instrucción ***deny any*** implícita al final de la ACL bloquee todo el tráfico, se agrega la instrucción ***permit ip any any***. Si no hay por lo menos una instrucción ***permit*** en una ACL, todo el tráfico en la interfaz donde se aplicó esa ACL se descarta. La ACL se debe aplicar en sentido de entrada en la interfaz G0/1 para filtrar el tráfico de la LAN 192.168.11.0/24 cuando ingresa a la interfaz del *router*.

En el ejemplo que se muestra en la figura 22, se deniega el tráfico de Telnet de cualquier origen a la LAN 192.168.11.0/24, pero se permite el resto del tráfico IP. Debido a que el tráfico destinado a la LAN 192.168.11.0/24 sale de la interfaz G0/1, la ACL se aplica a G0/1 con la palabra clave ***out***. Observe el uso de las palabras clave **any** en la instrucción permit. Esta instrucción permit se agrega para asegurar que no se bloquee ningún otro tipo de tráfico.

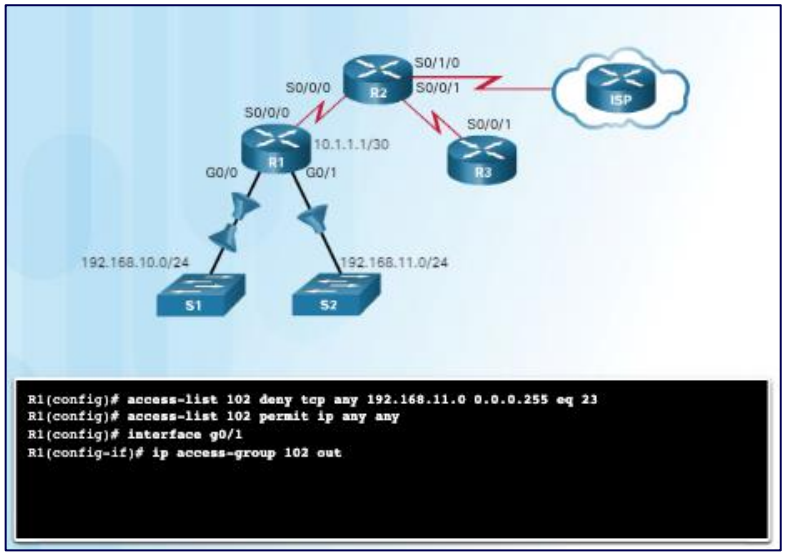


Figura 22: ACL extendida para denegar FTP.

Fuente: Cisco Networking Academy (2022)

Nota: en ambos ejemplos en las figuras 21 y 22, se utiliza la instrucción ***permit ip any any*** al final de la ACL. Para obtener mayor seguridad, se puede utilizar el comando **permit 192.168.11.0 0.0.0.255 any**.

4.9. Creación de ACL extendidas denominada

Las ACL extendidas denominada se crean esencialmente de la misma forma que las ACL estándar denominada. Para crear una ACL extendida denominada, realice los siguientes pasos:

Paso 1: desde el modo de configuración global, utilice el comando ***ip access-list extended*** se para definir un nombre para la ACL extendida.

Paso 2: en el modo de configuración de ACL denominada, especifique las condiciones para ***permit*** o ***deny***.

Paso 3: desde el modo de configuración de interfaces, aplique la ACL denominada con el comando **ip access-group** [**in** | **ou**t] *nombre*.

Paso 4: vuelva al modo EXEC con privilegios y verifique la ACL con el comando ***show access-lists*** nombre.

Paso 5: guarde las entradas en el archivo de configuración mediante el comando ***copy running-config startup-config***.

Para eliminar una ACL extendida denominada, utilice el comando de configuración global ***no ip access-list extended***.

En la figura 23, se muestran las versiones denominadas de las ACL creadas en los ejemplos anteriores. La ACL denominada SURFING permite que los usuarios en la LAN 192.168.10.0/24 accedan a sitios web. La ACL denominada BROWSING permite el tráfico de retorno de las conexiones establecidas. Cuando se utilizan las ACL denominada, las reglas se aplican en sentido de entrada y de salida en la interfaz G0/0.

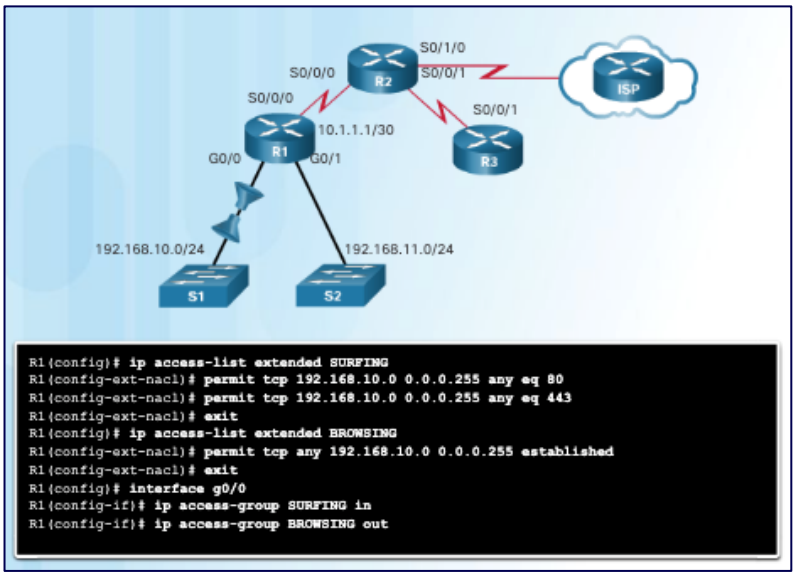


Figura 23: Creación de ACL extendidas con nombre.

Fuente: Cisco Networking Academy (2022)

4.10. Verificación de ACL extendidas

Después de configurar una ACL y aplicarla a una interfaz, utilice los comandos ***show*** del IOS de Cisco para verificar la configuración. En la figura 24, en el ejemplo de arriba se muestra el comando del IOS de Cisco que se utiliza para mostrar el contenido de todas las ACL. En el ejemplo de abajo, se muestra el resultado de emitir el comando ***show ip interface g0/0*** en el *router* R1.

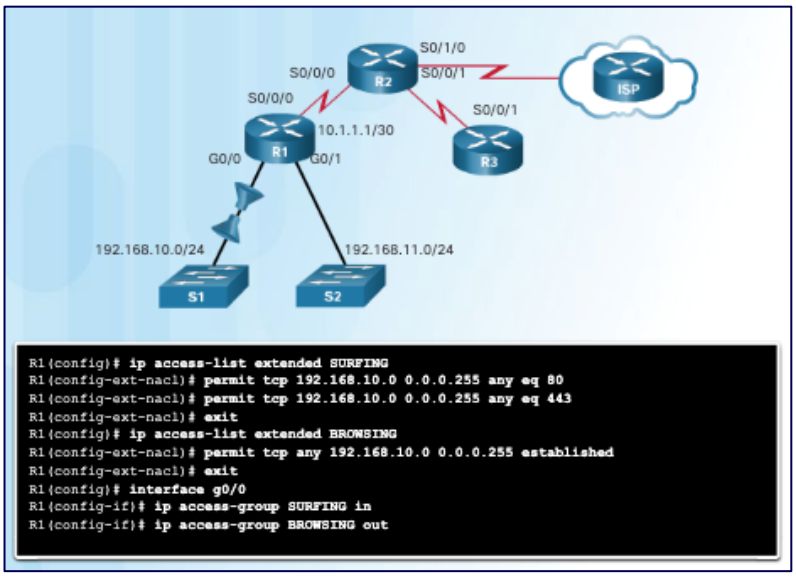


Figura 24: Verificación de ACL extendidas.

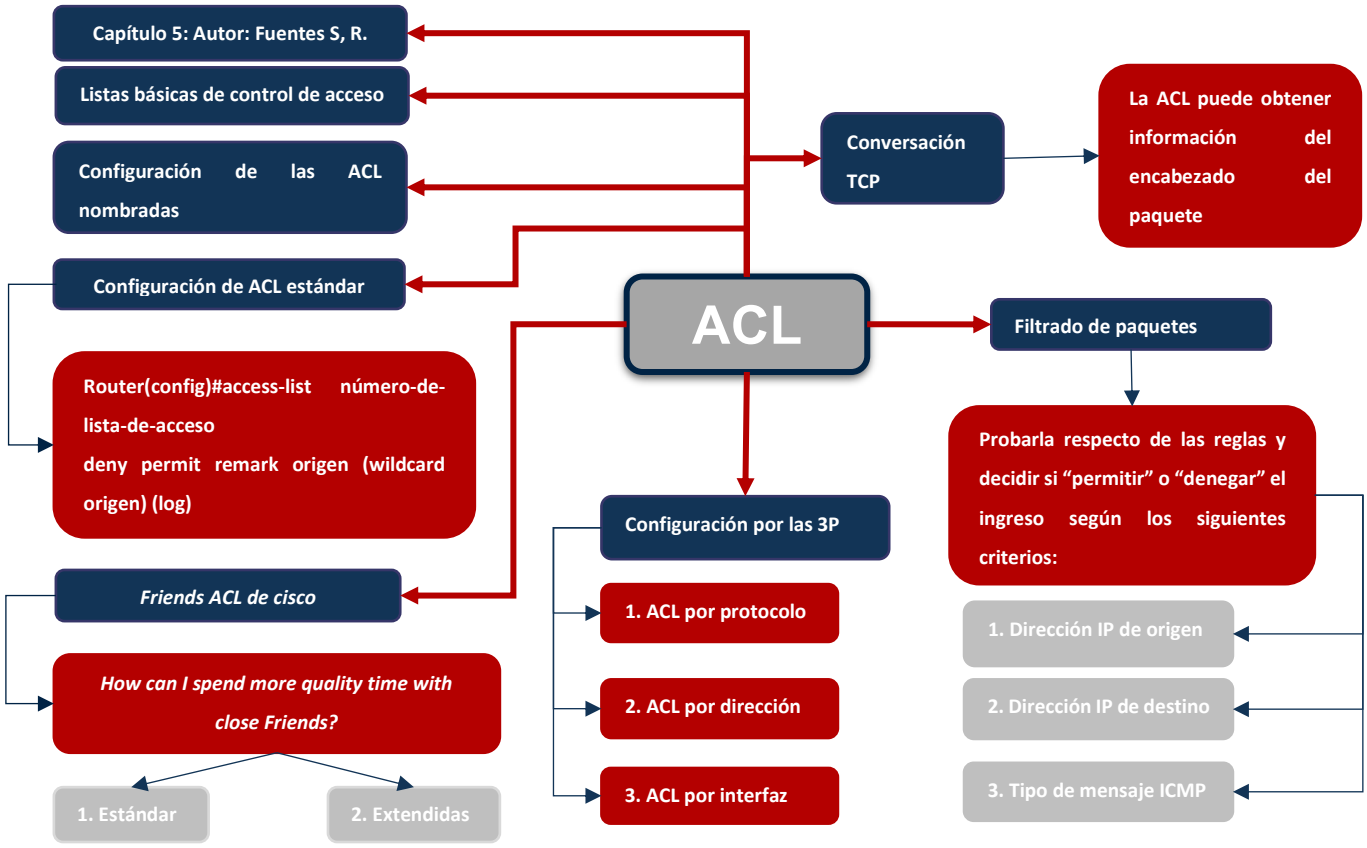
Cisco Networking Academy (2022)

A diferencia de las ACL estándar, las ACL extendidas no implementan la misma lógica interna ni la misma función de hash. El resultado y los números de secuencia que se muestran en el resultado del comando ***show access-lists*** están en el orden en que se introdujeron las instrucciones. Las entradas de host no se enumeran automáticamente antes de las entradas de rango.

El comando ***show ip interface*** se utiliza para verificar la ACL en la interfaz y el sentido en el que se aplicó. El resultado de este comando incluye el número o el nombre de la lista de acceso y el sentido en el que se aplicó la ACL. Los nombres de las ACL BROWSING y SURFING en mayúscula se destacan en el resultado que se ve en la pantalla.

Después de verificar la configuración de una ACL, el siguiente paso es confirmar que la ACL funcione según lo esperado, es decir, que bloquee y permita el tráfico según se espera.

Cierre



Mapa mental 1: Mapa mental de Tipos de Listas de Acceso.

Fuente: Elaboración propia

Referencias bibliográficas

- Cisco Networking Academy (2022). *Conexión de redes. Capítulo 4 – Listas de Control de acceso.* https://bit.ly/3vzi7lQ

- Cisco Networking Academy (2022). *Principios básicos de routing y switching. Capítulo 7 – Listas de Control de acceso*. https://bit.ly/3vzi7lQ