

# Creación y configuración de una regla para la lista de control de acceso (ACL) basada en IPv4 en los puntos de acceso WAP121 y WAP321

## Objetivo

Una lista de control de acceso (ACL) es una lista de filtros de tráfico de red y acciones correlacionadas que se utilizan para mejorar la seguridad. Una ACL contiene los hosts a los que se les permite o deniega el acceso al dispositivo de red. La función QoS contiene compatibilidad con servicios diferenciados (DiffServ) que permite que el tráfico se clasifique en secuencias y reciba un tratamiento de QoS determinado de acuerdo con los comportamientos por salto definidos.

En este artículo se explica cómo crear y configurar una ACL basada en IPv4 en puntos de acceso (WAP) WAP121 y WAP321.

## Dispositivos aplicables

- WAP121
- WAP321

## Versión del software

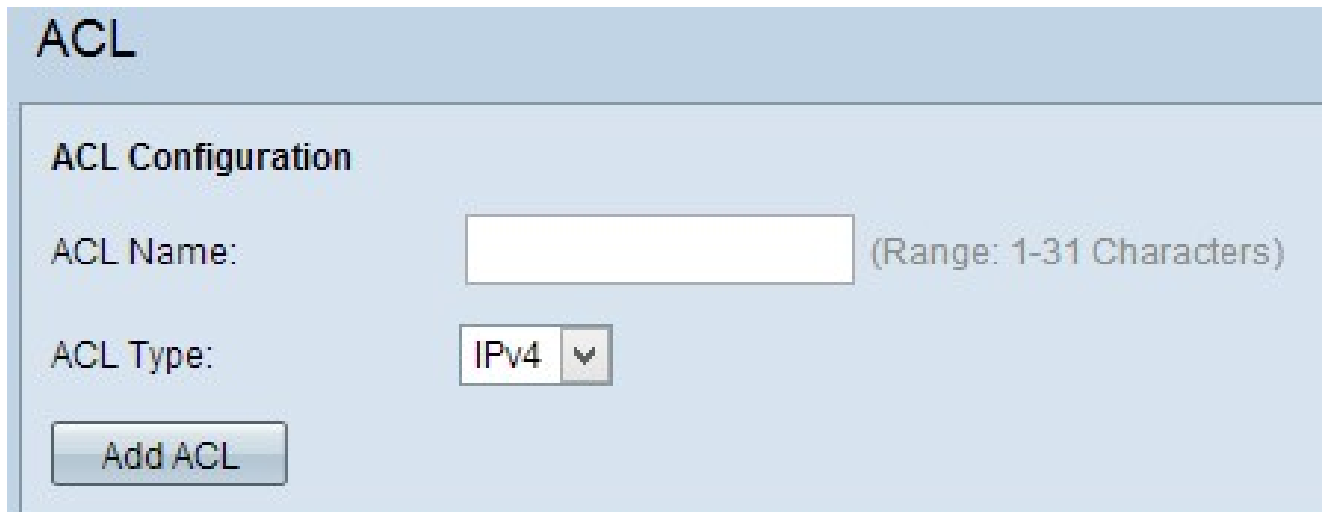
- v1.0.3.4

## Configuración de ACL basada en IPv4

Las ACL IP clasifican el tráfico para las Capas 3 en la pila IP. Cada ACL es un conjunto de hasta 10 reglas que se aplican al tráfico enviado desde un cliente inalámbrico o que debe recibir 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 se pueden basar en varios criterios y se pueden aplicar a uno o más campos dentro de un paquete, como la dirección IP de origen o destino, el puerto de origen o destino o el protocolo transportado en el paquete.

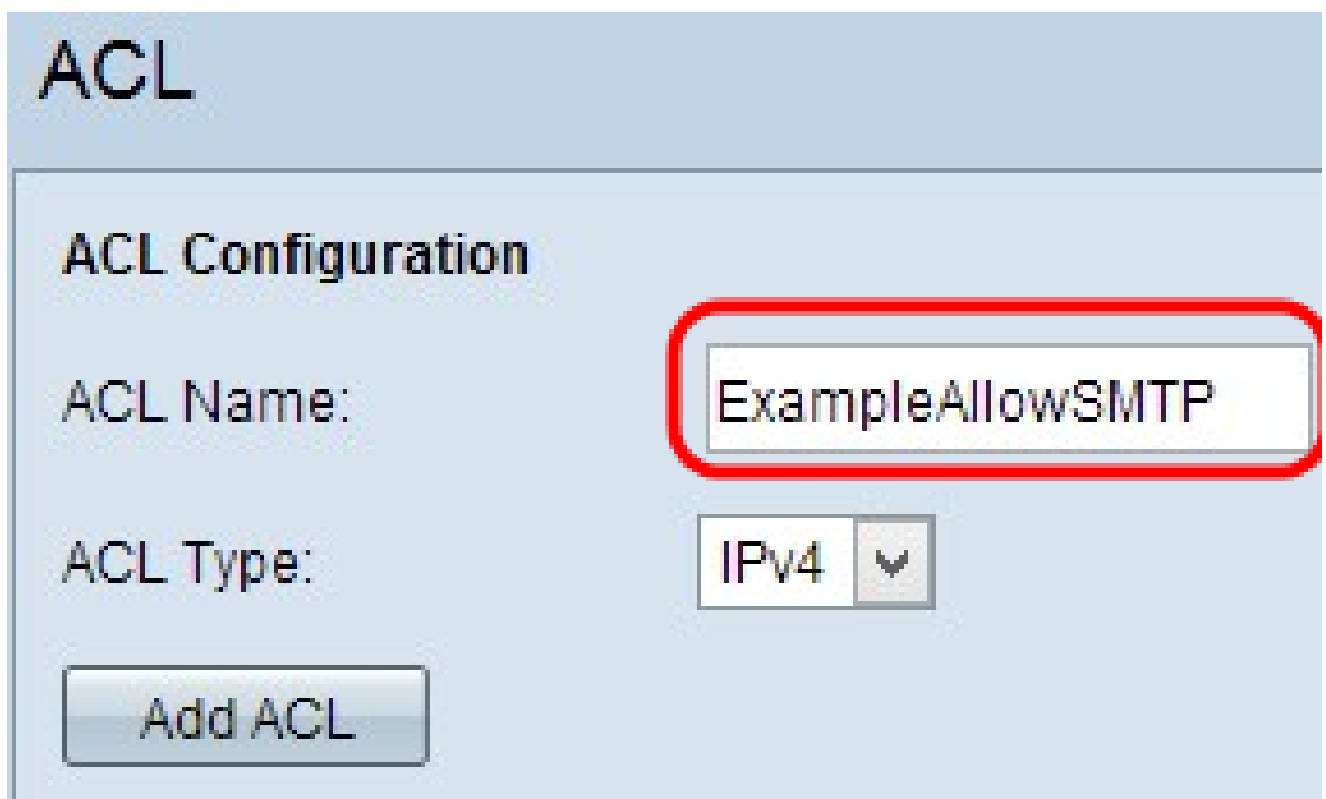
## Creación de ACL IPv4

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



The screenshot shows the 'ACL Configuration' section of a web interface. It features a title 'ACL' at the top left. Below it, the 'ACL Configuration' section contains two input fields: 'ACL Name:' with an empty text box and '(Range: 1-31 Characters)' to its right, and 'ACL Type:' with a dropdown menu currently set to 'IPv4'. At the bottom left of this section is a button labeled 'Add ACL'.

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



This screenshot is identical to the previous one, but the 'ACL Name' text box now contains the text 'ExampleAllowSMTP'. This text box is highlighted with a red rounded rectangular border. The 'ACL Type' dropdown remains set to 'IPv4' and the 'Add ACL' button is still visible at the bottom left.

Paso 3. Elija el tipo IPv4 para la ACL en la lista desplegable Tipo de ACL.

## ACL

### ACL Configuration

ACL Name:  (Range: 1-31 Characters)

ACL Type:

IPv4 ▼  
IPv4  
IPv6  
MAC

Add ACL

Paso 4. Haga clic en Agregar ACL para crear una nueva ACL IPv4.

## ACL

### ACL Configuration

ACL Name:  (Range: 1-31 Characters)

ACL Type:

IPv4 ▼

Add ACL

## Configuración de una regla para ACL IPv4

Paso 1. Elija la ACL de la lista desplegable Nombre de ACL-Tipo de ACL para la que deben configurarse las reglas.

### ACL Rule Configuration

ACL Name - ACL Type: ExampleAllowSMTP - IPv4 ▼

Rule: New Rule ▼

---

Action: Deny ▼

Match Every Packet:

Paso 2. Si debe configurarse una nueva regla para la ACL elegida, elija Nueva regla en la lista desplegable Regla; de lo contrario, elija una de las reglas presentes en la lista desplegable Regla.

### ACL Rule Configuration

ACL Name - ACL Type: ExampleAllowSMTP - IPv4 ▼

Rule: New Rule ▼

---

Action: Deny ▼

Match Every Packet:

Nota: Se pueden crear un máximo de 10 reglas para una sola ACL.

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

## ACL

**ACL Configuration**

ACL Name:  (Range: 1-31 Characters)

ACL Type:

---

**ACL Rule Configuration**

ACL Name - ACL Type:

Rule:

---

Action:  (Dropdown menu with options: Deny, Deny, Permit)

Match Every Packet:

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

Source IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:

Las opciones disponibles se describen de la siguiente manera:

- Denegar: bloquea todo el tráfico que cumpla los criterios de la regla para entrar o salir del dispositivo WAP.
- Permitir: permite que todo el tráfico que cumpla los criterios de la regla entre o salga del dispositivo WAP.

Paso 4. Marque la casilla de verificación Match Every Packet para hacer coincidir la regla para cada trama o paquete independientemente de su contenido. Si desea configurar un criterio de coincidencia específico, desmarque la casilla de verificación Match Every Packet.

**ACL Rule Configuration**

ACL Name - ACL Type:

Rule:

---

Action:

**Match Every Packet:**

Protocol:   Select From List:   Match to Value:  (Range)

Source IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port:   Select From List:   Match to Port:  (Range)

Destination IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port:   Select From List:   Match to Port:  (Range)

**Service Type**

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

IP Precedence:   (Range: 0 - 7)

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

Delete ACL:

Ahorro de tiempo: si marca la casilla de verificación Coincidir con cada paquete, vaya al [paso 13](#).

Paso 5. (Opcional) Marque la casilla de verificación Protocol para la 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 marcada, haga clic en uno de estos botones de opción.

**ACL Rule Configuration**

ACL Name - ACL Type:

Rule:

---

Action:

Match Every Packet:

Protocol:   Select From List:   Match to Value:  (Range: )

Source IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port:   Select From List:   Match to Port:  (Range: )

Destination IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port:   Select From List:   Match to Port:  (Range: )

**Service Type**

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

Las opciones se describen de la siguiente manera:

- **Seleccionar de la lista:** elija un protocolo de la lista desplegable **Seleccionar de la lista**. La lista desplegable tiene los protocolos ip, icmp, igmp, tcp y udp.
- **Coincidencia con valor:** para protocolo no presentado en la lista. Introduzca un ID de protocolo asignado por IANA estándar de 0 a 255.

**Paso 6. (Opcional)** 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. La máscara comodín le permite especificar a qué host de la dirección IP de origen se aplica esta lista de acceso.

**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)

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)

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: 0 - 255)

Delete ACL:

Paso 7. (Opcional) Marque la casilla de verificación Puerto de Origen para incluir un puerto de origen en la condición de coincidencia. Si la casilla de verificación Source Port está marcada, haga clic en uno de estos botones de opción.



**ACL Rule Configuration**

ACL Name - ACL Type:

Rule:

---

Action:

Match Every Packet:

Protocol:   Select From List:   Match to Value:  (Range: )

Source IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port:   Select From List:   Match to Port:  (Range: )

Destination IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port:   Select From List:   Match to Port:  (Range: )

**Service Type**

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

IP Precedence:   (Range: 0 - 7)

- Seleccionar de la lista: elija un puerto de origen de la lista desplegable Seleccionar de la lista. La lista desplegable tiene puertos ftp, ftpdata, http, smtp, snmp, telnet, tftp y www.

**ACL Rule Configuration**

ACL Name - ACL Type:

Rule:

---

Action:

Match Every Packet:

Protocol:   Select From List:   Match to Value:  (Range: )

Source IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port:   Select From List:   Match to Port:  (Range: )

Destination IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port:   Select From List:   Match to Port:  (Range: )

- Coincidir con puerto: para el puerto de origen no presentado en la lista. Introduzca el número de puerto, que oscila entre 0 y 65535.

Paso 8. (Opcional) Active la casilla de verificación Dirección IP de destino para incluir la dirección IP del destino en la condición de coincidencia. Introduzca la dirección IP y la máscara comodín del destino en sus campos respectivos. La máscara comodín le permite especificar a qué host de la dirección IP de destino se aplica esta lista de acceso.

The screenshot shows a configuration window for an Access Control List (ACL). The 'Action' is set to 'Deny'. The 'Match Every Packet' checkbox is unchecked. The 'Protocol' is set to 'ip'. The 'Source IP Address' is '192.168.10.0' with a wildcard mask of '0.0.0.255'. The 'Source Port' is set to 'ftp'. The 'Destination IP Address' is '192.168.20.0' with a wildcard mask of '0.0.0.255', which is highlighted with a red box. The 'Destination Port' is not set. The 'Service Type' is not set. The 'IP DSCP', 'IP Precedence', and 'IP TOS Bits' are not set. The 'Delete ACL' checkbox is unchecked. A 'Save' button is at the bottom.

Paso 9. (Opcional) 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 marcada, haga clic en uno de estos botones de opción.

Action:

Match Every Packet:

Protocol:   Select From List:   Match to Value:  (Range: )

Source IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port:   Select From List:   Match to Port:  (Range: )

Destination IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port:   Select From List:   Match to Port:  (Range: )

**Service Type**

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

IP Precedence:   (Range: 0 - 7)

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

Delete ACL:

- Seleccionar de la lista: elija un puerto de destino de la lista desplegable Seleccionar de la lista. La lista desplegable tiene puertos ftp, ftpdata, http, smtp, snmp, telnet, tftp y www.

Action:

Match Every Packet:

Protocol:   Select From List:   Match to Value:  (Range: )

Source IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port:   Select From List:   Match to Port:  (Range: )

Destination IP Address:   (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port:   Select From List:   Match to Port:  (Range: )

**Service Type**

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

IP Precedence:   (Range: 0 - 7)

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

Delete ACL:

- Coincidencia con puerto: para el puerto de destino no presentado en la lista. Introduzca el número de puerto, que oscila entre 0 y 65535, en el campo Coincidir con puerto.

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

Paso 10. (Opcional) Marque la casilla de verificación IP DSCP para hacer coincidir los paquetes basados en los valores de IP DSCP. Si la casilla de verificación IP DSCP está marcada, haga clic en uno de estos botones de opción. DSCP se utiliza para especificar las prioridades de tráfico sobre el encabezado IP de la trama. Esto categoriza todos los paquetes para el flujo de tráfico asociado con el valor DSCP IP que seleccione de la lista. Para obtener más información sobre DSCP, consulte [aquí](#).

The screenshot shows the 'ACL Rule Configuration' window. The 'ACL Name - ACL Type' is set to 'User1 - IPv4'. The 'Rule' is 'New Rule'. The 'Action' is 'Deny'. The 'Match Every Packet' checkbox is unchecked. The 'Protocol' is checked and set to 'Select From List'. The 'Source IP Address' is checked and set to '192.168.10.0'. The 'Source Port' is checked and set to 'Select From List'. The 'Destination IP Address' is checked and set to '192.168.20.0'. The 'Destination Port' is checked and set to 'Select From List'. The 'Service Type' is 'IP DSCP', which is checked and set to 'Select From List'. The 'IP DSCP' dropdown menu is open, showing a list of values: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs0, cs1, cs2, cs3, cs4, cs5, cs6. The value 'af11' is selected and highlighted in blue. The 'IP Precedence' and 'IP TOS Bits' checkboxes are unchecked. The 'Delete ACL' checkbox is unchecked. A 'Save' button is at the bottom.

- Seleccionar de la lista: elija un valor de DSCP IP de la lista desplegable Seleccionar de la lista. La lista desplegable tiene valores de reenvío garantizado (AS), clase de servicio (CS) o reenvío acelerado (EF) de DSCP.

- Coincidir con valor: para personalizar los valores DSCP. Introduzca el valor DSCP, que oscila entre 0 y 63, en el campo Coincidir con el valor.

Paso 11. (Opcional) Active 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 marcada, introduzca un valor de precedencia IP que oscile entre 0 y 7. Para obtener más información sobre la precedencia de IP, consulte [aquí](#).

**Service Type**

IP DSCP:   Select From List:   Match to Value: 24 (R)

IP Precedence:  5 (Range: 0 - 7)

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

Delete ACL:

Save

Paso 12. (Opcional) Marque la casilla de verificación IP TOS Bits para utilizar los bits de tipo de servicio del paquete en el encabezado IP como criterios de coincidencia. Si la casilla de verificación IP TOS Bits está marcada, introduzca los bits de TOS IP que oscilan entre 00-FF y la máscara TOS IP que oscilan entre 00-FF en los campos respectivos.

**Service Type**

IP DSCP:   Select From List:   Match to Value: 24 (R)

IP Precedence:  5 (Range: 0 - 7)

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

Delete ACL:

Save

Paso 13. (Opcional) Si desea eliminar la ACL configurada, marque la casilla de verificación Eliminar ACL.

**Service Type**

IP DSCP:   Select From List:   Match to Value:  (R:

IP Precedence:   (Range: 0 - 7)

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

Delete ACL:

Save

Paso 14. Haga clic en Guardar para guardar la configuración.

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).