Sistema de evaluación

Saltar a Tiempo restante | Saltar a Navegación | Saltar a Temas de la evaluación

ComputingPeru

Comenzar la evaluación - EWAN Chapter 5 - CCNA Exploration: Acceso a la WAN (Versión 4.0)

Tiempo restante: 00:19:14

Mostrando 1 de 2 Siguiente> Página: 1 IR <Ant.

1

```
R3# show running-config
<resultado omitido>
interface serial0/0/1
 ip address 10.2.2.2 255.255.255.252
 ip access-group 101 in

access-list 101 permit tcp any host 10.2.2.2 eq telnet
access-list 101 dynamic testlist timeout 15 permit ip any 192.168.30.0 0.0.0.255

line vty 0
 login local
 autocommand access-enable timeout 5
<resultado omitido>
```

Consulte la ilustración. ¿Cuál es el efecto de la configuración que se muestra?

- (•) Los usuarios que intentan acceder a los hosts en la red 192.168.30.0/24 deberán establecer una conexión telnet con R3.
- ( ) Los hosts que se conectan a recursos en la red 191.68.30.0/24 tienen un tiempo de espera de 15 minutos.
- ( ) Cualquiera que intente establecer una conexión telnet en R3 tendrá un límite absoluto de 5 minutos.
- ( ) El acceso Telnet a R3 sólo se admitirá en Serial 0/0/1.

2 ¿Cuáles de las siguientes son dos afirmaciones verdaderas acerca de la importancia de la máscara wildcard de la lista de control de acceso 0.0.0.7? (Elija dos opciones).

- [ ] Se pasarán por alto los primeros 29 bits de una dirección IP determinada.
- [x] Se pasarán por alto los últimos 3 bits de una dirección IP determinada.
- [ ] Se verificarán los primeros 32 bits de una dirección IP determinada.
- [x] Se verificarán los primeros 29 bits de una dirección IP determinada.
- [ ] Se verificarán los últimos 3 bits de una dirección IP determinada.

3

```
R2# show ip access-list
    Standard IP access list WEBSERVER
    10 permit 192.168.10.11 0.0.255.255
    20 permit host 192.168.10.13
```

Consulte la ilustración. ¿De qué manera esta lista de acceso procesa un paquete con la dirección de origen 10.1.1.1 y con la dirección de destino 192.168.10.13?

- ( ) Se admite debido al deny any (denegar todo) implícito.
- (•) Se descarta porque no coincide con ninguno de los elementos de la ACL.
- ( ) Está permitido porque la línea 10 de la ACL permite los paquetes que se dirigen a 192.168.0.0/16.
- ( ) Está permitido porque la línea 20 de la ACL permite los paquetes que se dirigen al host 192.168.10.13.

4 ¿Cuáles de los siguientes son tres elementos que se deben configurar antes de que una ACL dinámica se active en un router? (Elija tres opciones).

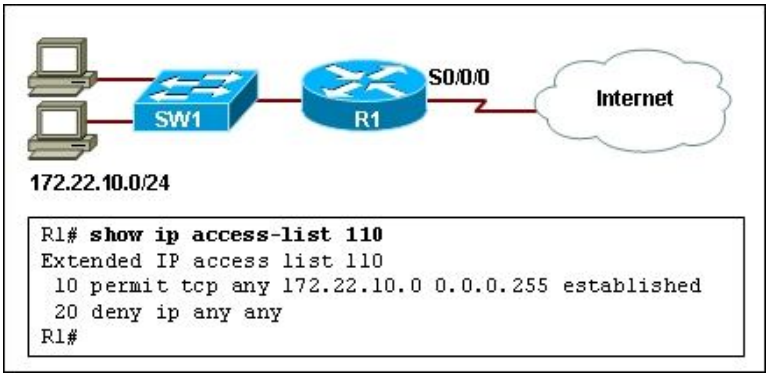
- [x] ACL extendida
- [ ] ACL reflexiva
- [ ] registro de consola
- [x] autenticación

- [x] conectividad Telnet
- [ ] cuenta de usuario con nivel de privilegio de 15

5 ¿Dónde se debe colocar la lista de control de acceso estándar?
- cerca del origen
- (•) cerca del destino
- en un puerto Ethernet
- en un puerto serial

6 ¿Cuál es la forma predeterminada en la que el tráfico IP se filtra en un router Cisco?
- bloqueado hacia adentro y hacia afuera de todas las interfaces
- bloqueado en todas las interfaces entrantes, pero permitido en todas las interfaces salientes
- (•) permitido hacia adentro y hacia afuera de todas las interfaces
- bloqueado en todas las interfaces salientes, pero permitido en todas las interfaces entrantes

7



Consulte la ilustración. ¿Qué afirmación acerca de la ACL 110 es verdadera, en caso de que ACL 110 se aplique en la dirección de entrada en S0/0/0 de R1?
- Denegará el tráfico TCP a Internet si el tráfico se origina de la red 172.22.10.0/24.
- No permitirá el tráfico TCP proveniente de Internet para entrar a la red 172.22.10.0/24.
- Permitirá cualquier tráfico TCP proveniente de Internet para entrar a la red 172.22.10.0/24.
- (•) Permitirá cualquier tráfico TCP originado desde la red 172.22.10.0/24 para retornar entrante a la interfaz S0/0/0.

8 ¿Cuáles de las siguientes son dos afirmaciones verdaderas con respecto a la siguiente ACL extendida? (Elija dos opciones.)

access-list 101 deny tcp 172.16.3.0 0.0.0.255 any eq 20
access-list 101 deny tcp 172.16.3.0 0.0.0.255 any eq 21
access-list 101 permit ip any any

- [x] Se deniega el tráfico FTP que se origina en la red 172.16.3.0/24.
- [ ] Se deniega implícitamente todo el tráfico.
- [ ] Se deniega el tráfico FTP destinado a la red 172.16.3.0/24.
- [ ] Se deniega el tráfico Telnet que se origina en la red 172.16.3.0/24.
- [x] Está permitido el tráfico Web que se origina en la red 172.16.3.0/24.

9 La interfaz s0/0/0 ya tiene una ACL de IP aplicada como entrante. ¿Qué ocurre cuando el administrador de red intenta aplicar una segunda ACL de IP entrante?
- (•) La segunda ACL se aplica a la interfaz y reemplaza a la primera.
- Ambas ACL se aplican a la interfaz.
- El administrador de red recibe un error.
- Sólo la primera ACL sigue aplicada a la interfaz.

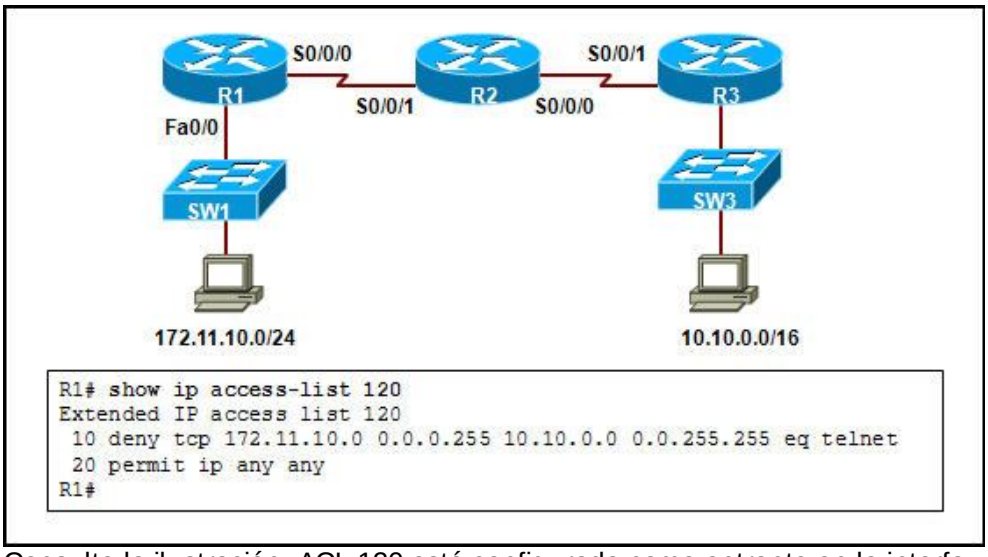
10 ¿De qué manera las ACL estándar de Cisco filtran el tráfico?
- por puerto UDP de destino
- por tipo de protocolo
- (•) por dirección IP de origen
- por puerto UDP de origen
- por dirección IP de destino

11 ¿Cuáles de las siguientes son dos afirmaciones verdaderas con respecto a las ACL nombradas?

(Elija dos opciones).
- [ ] Sólo las ACL nombradas permiten introducir comentarios.
- [x] Los nombres se pueden utilizar para ayudar a identificar la función de la ACL.
- [ ] Las ACL nombradas ofrecen opciones de filtrado más específicas que las ACL numeradas.
- [x] Algunas ACL complejas, como las ACL reflexivas, deben ser definidas con ACL nombradas.
- [ ] Se puede configurar más de una ACL IP nombrada en cada dirección de la interfaz de un router.

12 ¿Cuáles de las siguientes son tres afirmaciones que describen el procesamiento de paquetes por parte de las ACL? (Elija tres opciones).
- [x] Un **deny any** implícito rechaza cualquier paquete que no coincide con cualquier sentencia ACL.
- [x] Un paquete puede rechazarse o enviarse según lo indica la sentencia que coincide.
- [ ] Un paquete que se ha denegado por una sentencia puede ser permitido por una sentencia posterior.
- [ ] Un paquete que no coincide con las condiciones de ninguna sentencia ACL se enviará de manera predeterminada.
- [x] Cada sentencia se verifica sólo hasta que se detecta una coincidencia o hasta el final de la lista de sentencias ACL.
- [ ] Cada paquete se compara con las condiciones de cada sentencia en la ACL antes de tomar una decisión de envío.

13



Consulte la ilustración. ACL 120 está configurada como entrante en la interfaz serial0/0/0 en el router R1, pero los hosts de la red 172.11.10.0/24 pueden conectarse mediante Telnet a la red 10.10.0.0/16. Sobre la base de la configuración proporcionada, ¿qué debe hacerse para solucionar el problema?
- (•) Aplicar la ACL saliente en la interfaz serial0/0/0 en el router R1.
- ( ) Aplicar la ACL saliente en la interfaz FastEthernet0/0 en el router R1.
- ( ) Incluir la palabra clave **established** al final de la primera línea de la ACL.
- ( ) Incluir una sentencia en la ACL para denegar el tráfico UDP que se origina desde la red 172.11.10.0/24.

14 Un administrador de red debe permitir el tráfico a través del router firewall para las sesiones que se originan en el interior de la red de la empresa, pero bloquear el tráfico en las sesiones que se originan afuera de la red de la empresa. ¿Qué tipo de ACL es la más adecuada?
- ( ) dinámica
- ( ) basada en puerto
- (•) reflexiva
- ( ) basada en el tiempo

15

```
Router1(config)# time-range EVERYOTHERDAY
Router1(config-time-range)# periodic Monday Wednesday Friday 8:00 to 17:00
Router1(config)# access-list 101 permit tcp 10.1.1.0 0.0.0.255 172.16.1.0 0.0.0.255 eq telnet time-range EVERYOTHERDAY
Router1(config)# interface fa0/0
Router1(config-if)# ip address 10.1.1.1 255.255.255.0
Router1(config-if)# ip access-group 101 in
```

Consulte la ilustración. ¿Cómo tratará el Router1 el tráfico que coincida con el requisito del intervalo temporal de EVERYOTHERDAY?

- El tráfico TCP que ingresa a fa0/0 desde 172.16.1.254/24 destinado a la red 10.1.1.0/24 está permitido.
- El tráfico TCP que ingresa a fa0/0 desde 10.1.1.254/24 destinado a la red 172.16.1.0/24 está permitido.
- El tráfico Telnet que ingresa a fa0/0 desde 172.16.1.254/24 destinado a la red 10.1.1.0/24 está permitido.
- El tráfico Telnet que ingresa a fa0/0 desde 10.1.1.254/24 destinado a la red 172.16.1.0/24 está permitido.

Sistema de evaluación

Saltar a Tiempo restante | Saltar a Navegación | Saltar a Temas de la evaluación

Comenzar la evaluación - EWAN Chapter 5 - CCNA Exploration: Acceso a la WAN (Versión 4.0)

Tiempo restante: 00:18:17

Mostrando 2 de 2 Siguiente> Página: 2 IR <Ant.

16 Se introdujeron los siguientes comandos en un router.

Router(config)# **access-list 2 deny 172.16.5.24**
Router(config)# **access-list 2 permit any**

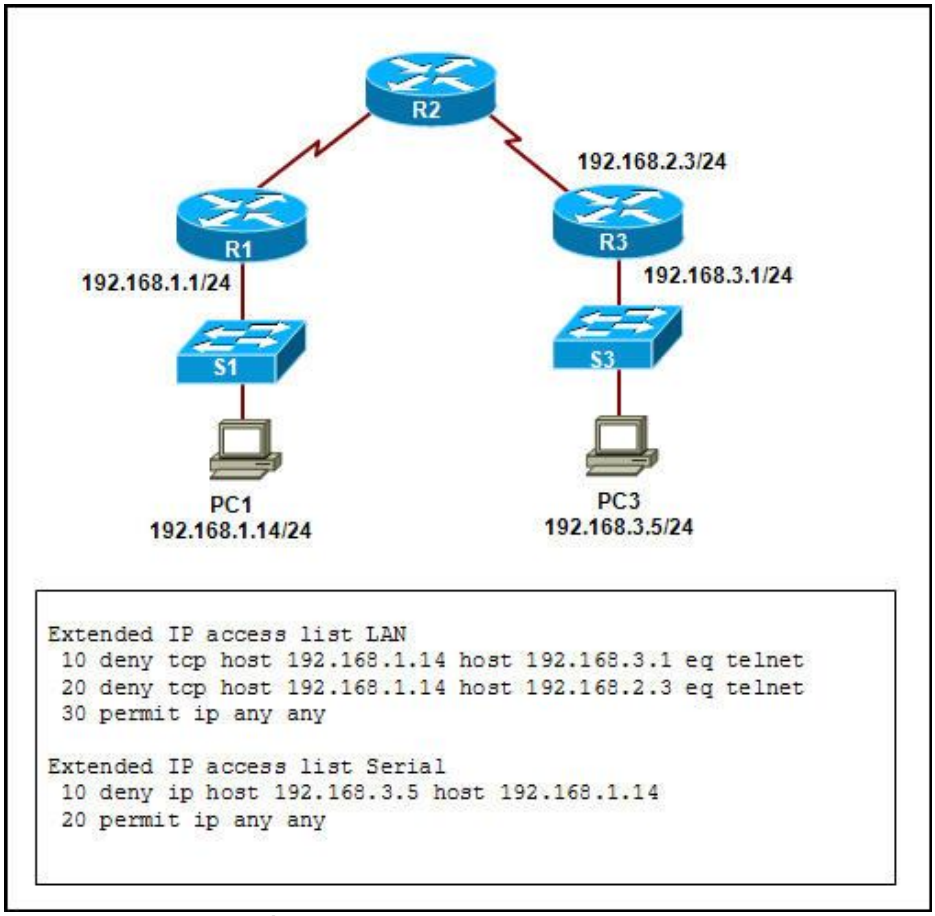
The ACL is correctly applied to an interface. ¿Qué se puede concluir sobre este conjunto de comandos?

- (•) Se supone una máscara wildcard 0.0.0.0.
- ( ) Las sentencias de lista de acceso están mal configuradas.
- ( ) A todos los nodos de la red 172.16.0.0 se les negará acceso a otras redes.
- ( ) No se permitirá tráfico para acceder a los nodos y servicios de la red 172.16.0.0.

17 ¿Cuáles de las siguientes son afirmaciones correctas acerca de las ACL extendidas? (Elija dos opciones).

- [ ] Las ACL extendidas usan un número dentro del intervalo del 1 al 99.
- [ ] Las ACL extendidas finalizan con una sentencia de permiso implícito.
- [x] Las ACL extendidas evalúan las direcciones origen y destino.
- [x] Se pueden usar los números de puerto para agregar mayor definición a una ACL.
- [ ] Se pueden colocar varias ACL en la misma interfaz, siempre y cuando estén en la misma dirección.

18




```
Extended IP access list LAN
 10 deny tcp host 192.168.1.14 host 192.168.3.1 eq telnet
 20 deny tcp host 192.168.1.14 host 192.168.2.3 eq telnet
 30 permit ip any any

Extended IP access list Serial
 10 deny ip host 192.168.3.5 host 192.168.1.14
 20 permit ip any any
```

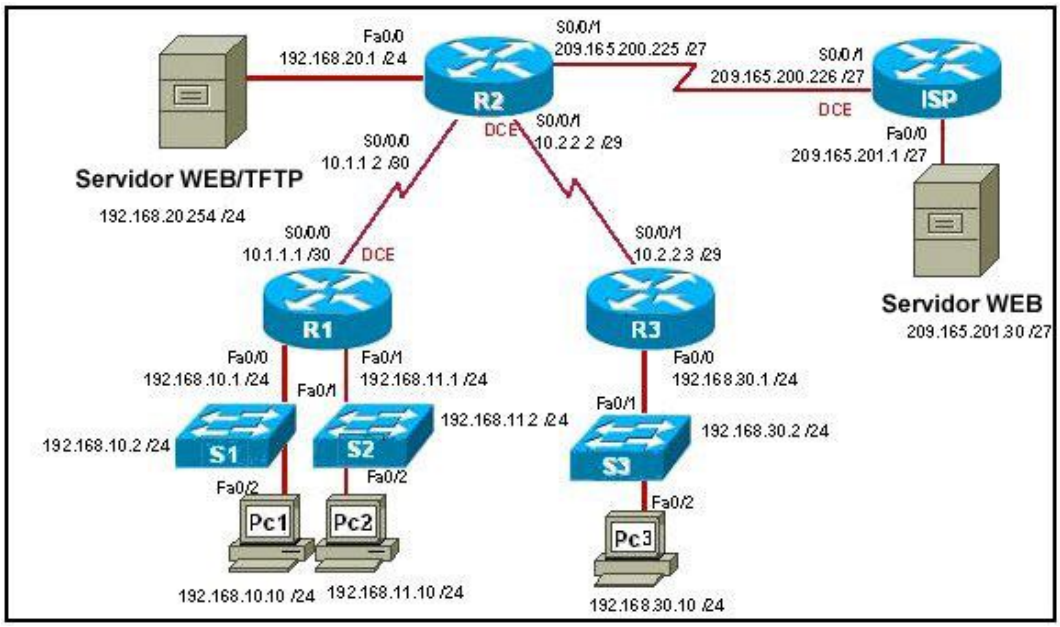
Consulte la ilustración. Un administrador ha configurado dos listas de acceso en R1. La lista entrante en la interfaz serial se llama **Serial** y la lista entrante en la interfaz LAN se llama **LAN**. ¿Qué efecto producirán las listas de control de acceso?

- La PC1 no podrá conectarse mediante Telnet a R3 y la PC3.
- R3 no podrá comunicarse con la PC1 y la PC3.
- La PC3 no puede conectarse mediante Telnet a R3 y no puede comunicarse con la PC1.
- La PC1 no podrá conectarse mediante Telnet con R3 y la PC3 no podrá comunicarse con la PC1.

19 ¿Cuál de las siguientes afirmaciones sobre las ACL estándar es verdadera?

- Las ACL estándar deben numerarse y no pueden nombrarse.
- Deberán colocarse tan cerca del destino como sea posible.
- Puede filtrar según la dirección de destino y la dirección de origen así como en los puertos de destino y de origen.
- Cuando se aplican en la interfaz de salida, los paquetes de entrada se procesan antes de que se enruten a la interfaz de salida.

20



Consulte la ilustración. Al crear una ACL extendida para denegar el tráfico desde la red 192.168.30.0 destinado al servidor Web 209.165.201.30, ¿cuál es la mejor ubicación para aplicar la ACL?

- (•) Fa0/0 del ISP saliente
- ( ) S0/0/1 de R2 entrante
- ( ) Fa0/0 de R3 entrante
- ( ) S0/0/1 de R3 saliente

21 Un técnico está creando una ACL y necesita una forma de indicar únicamente la subred 172.16.16.0/21. ¿Qué combinación de dirección de red y máscara wildcard permitirá llevar a cabo la tarea deseada?

- ( ) 172.16.0.0 0.0.255.255
- ( ) 127.16.16.0 0.0.0.255
- (•) 172.16.16.0 0.0.7.255
- ( ) 172.16.16.0 0.0.15.255
- ( ) 172.16.16.0 0.0.255.255

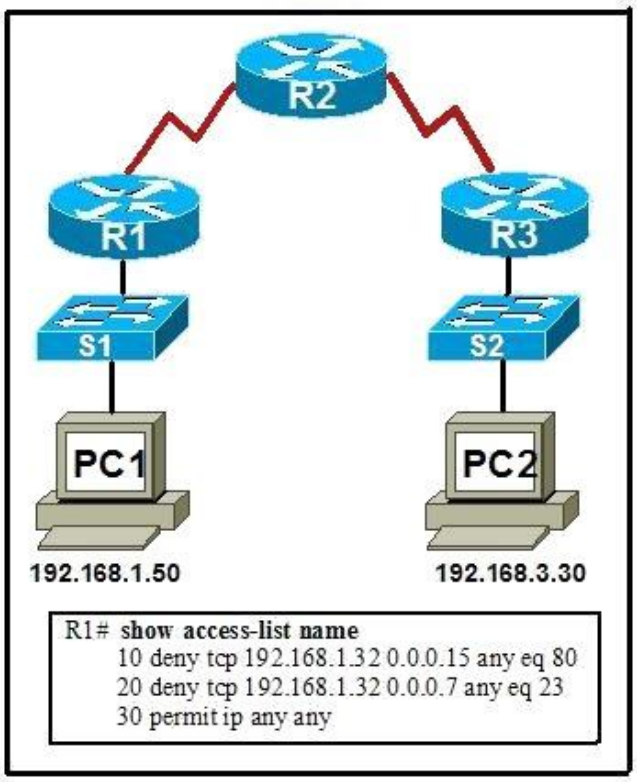
22 ¿Cuáles de los siguientes son tres parámetros que pueden usar las ACL para filtrar el tráfico? (Elija tres opciones).

- [ ] tamaño del paquete
- [x] suite de protocolos
- [x] dirección de origen
- [x] dirección destino
- [ ] Interfaz de router de origen
- [ ] Interfaz de router de destino

23 ¿Qué beneficio ofrece una ACL extendida sobre una ACL estándar?

- ( ) Las ACL extendidas pueden nombrarse, pero las ACL estándar no.
- ( ) A diferencia de las ACL estándar, las ACL pueden aplicarse en la dirección de entrada y salida.
- ( ) Según el contenido, una ACL extendida puede filtrar paquetes como información en un correo electrónico o en un mensaje instantáneo.
- (•) Además de la dirección de origen, una ACL extendida también puede filtrar según el puerto de origen, el puerto de destino y la dirección de destino.

24



Consulte la ilustración. El administrador desea bloquear el tráfico Web de 192.168.1.50 para que no llegue al puerto predeterminado del servicio Web en 192.168.3.30. Para lograr esto, el nombre de la lista de control de acceso se aplica como entrante en la interfaz R1 LAN del router. Después de probar la lista, el administrador ha advertido que el tráfico Web permanece exitoso. ¿Por qué el tráfico Web alcanza su destino?

- El tráfico Web no utiliza el puerto 80 de manera predeterminada.
- La lista de acceso se aplica en la dirección incorrecta.
- La lista de acceso deberá colocarse más cerca del destino, en R3.
- El grupo de direcciones de origen especificado en la línea 10 no incluye el host 192.168.1.50.

25 ¿Qué función requerirá el uso de una ACL nombrada en lugar de una ACL numerada?

- La capacidad de filtrar tráfico sobre la base de un protocolo específico.
- La capacidad de filtrar tráfico sobre la base de un destino y un conjunto completo de protocolos.
- La capacidad de especificar direcciones de destino y de origen para utilizar una vez que se identifique el tráfico.
- La capacidad de editar la ACL y añadir sentencias adicionales en el medio de una lista sin quitar ni volver a crear la lista.