

# Configuración de la Lista de control de acceso (ACL) basada en IPv4 e IPv6 en los puntos de acceso WAP551 y WAP561

## Objetivo

Las listas de acceso (ACL) son colecciones de condiciones de permiso y denegación, denominadas reglas, que proporcionan seguridad para bloquear a usuarios no autorizados y permitir que los usuarios autorizados accedan a recursos específicos. Las ACL pueden bloquear cualquier intento injustificado de alcanzar los recursos de red. La función QoS contiene compatibilidad con servicios diferenciados (DiffServ) que permite clasificar el tráfico en secuencias y recibir cierto tratamiento de QoS de acuerdo con los comportamientos definidos por salto.

En este artículo se explica cómo crear y configurar ACL basadas en IPv4 e IPv6 en puntos de acceso WAP551 y WAP561 (WAP).

## Dispositivos aplicables

- WAP551
- WAP561

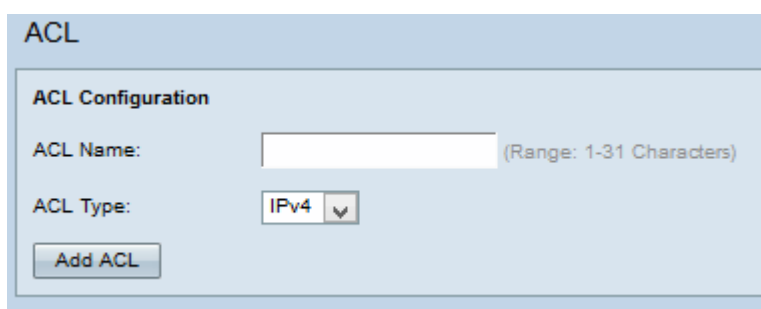
## Versión del software

- v1.0.4.2

## Configuración de ACL

Las ACL IP clasifican el tráfico para la Capa 3 en la pila IP. Cada ACL es un conjunto de hasta 10 reglas aplicadas al tráfico enviado desde un cliente inalámbrico o para ser recibido por un cliente inalámbrico. Cada regla especifica si el contenido de un campo determinado debe utilizarse para permitir o denegar el acceso a la red. Las reglas pueden basarse en diversos criterios y aplicarse a uno o más campos dentro de un paquete, como la dirección IP de origen o destino, el puerto de origen o de destino o el protocolo transportado en el paquete.

Paso 1. Inicie sesión en la utilidad de configuración web y elija **Client QoS > ACL**. Se abre la página **ACL**:



ACL

ACL Configuration

ACL Name:  (Range: 1-31 Characters)

ACL Type: IPv4 ▼

Add ACL

ACL Configuration

ACL Name:  (Range: 1-31 Characters)

ACL Type:

Paso 2. Introduzca el nombre de la ACL en el campo Nombre de la ACL.

Paso 3. Elija el tipo de ACL deseado en la lista desplegable Tipo de ACL. Si se elige IPv6, consulte la sección [Configuración de ACL IPv6](#). Si se elige la ACL basada en MAC de la lista desplegable Tipo de ACL, consulte el artículo [Configuración de la Lista de Control de Acceso Basada en MAC \(ACL\) en los Puntos de Acceso WAP551 y WAP561](#).

Paso 4. Haga clic en **Agregar ACL** para crear una nueva ACL.

## Configuración de ACL IPv4

**Nota:** Si se elige IPv4 en la lista desplegable Tipo de ACL, siga los pasos que se indican a continuación para configurar las reglas de ACL IPv4.

ACL Configuration

ACL Name:  (Range: 1-31 Characters)

ACL Type:

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

---

Action:

Match Every Packet:

Protocol:  Select From List:   Match to Value:  (Range: 0 - 255)

Source IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:  (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Source Port:  Select From List:   Match to Port:  (Range: 0 - 65535)

Destination IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:  (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Destination Port:  Select From List:   Match to Port:  (Range: 0 - 65535)

Service Type

IP DSCP:  Select From List:   Match to Value:  (Range: 0 - 63)

IP Precedence:   (Range: 0 - 7)

IP TOS Bits:   (Range: 00 - FF) IP TOS Mask:  (Range: 00 - FF)

Delete ACL:

Paso 1. Elija la ACL creada en la lista desplegable ACL Name-ACL Type .

ACL Name - ACL Type:

Rule:

Action:

Paso 2. Si debe configurarse una nueva regla y si hay menos de 10 reglas para la ACL seleccionada, elija **Nueva regla** en la lista desplegable Regla. De lo contrario, elija una de las reglas actuales de la lista desplegable Regla.

**Nota:** Se puede crear un máximo de 10 reglas para una única ACL.

Paso 3. Elija la acción para la regla ACL en la lista desplegable Acción.

·Denegar: bloquea todo el tráfico que cumple los criterios de regla para entrar o salir del dispositivo WAP.

·Permit: permite que todo el tráfico que cumple los criterios de regla ingrese o salga del dispositivo WAP.

Action:

Match Every Packet:

Protocol:   Select From List:   Match to Value:  (Range: 0 - 255)

Source IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:  (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Source Port:   Select From List:   Match to Port:  (Range: 0 - 65535)

Destination IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:  (xxx.xxx.xxx.xxx - "0s for matching, 1s for no matching")

Destination Port:   Select From List:   Match to Port:  (Range: 0 - 65535)

**Nota:** Todos los pasos siguientes son opcionales. Los cuadros marcados se activarán. Desactive la casilla si no desea aplicar una regla específica.

Paso 4. Marque la casilla de verificación **Coincidir con todos los paquetes** para que coincida con la regla para cada trama o paquete, independientemente de su contenido. Desactive la casilla de verificación **Coincidir con todos los paquetes** para configurar cualquier criterio de coincidencia adicional.

**Timesaver:** Si se marca Coincidir con todos los paquetes, pase al Paso 10.

Paso 5. Marque la casilla de verificación **Protocol** para utilizar una condición de coincidencia de protocolo L3 o L4 basada en el valor del campo IP Protocol en los paquetes IPv4. Si la casilla de verificación Protocol está activada, haga clic en uno de estos botones de opción:

·Seleccionar de la lista: protocolo para elegir de la lista desplegable Seleccionar de la lista.

·Coincidencia con valor: para el protocolo no presentado en la lista. Introduzca un ID de protocolo asignado por IANA estándar que oscile entre 0 y 255.

Paso 6. Active la casilla de verificación **Dirección IP de Origen** para incluir la dirección IP del origen en la condición de coincidencia. Introduzca la dirección IP y la máscara comodín del origen en los campos correspondientes.

Paso 7. Marque la casilla de verificación **Source Port** para incluir un puerto de origen en la condición de coincidencia. Si la casilla de verificación Puerto de origen está activada, haga clic en uno de estos botones de opción:

·Seleccionar de la lista: puerto de origen para elegir de la lista desplegable Seleccionar de la lista.

·Coincidencia con puerto: para el puerto de origen no presentado en la lista. Introduzca el número de puerto que va de 0 a 65535 e incluye tres tipos diferentes de puertos.

- 0 a 1023 — Puertos conocidos.

- 1024 a 49151 — Puertos registrados.

- 49152 a 65535 — Puertos dinámicos y/o privados.

Paso 8. Active la casilla de verificación **Destination IP Address** para incluir la dirección IP del destino en la condición match. Introduzca la dirección IP y la máscara comodín del destino en los campos correspondientes.

Paso 9. Marque la casilla de verificación **Puerto de destino** para incluir un puerto de destino en la condición de coincidencia. Si la casilla de verificación Puerto de destino está activada, haga clic en uno de estos botones de opción.

·Seleccionar de la lista: puerto de destino para elegir de la lista desplegable Seleccionar de la lista.

·Coincidencia con puerto: para el puerto de destino no presentado en la lista. Introduzca el número de puerto que va de 0 a 65535 en el campo Coincidencia con puerto. El rango incluye tres tipos diferentes de puertos.

- 0 a 1023 — Puertos conocidos.

- 1024 a 49151 — Puertos registrados.

- 49152 a 65535 — Puertos dinámicos y/o privados.

**Nota:** Sólo se puede seleccionar uno de los servicios del área Tipo de servicio y se puede agregar para la condición de coincidencia.

Paso 10. Marque la casilla de verificación **IP DSCP** para que coincida con los paquetes según los valores IP DSCP. Si está marcada la casilla de verificación IP DSCP, haga clic en uno de estos botones de opción:

·Seleccionar de la lista: elija el valor IP DSCP deseado en la lista desplegable Seleccionar de la lista.

·Coincidencia con valor: para personalizar los valores DSCP. Introduzca el valor DSCP que va de 0 a 63 en el campo Match to value (Coincidencia con valor).

Paso 11. Marque la casilla de verificación **Precedencia IP** para incluir un valor de Precedencia IP en la condición de coincidencia. Si la casilla de verificación Precedencia IP está activada, introduzca un valor de precedencia IP que oscile entre 0 y 7. Los valores de

precedencia IP y la descripción del valor correspondiente se pueden explicar de la siguiente manera:

- 0: Rutina o mejor esfuerzo
- 1: Prioridad
- 2 — Inmediato
- 3: Flash (utilizado principalmente para señalización de voz o vídeo)
- 4: sustitución de Flash
- 5: Crítico (utilizado principalmente para RTP de voz)
- 6: Internet
- 7: red

Paso 12. Marque la casilla de verificación **Bits de TOS IP para utilizar los bits de Tipo de Servicio en el encabezado IP como criterios de coincidencia**. Si la casilla de verificación IP TOS Bits está activada, introduzca los bits IP TOS que van de 00 a FF y la máscara IP TOS que va de 00 a FF en los campos respectivos.

Paso 13. Para eliminar la ACL configurada, marque la casilla **Delete ACL** y luego haga clic en **Save**.

## [Configuración de ACL IPv6](#)

**Nota:** Si se elige IPv6 en la lista desplegable Tipo de ACL, siga estos pasos para configurar las reglas de ACL IPv6.

**ACL**

**ACL Configuration**

ACL Name:  (Range: 1-31 Characters)

ACL Type:

**ACL Rule Configuration**

ACL Name - ACL Type:

Rule:

---

Action:

Match Every Packet:

Protocol:   Select From List:   Match to Value:  (Range: 0 - 255)

Source IPv6 Address:   Source IPv6 Prefix Length:  (Range: 1 - 128)

Source Port:   Select From List:   Match to Port:  (Range: 0 - 65535)

Destination IPv6 Address:   Destination IPv6 Prefix Length:  (Range: 1 - 128)

Destination Port:   Select From List:   Match to Port:  (Range: 0 - 65535)

IPv6 Flow Label:   (Range: 00000 - FFFFF)

IPv6 DSCP:   Select From List:   Match to Value:  (Range: 0 - 63)

Delete ACL:

Paso 1. Elija la ACL creada en la lista desplegable ACL Name-ACL Type .

**ACL Rule Configuration**

ACL Name - ACL Type:

Rule:

---

Action:

Paso 2. Si se debe configurar una nueva regla para la ACL seleccionada, elija **Nueva regla** en la lista desplegable Regla. De lo contrario, elija una de las reglas actuales de la lista desplegable Regla.

**Nota:** Se puede crear un máximo de 10 reglas para una única ACL.

Paso 3. Elija la acción para la regla ACL en la lista desplegable Acción.

·Denegar: bloquea todo el tráfico que cumple los criterios de regla para entrar o salir del dispositivo WAP.

·Permit: permite que todo el tráfico que cumple los criterios de regla ingrese o salga del dispositivo WAP.

Match Every Packet:	<input type="checkbox"/>	
Protocol:	<input checked="" type="checkbox"/> <input type="radio"/> Select From List: <input type="text" value="icmpv6"/>	<input type="radio"/> Match to Value: <input type="text"/> (Range: 0 - 255)
Source IPv6 Address:	<input checked="" type="checkbox"/> <input type="text" value="2001:db8:a442:3::"/>	Source IPv6 Prefix Length: <input type="text" value="64"/> (Range: 1 - 128)
Source Port:	<input checked="" type="checkbox"/> <input type="radio"/> Select From List: <input type="text"/>	<input type="radio"/> Match to Port: <input type="text" value="56"/> (Range: 0 - 65535)
Destination IPv6 Address:	<input checked="" type="checkbox"/> <input type="text" value="2001:db8:beef:3::"/>	Destination IPv6 Prefix Length: <input type="text" value="64"/> (Range: 1 - 128)
Destination Port:	<input checked="" type="checkbox"/> <input type="radio"/> Select From List: <input type="text" value="snmp"/>	<input type="radio"/> Match to Port: <input type="text"/> (Range: 0 - 65535)

**Nota:** Todos los pasos siguientes son opcionales. Los cuadros marcados se activarán. Desactive la casilla si no desea aplicar una regla específica.

Paso 4. Marque la casilla de verificación **Coincidir con todos los paquetes** para que coincida con la regla para cada trama o paquete, independientemente de su contenido. Desactive la casilla de verificación **Coincidir con todos los paquetes** para configurar cualquier criterio de coincidencia adicional.

**Timesaver:** Si se marca **Coincidir con todos los paquetes**, pase al Paso 12.

Paso 5. Marque la casilla de verificación **Protocol** para utilizar una condición de coincidencia de protocolo L3 o L4 basada en el valor del campo IP Protocol en los paquetes IPv6. Si la casilla de verificación Protocol está activada, haga clic en uno de estos botones de opción.

- Seleccionar de la lista: protocolo para elegir de la lista desplegable Seleccionar de la lista.
- Coincidencia con valor: para el protocolo no presentado en la lista. Introduzca un ID de protocolo asignado por IANA estándar que oscile entre 0 y 255.

Paso 6. Active la casilla de verificación **Dirección IP de Origen** para incluir una dirección IP del origen en la condición de coincidencia. Introduzca la dirección IP y la máscara comodín del origen en los campos correspondientes.

Paso 7. Marque la casilla de verificación **Source Port** para incluir un puerto de origen en la condición de coincidencia. Si la casilla de verificación Puerto de origen está activada, haga clic en uno de los siguientes botones de opción:

- Seleccionar de la lista: puerto de origen para elegir de la lista desplegable Seleccionar de la lista.
- Coincidencia con puerto: para los puertos de origen no presentados en la lista. Introduzca el número de puerto que va de 0 a 65535 e incluye tres tipos diferentes de puertos.
  - 0 a 1023 — Puertos conocidos.
  - 1024 a 49151 — Puertos registrados.
  - 49152 a 65535 — Puertos dinámicos y/o privados.

Paso 8. Active la casilla de verificación **Destination IP Address** para incluir la dirección IP del destino en la condición match. Introduzca la dirección IP y la máscara comodín del destino en los campos correspondientes.

Paso 9. Marque la casilla de verificación **Puerto de destino** para incluir un puerto de destino

en la condición de coincidencia. Si la casilla de verificación Puerto de destino está activada, haga clic en uno de estos botones de opción:

·Seleccionar de la lista: puerto de destino para elegir de la lista desplegable Seleccionar de la lista.

·Coincidencia con puerto: para el puerto de destino no presentado en la lista. Introduzca el número de puerto que va de 0 a 65535 en el campo Coincidencia con puerto. El rango incluye tres tipos diferentes de puertos.

- 0 a 1023 — Puertos conocidos.

- 1024 a 49151 — Puertos registrados.

- 49152 a 65535 — Puertos dinámicos y/o privados.

IPv6 Flow Label:  0304 (Range: 00000 - FFFFF)

IPv6 DSCP:   Select From List:   Match to Value: 45 (Range: 0 - 63)

Delete ACL:

Paso 10. Marque la casilla de verificación **IPv6 Flow Label** para incluir la etiqueta de flujo IPv6 en la condición de coincidencia. El campo de etiqueta de flujo de 20 bits del encabezado IPv6 puede ser utilizado por un origen para etiquetar un conjunto de paquetes que pertenecen al mismo flujo. Introduzca el número que va de 00000 a FFFFF en el campo de etiqueta de flujo de IPv6.

Paso 11. Marque la casilla de verificación **IPv6 DSCP** para incluir los valores IP DSCP en la condición de coincidencia. Si la casilla de verificación IP DSCP está activada, haga clic en uno de estos botones de opción.

·Seleccionar de la lista: valor DSCP IP para elegir de la lista desplegable Seleccionar de la lista.

·Coincidencia con valor: para personalizar el valor DSCP que va de 0 a 63.

Paso 12. (Opcional) Para eliminar la ACL configurada, marque la casilla de verificación **Eliminar ACL**.

Paso 13. Click Save.