

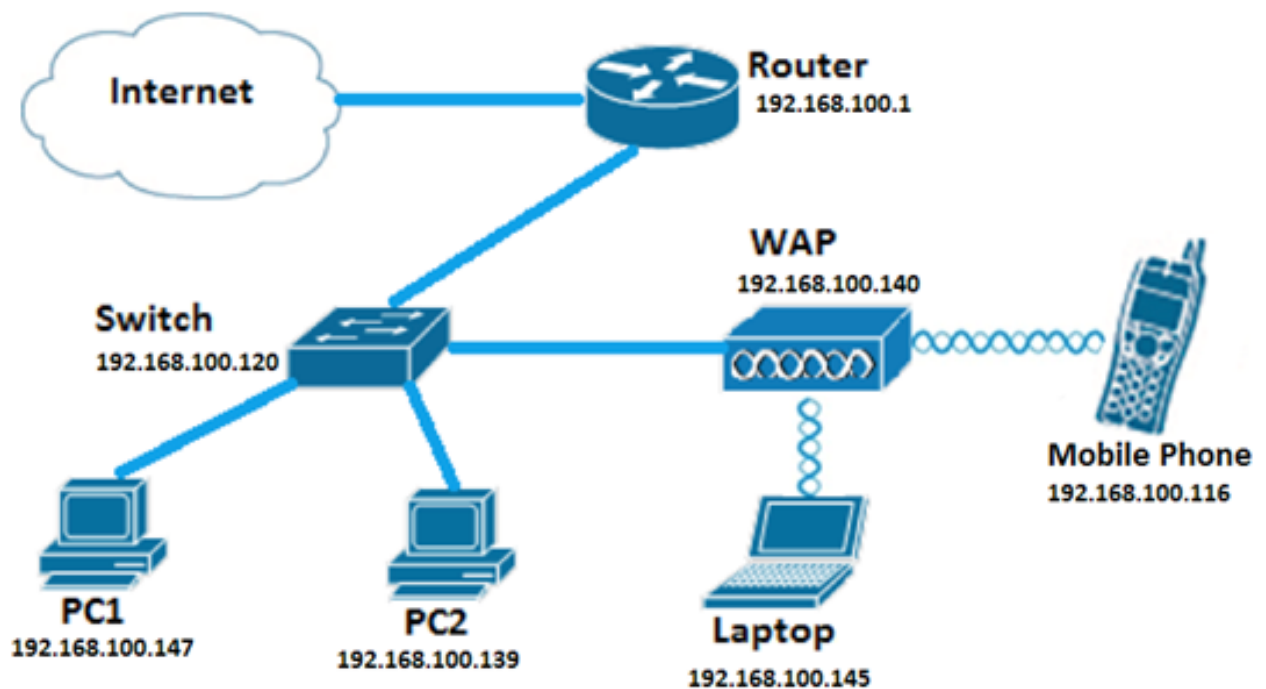
Configuración de IPv4 ACL en WAP125 y WAP581

Introducción

Las listas de control de acceso (ACL) de protocolo de Internet versión 4 (IPv4) y de protocolo de Internet versión 6 (IPv6) son un conjunto de reglas aplicadas a los paquetes recibidos por el punto de acceso inalámbrico (WAP). Cada regla se utiliza para determinar si se debe permitir o denegar el acceso a la red. Las ACL se pueden configurar para inspeccionar campos de una trama como la dirección IP de origen o de destino, el identificador (ID) de red de área local virtual (VLAN) o la clase de servicio (CoS). Cuando una trama ingresa al puerto del dispositivo WAP, inspecciona la trama y verifica las reglas ACL en relación con el contenido de la trama. Si alguna de las reglas coincide con el contenido, se realiza una acción permit o deny en la trama.

La configuración de ACL IPv4 se utiliza normalmente para autorizar el acceso a los recursos de red para seleccionar dispositivos en la red.

Nota: Hay una negación implícita al final de cada regla creada.



Nota: En esta situación, se permitirá que todo el tráfico de PC2 acceda a la red. Se denegará todo el resto del tráfico de otros hosts.

Objetivo

Este artículo pretende mostrarle cómo configurar una ACL IPv4 en un punto de acceso WAP125 y WAP581.

Dispositivos aplicables

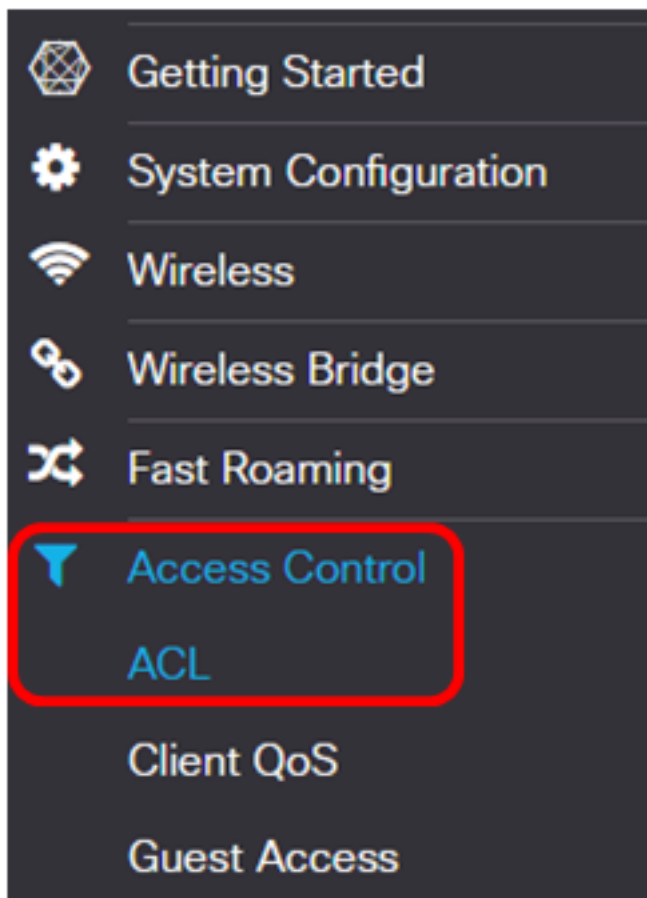
- WAP125
- WAP581

Versión del software

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

Configuración de una ACL IPv4

Paso 1. Inicie sesión en la utilidad basada en web del WAP y elija **Access Control > ACL**.

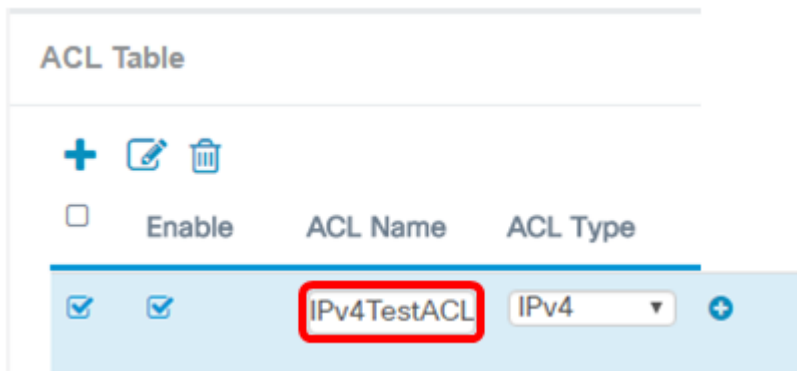


Paso 2. Haga clic en el **+** botón para crear una nueva ACL.

ACL Table

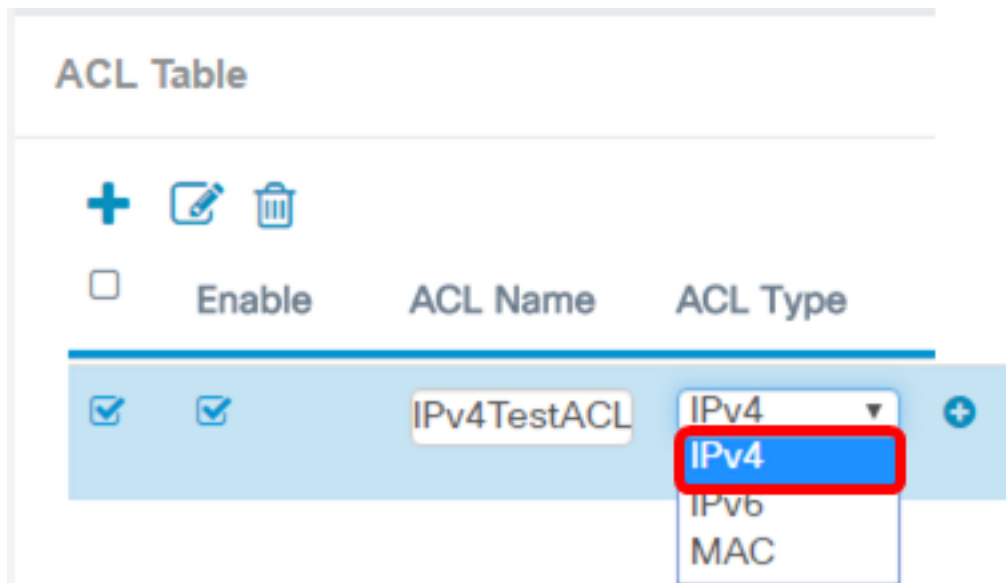



Paso 3. Ingrese un nombre para la ACL en el campo *ACL Name*.



Nota: En este ejemplo, se ingresa IPv4TestACL.

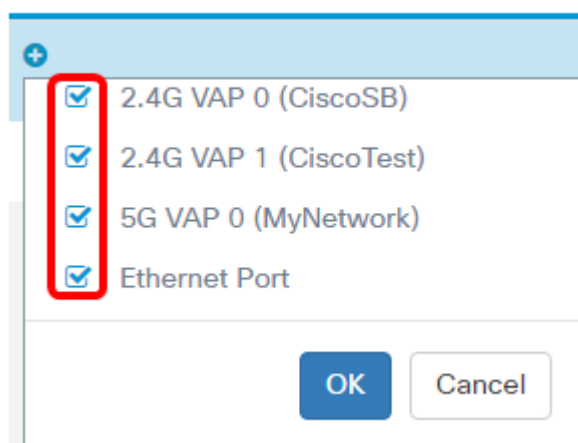
Paso 4. Elija IPv4 en la lista desplegable Tipo de ACL.



Paso 5. Haga clic en el  botón y elija una interfaz de la lista desplegable Interfaz asociada. Las opciones son:

- 2.4G VAP 0 (nombre de SSID): esta opción aplicará la ACL MAC al punto de acceso virtual (VAP) de 2,4 GHz. La sección SSID Name puede cambiar dependiendo del nombre SSID configurado en el WAP.
- 5G VAP0 (nombre de SSID): esta opción aplicará la ACL MAC al VAP de 5 GHz.
- Puerto Ethernet: esta opción aplicará la ACL MAC a la interfaz Ethernet del WAP.

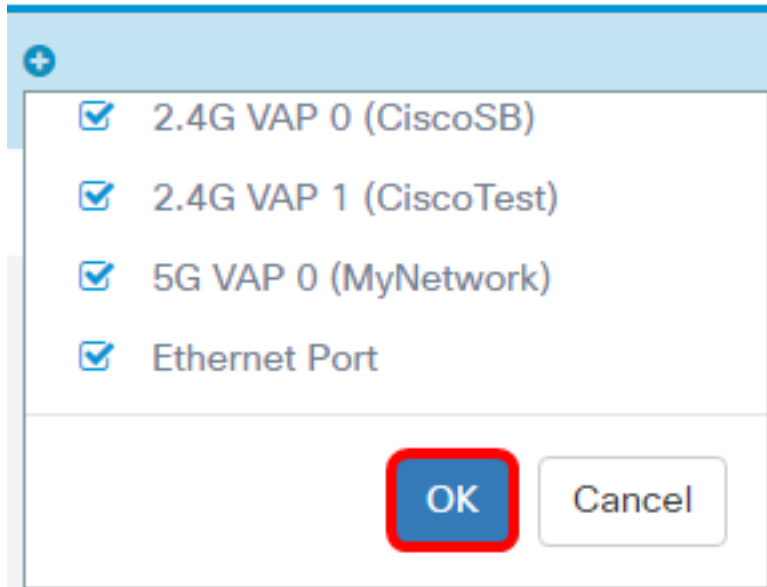
Associated Interface



Nota: Se pueden asociar varias interfaces a una ACL. Sin embargo, no se puede asociar a una ACL cuando ya se ha asociado a otra ACL. En este ejemplo, todas las interfaces se asocian a IPv4TestACL. Desactive la casilla para desasociar la interfaz de la ACL.

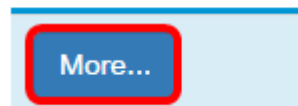
Paso 6. Click OK.

Associated Interface



Paso 7. Haga clic en el botón **More...** para configurar los parámetros de la ACL.

Details Of Rule(s)

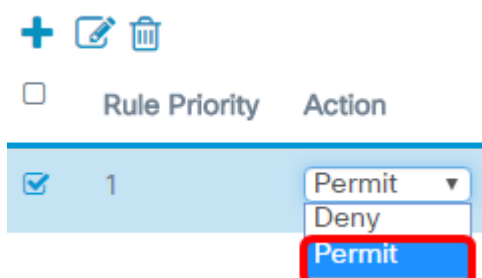


Paso 8. Haga clic en el **+** botón para agregar una nueva regla.



Paso 9. Elija una acción de la lista desplegable Acción. Las opciones son:

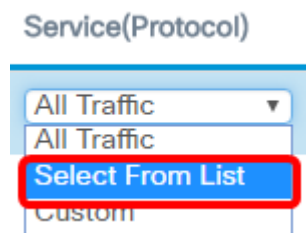
- Permit: esta opción permitirá que los paquetes que coinciden con los criterios de ACL se conecten a la red.
- Denegar: esta opción impedirá que los paquetes que coinciden con los criterios de ACL se conecten a la red.



Nota: En este ejemplo, se elige Permitir.

Paso 10. Elija un servicio o protocolo que se filtrará desde la lista desplegable Servicio (protocolo). Las opciones son:

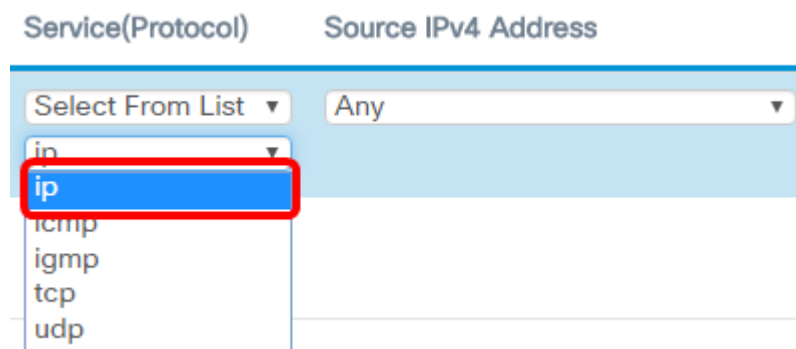
- Todo el tráfico: esta opción tratará todos los paquetes como una coincidencia con el filtro ACL.
- Seleccionar de la lista: esta opción le permitirá elegir IP, ICMP, IGMP, TCP o UDP como filtros para la ACL. Si se elige esta opción, vaya al paso 11.
- Personalizado: esta opción le permitirá introducir un identificador de protocolo personalizado como filtro para los paquetes. El valor es un número hexadecimal de cuatro dígitos. El rango va de 0 a 255.



Nota: En este ejemplo, se elige Seleccionar de la lista.

Paso 11. Defina el protocolo que debe permitirse conectar a la red. Las opciones son:

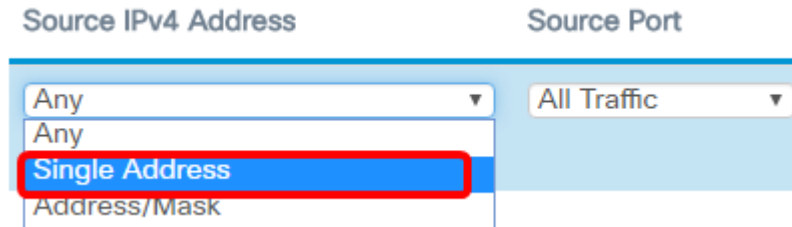
- ip: esta opción permitirá que el punto de acceso filtre los hosts que acceden a la red utilizando su dirección IP como filtro.
- icmp: esta opción permitirá que el punto de acceso filtre los paquetes del protocolo de mensajes de control de Internet (ICMP) que ingresan a la red a través del punto de acceso.
- igmp: esta opción permitirá que el punto de acceso filtre los paquetes del protocolo de administración de grupos de Internet (IGMP) que ingresan a la red a través del punto de acceso.
- tcp: esta opción permitirá que los paquetes TCP (del inglés Transmission Control Protocol, protocolo de control de transmisión) del punto de acceso entren en la red a través del punto de acceso.
- udp: esta opción permitirá que el punto de acceso filtre los paquetes del protocolo de datagramas de usuario (UDP) que entran en la red a través del punto de acceso.



Nota: En este ejemplo, se elige ip.

Paso 12. Defina la dirección IPv4 de origen en la lista desplegable Dirección IPv4 de origen. Las opciones son:

- Any — Esta opción permitirá que el WAP aplique el filtro a los paquetes desde cualquier dirección IP.
- Single Address: esta opción permitirá que el WAP aplique el filtro a los paquetes de una dirección IP especificada.
- Dirección/Máscara: esta opción permitirá que el WAP aplique el filtro a los paquetes a una dirección IP y la máscara de la IP.



Nota: En este ejemplo, se elige la dirección única.

Paso 13. Introduzca la dirección IP del host que debe permitirse al acceder a la red.

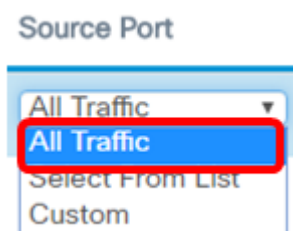


Nota: En este ejemplo, se ingresa 192.168.100.139. Esta es la dirección IP de PC2.

Paso 14. Elija un puerto de origen para la condición. Las opciones son:

- Todo el tráfico: esta opción permitirá todos los paquetes del puerto de origen que cumplan los criterios.
- Seleccionar de la lista: esta opción permite elegir ftp, ftpdata, http, smtp, snmp, telnet, tftp y www.
- Personalizado: esta opción le permitirá introducir un número de puerto IANA que coincida con el puerto de origen identificado en el encabezado del datagrama. El rango de puertos está entre 0 y 65535 e incluye lo siguiente:

- 0 a 1023 — Puertos conocidos
- 1024 — 49151 — Puertos registrados
- 49152 — 65535 — Puertos dinámicos y/o privados



Nota: En este ejemplo, se elige Todo el tráfico.

Paso 15. Elija una dirección de destino en la lista desplegable Dirección IPv4 de destino. Las opciones son:

- Any: Esta opción trata cualquier dirección IP como una coincidencia con la sentencia

ACL.

- Single Address: esta opción le permite introducir una dirección IP específica para la condición ACL.
- Dirección/Máscara: esta opción le permite introducir un rango o una máscara de dirección IP.

The image shows a configuration interface with two dropdown menus. The first dropdown, labeled 'Source Port', has 'All Traffic' selected. The second dropdown, labeled 'Destination IPv4 Address', is open and shows 'Any' selected and highlighted with a red box. Below 'Any', the options 'Single Address' and 'Address/Mask' are visible.

Nota: En este ejemplo, se elige Any (Cualquiera).

Paso 16. Elija un puerto de destino en la lista desplegable Puerto de destino. Las opciones son:

- Any: Esta opción trata todos los puertos de destino de los paquetes como una coincidencia con la sentencia de la ACL.
- Seleccionar de la lista: esta opción permite elegir una palabra clave asociada al puerto de destino que coincida. Las opciones son: ftp, ftpdata, http, smtp, snmp, telnet, tftp y www. Estas palabras clave se traducen a sus números de puerto correspondientes.
- Personalizado: esta opción le permitirá introducir un número de puerto IANA que coincida con el puerto de origen identificado en el encabezado del datagrama. El rango de puertos está entre 0 y 65535 e incluye lo siguiente:
 - 0 a 1023 — Puertos conocidos
 - 1024 — 49151 — Puertos registrados
 - 49152 — 65535 — Puertos dinámicos y/o privados

Paso 17. Elija un tipo de servicio que coincida con el tipo de paquete de la lista desplegable Tipo de servicio. Las opciones son:

- Any: Esta opción trata cualquier servicio como una coincidencia para los paquetes.
- Seleccionar de la lista: esta opción coincide con los paquetes según sus valores de punto de código de servicios diferenciados (DSCP), clase de servicio (CoS) o reenvío acelerado (EF).
- DSCP: la opción coincide con los paquetes según su valor DSCP personalizado. Al elegir esta opción, introduzca un valor entre 0 y 63 en el campo DSCP Value (Valor DSCP).
- Precedencia: esta opción coincide con los paquetes en función de su valor de precedencia IP. Cuando se elige esta opción, introduzca un valor de precedencia IP de 0 a 7.
- ToS/Mask: esta opción le permite ingresar una Máscara IP ToS para identificar las posiciones de bits en el valor de bits de transmisión IP que se utilizan para la comparación con el campo ToS de IP en un paquete.

Destination Port Type Of Service

Any Any

Any

Select From List

DSCP

Precedence

ToS/Mask

Paso 18. (Opcional) Repita del paso 8 al paso 17 hasta que se complete la ACL.

Nota: Dado que hay una negación implícita al final de cada regla creada, no hay necesidad de agregar una regla de denegación a la ACL para evitar el acceso desde otros dispositivos de la red.

Paso 19. (Opcional) Cambie el orden de las condiciones en la ACL haciendo clic en los botones hacia arriba y hacia abajo hasta que estén en el orden correcto.

+ ✎ 🗑️

Rule Priority

1 ▼

2 ▲

Paso 20. Click OK.

Source Port Destination IPv4 Address

All Traffic Any



Paso 21. Click **Save**.

WAP125-wap5e0940 cisco ? i ↻

ACL Save

ACL Table

+ ✎ 🗑️

<input type="checkbox"/>	<input type="checkbox"/>	ACL Name	ACL Type	Associated Interface	Details Of Rule(s)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TestIPv4ACL	IPv4	<ul style="list-style-type: none"> 2.4G VAP 0 (CiscoSB) 2.4G VAP 1 (CiscoTest) 5G VAP 0 (MyNetwork) Ethernet Port 	More...

Ahora debería haber completado la configuración de una ACL IPv4 que permitiría que sólo un host accediera a la red cuando se conectara al WAP.