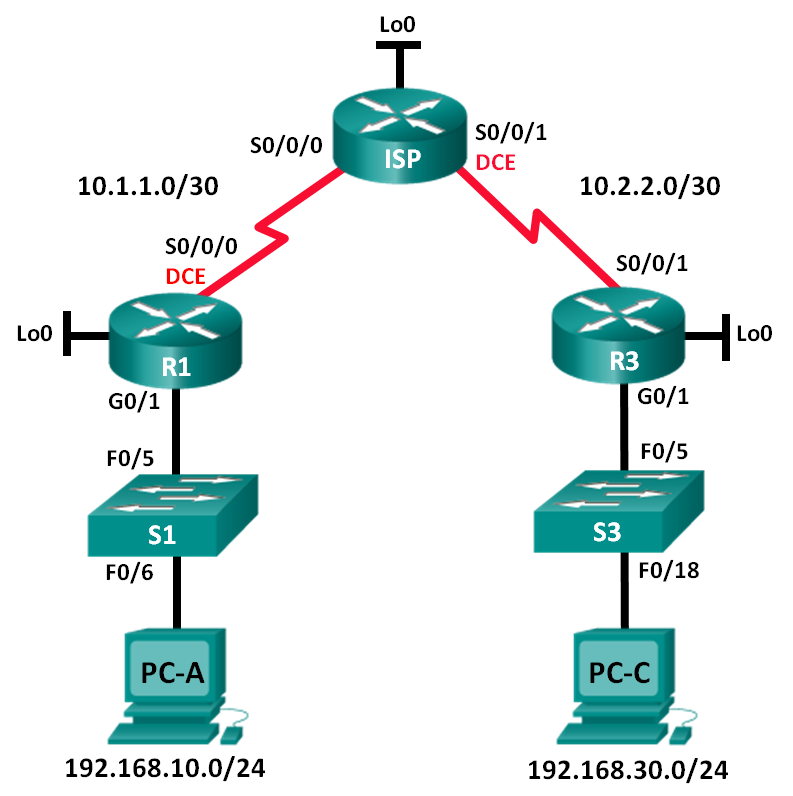
Configuración y verificación de ACL IPv4 estándar



1. Objetivos

Configurar y verificar ACL estándar numeradas y con nombre

* Configurar, aplicar y verificar una ACL estándar numerada.
* Configurar, aplicar y verificar una ACL con nombre.
* Probar la ACL.

1. Aspectos básicos/situación

La seguridad de red es una cuestión importante al diseñar y administrar redes IP. La capacidad para configurar reglas apropiadas para filtrar los paquetes, sobre la base de las políticas de seguridad establecidas, es una aptitud valiosa.

En esta práctica de laboratorio, establecerá reglas de filtrado para dos oficinas representadas por el R1 y el R3. La administración estableció algunas políticas de acceso entre las redes LAN ubicadas en el R1 y el R3, que usted debe implementar. El router ISP que se ubica entre el R1 y el R3 no tendrá ninguna ACL. Usted no tiene permitido el acceso administrativo al router ISP, debido a que solo puede controlar y administrar sus propios equipos.

1. Tabla de asignación de direcciones

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Dispositivo | Interfaz | Dirección IP | Máscara de subred | Gateway predeterminado |
| R1 | G0/1 | 192.168.10.1 | 255.255.255.0 | N/D |
|  | Lo0 | 192.168.20.1 | 255.255.255.0 | N/D |
|  | S0/0/0 (DCE) | 10.1.1.1 | 255.255.255.252 | N/D |
| ISP | S0/0/0 | 10.1.1.2 | 255.255.255.252 | N/D |
|  | S0/0/1 (DCE) | 10.2.2.2 | 255.255.255.252 | N/D |
|  | Lo0 | 209.165.200.225 | 255.255.255.224 | N/D |
| R3 | G0/1 | 192.168.30.1 | 255.255.255.0 | N/D |
|  | Lo0 | 192.168.40.1 | 255.255.255.0 | N/D |
|  | S0/0/1 | 10.2.2.1 | 255.255.255.252 | N/D |
| S1 | VLAN 1 | 192.168.10.11 | 255.255.255.0 | 192.168.10.1 |
| S3 | VLAN 1 | 192.168.30.11 | 255.255.255.0 | 192.168.30.1 |
| PC-A | NIC | 192.168.10.3 | 255.255.255.0 | 192.168.10.1 |
| PC-C | NIC | 192.168.30.3 | 255.255.255.0 | 192.168.30.1 |

Parte 1: Configurar y verificar ACLs estándar numeradas

Paso 1. Verificar la conectividad entre los dispositivos

**Nota:** Es muy importante probar si la conectividad funciona **antes** de configurar y aplicar listas de acceso. Tiene que asegurarse de que la red funcione adecuadamente antes de empezar a filtrar el tráfico.

* + 1. Desde la PC-A, haga ping a la PC-C y a la interfaz loopback en el R3.
    2. Desde el R1, haga ping a la PC-C y a la interfaz loopback en el R3.
    3. Desde la PC-C, haga ping a la PC-A y a la interfaz loopback en el R1.
    4. Desde el R3, haga ping a la PC-A y a la interfaz loopback en el R1.

Paso 2. Configurar una ACL estándar numerada

Las ACL estándar filtran el tráfico únicamente sobre la base de la dirección IP de origen. Una práctica recomendada típica para las ACL estándar es configurarlas y aplicarlas lo más cerca posible del destino. Para la primera lista de acceso, cree una ACL estándar numerada que permita que el tráfico proveniente de todos los hosts en la red 192.168.10.0/24 y de todos los hosts en la red 192.168.20.0/24 acceda a todos los hosts en la red 192.168.30.0/24. La política de seguridad también indica que debe haber una entrada de control de acceso (ACE) **deny any**, también conocida como “instrucción de ACL”, al final de todas las ACL.

Según las mejores prácticas recomendadas por Cisco, ¿en qué router colocaría esta ACL? \_\_\_\_\_\_\_\_\_\_\_

¿En qué interfaz colocaría esta ACL? ¿En qué sentido la aplicaría?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

G0/1. La ACL debe aplicarse en sentido de salida. Los estudiantes pueden responder colocando la ACL en la interfaz S0/0/1 en R3 en la dirección de **entrada**. Destaque que esto también impediría con eficacia que las LAN en R1 lleguen a la red 192.168.40.0/24.

* + 1. Configure la ACL en el R3. Use 1 como el número de lista de acceso.

R3(config)# **access-list 1 remark Allow R1 LANs Access**

R3(config)# **access-list 1 permit 192.168.10.0 0.0.0.255**

R3(config)# **access-list 1 permit 192.168.20.0 0.0.0.255**

R3(config)# **access-list 1 deny any**

* + 1. Aplique la ACL a la interfaz apropiada en el sentido correcto.

R3(config)# **interface g0/1**

R3(config-if)# **ip access-group 1 out**

* + 1. Verifique una ACL numerada.

El uso de diversos comandos **show** puede ayudarle a verificar la sintaxis y la colocación de las ACL en el router.

¿Qué comando usaría para ver la lista de acceso 1 en su totalidad, con todas las ACE?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

R3# **show access-lists 1**

o

R3# **show access-lists**

¿Qué comando usaría para ver dónde se aplicó la lista de acceso y en qué sentido?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

R3# **show ip interface g0/1**

o

R3# **show ip interface**

* + - 1. En el R3, emita el comando **show access-lists 1**.

R3# **show** **access-list 1**

Lista de acceso IP estándar 1

10 permit 192.168.10.0, wildcard bits 0.0.0.255

20 permit 192.168.20.0, wildcard bits 0.0.0.255

30 deny any

* + - 1. En el R3, emita el comando **show ip interface g0/1**.

R3# **show ip interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

Internet address is 192.168.30.1/24

Broadcast address is 255.255.255.255

Address determined by non-volatile memory

MTU is 1500 bytes

Helper address is not set

Directed broadcast forwarding is disabled

Multicast reserved groups joined: 224.0.0.10

Outgoing access list is 1

Inbound access list is not set

Resultado omitido

* + - 1. Pruebe la ACL para ver si permite que el tráfico de la red 192.168.10.0/24 acceda a la red 192.168.30.0/24. Desde la PC-A, haga ping a la dirección IP de la PC-C. ¿Fueron correctos los pings? \_\_\_\_\_\_\_ Sí
      2. Pruebe la ACL para ver si permite que el tráfico de la red 192.168.20.0/24 acceda a la red 192.168.30.0/24. Debe hacer un ping extendido y usar la dirección loopback 0 en el R1 como origen. Haga ping a la dirección IP de la PC-C. ¿Fueron correctos los pings? \_\_\_\_\_\_\_ Sí

R1# **ping**

Protocol [ip]:

Target IP address: **192.168.30.3**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: **y**

Source address or interface: **192.168.20.1**

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.30.3, timeout is 2 seconds:

Packet sent with a source address of 192.168.20.1

!!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 28/29/32 ms

* + 1. Desde la petición de entrada del R1, vuelva a hacer ping a la dirección IP de la PC-C.

R1# **ping 192.168.30.3**

¿El ping se realizó correctamente? ¿Por qué o por qué no?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

No, los pings fallaron. Cuando hace ping desde el router, este usa la interfaz más cercana al destino como la dirección de origen. La dirección de origen de los pings era 10.1.1.1. La lista de acceso en el R3 solo permite el acceso de las redes 192.168.10.0/24 y 192.168.20.0/24.

Parte 2: Configurar y verificar ACL estándar con nombre

Paso 1. Configurar una ACL estándar con nombre

Cree una ACL estándar con nombre que se ajuste a la siguiente política: permitir que el tráfico de todos los hosts en la red 192.168.40.0/24 tenga acceso a todos los hosts en la red 192.168.10.0/24. Además, solo debe permitir el acceso del host PC-C a la red 192.168.10.0/24. El nombre de esta lista de acceso debe ser BRANCH-OFFICE-POLICY.

Según las mejores prácticas recomendadas por Cisco, ¿en qué router colocaría esta ACL? \_\_\_\_\_\_\_\_\_\_\_ R1

¿En qué interfaz colocaría esta ACL? ¿En qué sentido la aplicaría?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

G0/1. La ACL debe aplicarse en sentido de salida. Los estudiantes pueden responder colocando la ACL en la interfaz S0/0/0 en R1 en la dirección de entrada. Destaque que esto también impediría con eficacia que todo el tráfico de las LAN en R3 lleguen a la red 192.168.20.0/24.

* + 1. Cree la ACL estándar con nombre BRANCH-OFFICE-POLICY en el R1.

R1(config)# **ip access-list standard BRANCH-OFFICE-POLICY**

R1(config-std-nacl)# **permit host 192.168.30.3**

R1(config-std-nacl)# **permit 192.168.40.0 0.0.0.255**

R1(config-std-nacl)# **end**

R1#

\*Feb 15 15:56:55.707: %SYS-5-CONFIG\_I: Configured from console by console

Observe la primera ACE permit en la lista de acceso. ¿Cuál sería otra forma de escribir esto?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

R1(config-std-nacl)# **permit 192.168.30.3 0.0.0.0**

* + 1. Aplique la ACL a la interfaz apropiada en el sentido correcto.

R1# **config t**

R1(config)# **interface g0/1**

R1(config-if)# **ip access-group BRANCH-OFFICE-POLICY out**

* + 1. Verifique una ACL con nombre.
       1. En el R1, emita el comando **show access-lists**.

R1# **show** **access-lists**

Standard IP access list BRANCH-OFFICE-POLICY

10 permit 192.168.30.3

20 permit 192.168.40.0, wildcard bits 0.0.0.255

¿Hay alguna diferencia entre esta ACL en el R1 y la ACL en el R3? Si es así, ¿cuál es?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Aunque no hay una línea 30 con **deny any** en el R1, la instrucción está implícita. Quizá desee hacer énfasis en esto. Es aconsejable que configuren realmente la ACE **deny any**, ya que esto refuerza el concepto debido a que aparece en la ACL cuando se emite un comando **show access-lists**. Es fácil olvidar la instrucción **deny any** implícita cuando se resuelven problemas en las ACL. Esto podría provocar que se deniegue el tráfico que se debería haber permitido.

* + - 1. En el R1, emita el comando **show ip interface g0/1**.

R1# **show ip interface g0/1**

GigabitEthernet0/1 is up, line protocol is up

Internet address is 192.168.10.1/24

Broadcast address is 255.255.255.255

Address determined by non-volatile memory

MTU is 1500 bytes

Helper address is not set

Directed broadcast forwarding is disabled

Multicast reserved groups joined: 224.0.0.10

Outgoing access list is BRANCH-OFFICE-POLICY

Inbound access list is not set

<Resultado omitido>

* + - 1. Probar la ACL. Desde el símbolo del sistema en la PC-C, haga ping a la dirección IP de la PC-A. ¿Fueron correctos los pings? \_\_\_\_\_\_\_
      2. Pruebe la ACL para asegurarse de que solo el host PC-C tenga acceso a la red 192.168.10.0/24. Debe hacer un ping extendido y usar la dirección G0/1 en el R3 como origen. Haga ping a la dirección IP de la PC-A. ¿Fueron correctos los pings? \_\_\_\_\_\_\_ No

R3# **ping**

Protocol [ip]:

Target IP address: **192.168.10.3**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: **y**

Source address or interface: **192.168.30.1**

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:

Packet sent with a source address of 192.168.30.1

U.U.U

* + - 1. Pruebe la ACL para ver si permite que el tráfico de la red 192.168.40.0/24 acceda a la red 192.168.10.0/24. Debe hacer un ping extendido y usar la dirección loopback 0 en el R3 como origen. Haga ping a la dirección IP de la PC-A. ¿Fueron correctos los pings? \_\_\_\_\_\_\_ Sí

R3# **ping**

Protocol [ip]:

Target IP address: **192.168.10.3**

Repeat count [5]:

Datagram size [100]:

Timeout in seconds [2]:

Extended commands [n]: **y**

Source address or interface: **192.168.40.1**

Type of service [0]:

Set DF bit in IP header? [no]:

Validate reply data? [no]:

Data pattern [0xABCD]:

Loose, Strict, Record, Timestamp, Verbose[none]:

Sweep range of sizes [n]:

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.10.3, timeout is 2 seconds:

Packet sent with a source address of 192.168.40.1

!!!!!

Reflexión

* 1. Como puede observar, las ACL estándar son muy eficaces y funcionan muy bien. ¿Por qué tendría la necesidad de usar ACL extendidas?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Las ACL estándar solo realizan filtrado según la dirección de origen. Además, no son granulares. Permiten o deniegan TODO (protocolos y servicios). Si bien las ACL extendidas son más difíciles de componer, son adecuadas para las redes complejas en las que quizá necesite permitir solo el acceso de ciertos puertos a las redes y denegar otros.

* 1. Generalmente, se requiere escribir más al usar una ACL con nombre que una ACL numerada. ¿Por qué elegiría ACL con nombre en vez de ACL numeradas?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Los estudiantes podrían mencionar dos razones aquí. La primera razón es que usar ACL con nombre le proporciona la capacidad de modificar líneas específicas dentro de la ACL, sin necesidad de volver a escribir todo. NOTA: Las versiones más recientes del IOS permiten la modificación de las ACL numeradas del mismo modo que las ACL con nombre. En segundo lugar, se recomienda tener una ACL con nombre, ya que ayuda a registrar el propósito de la ACL con un nombre descriptivo.