

Configuración de la lista de control de acceso (ACL) basada en IPv4 y la entrada de control de acceso (ACE) en un switch

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. Bloquea o permite a los usuarios acceder a recursos específicos. Una ACL contiene los hosts a los que se les permite o deniega el acceso al dispositivo de red.

La ACL basada en IPv4 es una lista de direcciones IPv4 de origen que utilizan información de capa 3 para permitir o denegar el acceso al tráfico. Las ACL IPv4 restringen el tráfico relacionado con IP en función de los filtros IP configurados. Un filtro contiene las reglas para coincidir con un paquete IP, y si el paquete coincide, la regla también estipula si el paquete debe ser permitido o denegado.

Una entrada de control de acceso (ACE) contiene los criterios reales de la regla de acceso. Una vez creada la ACE, se aplica a una ACL.

Debe utilizar listas de acceso para proporcionar un nivel básico de seguridad para acceder a la red. Si no configura las listas de acceso en los dispositivos de red, todos los paquetes que pasan a través del switch o el router podrían estar permitidos en todas las partes de la red.

Este artículo proporciona instrucciones sobre cómo configurar ACL y ACE basadas en IPv4 en el switch gestionado.

Dispositivos aplicables

- Serie Sx350
- Serie SG350X
- Serie Sx500
- Serie Sx550X

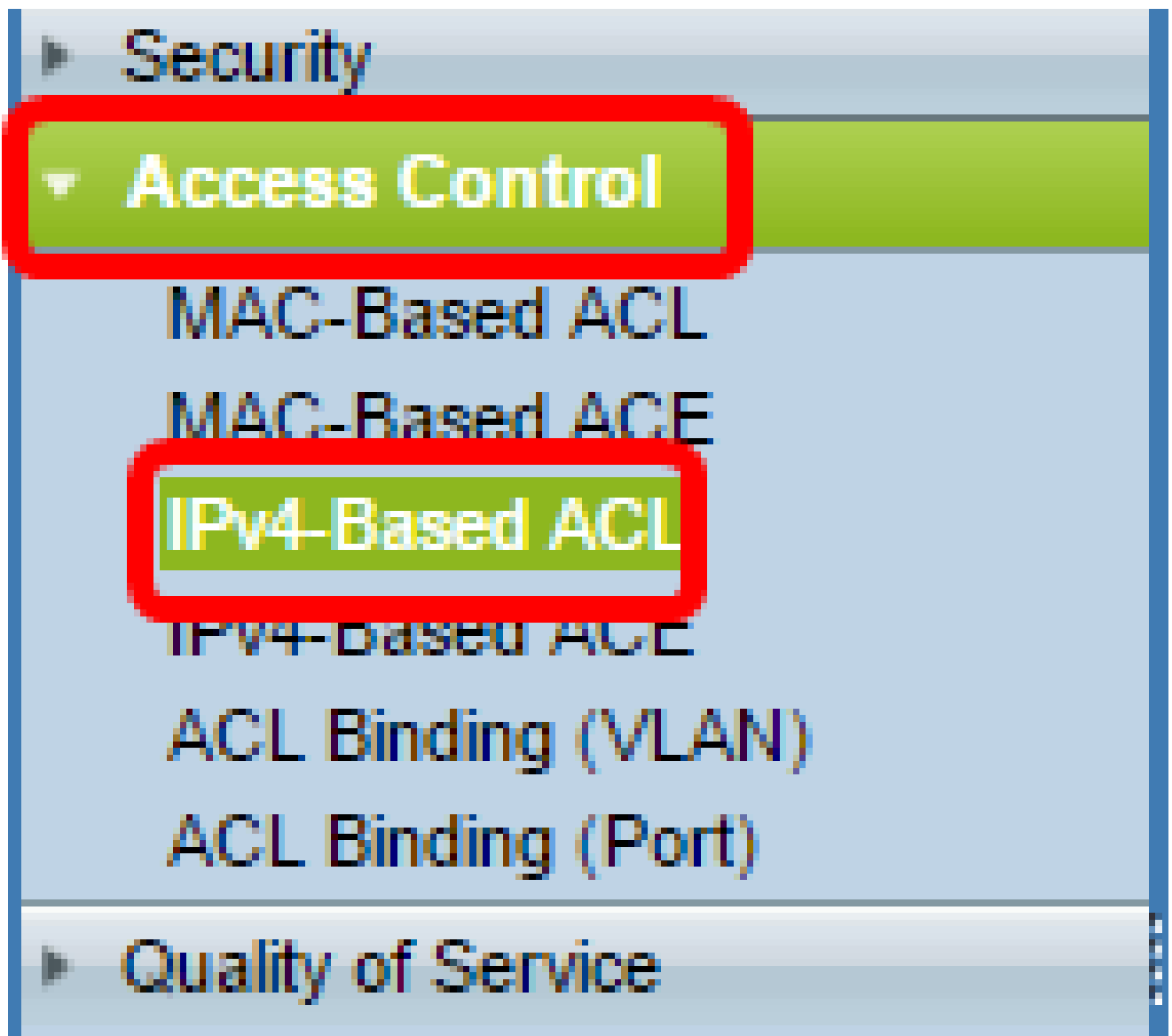
Versión del software

- 1.4.5.02 - Serie Sx500
- 2.2.5.68 - Serie Sx350, Serie SG350X, Serie Sx550X

Configuración de ACL y ACE basadas en IPv4

Configuración de ACL basada en IPv4

Paso 1. Inicie sesión en la utilidad basada en Web y vaya a Control de acceso > ACL basada en IPv4.



Paso 2. 'Haga clic en el botón Add (Agregar).'

IPv4-Based ACL

IPv4-Based ACL Table



ACL Name

0 results found.

Add...

Delete

IPv4-Based ACE Table

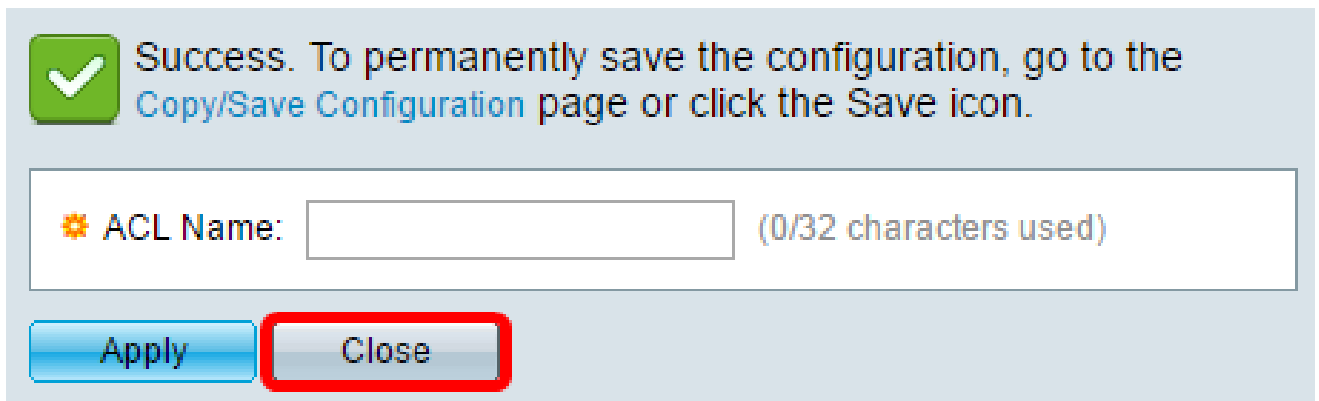
Paso 3. Ingrese el nombre de la nueva ACL en el campo ACL Name.

ACL Name: (8/32 characters used)

Apply Close

Nota: En este ejemplo, se utiliza ACL IPv4.

Paso 4. Haga clic en Aplicar y luego en Cerrar.



Success. To permanently save the configuration, go to the [Copy/Save Configuration](#) page or click the Save icon.

⚙️ ACL Name: (0/32 characters used)

Paso 5. (Opcional) Haga clic en Guardar para guardar los ajustes en el archivo de configuración de inicio.



MP 48-Port Gigabit PoE Stackable Managed Switch

IPv4-Based ACL

IPv4-Based ACL Table

<input type="checkbox"/>	ACL Name
<input type="checkbox"/>	IPv4 ACL

Ahora debería haber configurado una ACL basada en IPv4 en su switch.

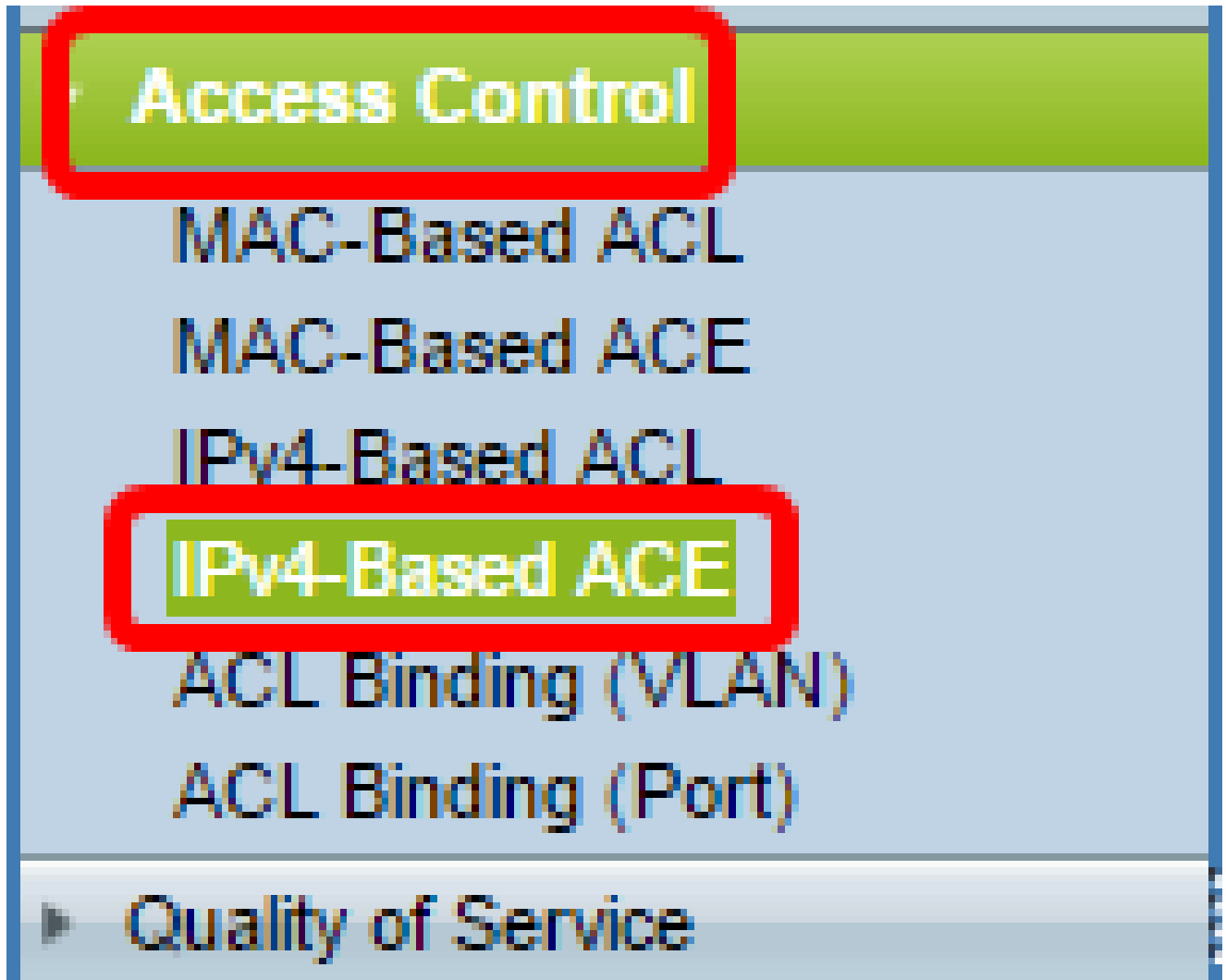
Configuración de ACE basada en IPv4

Cuando se recibe un paquete en un puerto, el switch procesa el paquete a través de la primera ACL. Si el paquete coincide con un filtro ACE de la primera ACL, tiene lugar la acción ACE. Si el paquete no coincide con ninguno de los filtros ACE, se procesa la siguiente ACL. Si no se encuentra ninguna coincidencia con ninguna ACE en todas las ACL relevantes, el paquete se descarta de forma predeterminada.

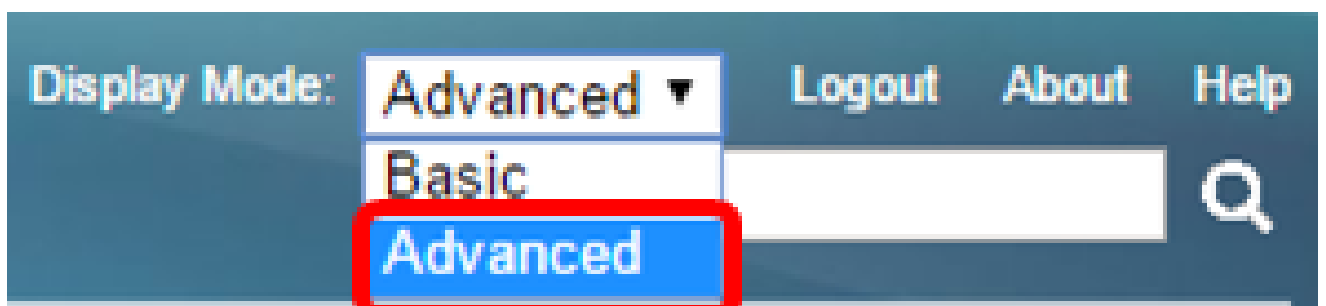
En esta situación, se creará una ACE para denegar el tráfico enviado desde una dirección IPv4 de origen definida por el usuario específica a cualquier dirección de destino.

Nota: Esta acción predeterminada se puede evitar mediante la creación de una ACE de baja prioridad que permita todo el tráfico.

Paso 1. En la utilidad basada en Web, vaya a Control de acceso > ACE basada en IPv4.



Importante: para aprovechar al máximo las funciones disponibles del conmutador, cambie al modo avanzado seleccionando Avanzado en la lista desplegable Modo de visualización de la esquina superior derecha de la página.



Paso 2. Elija una ACL de la lista desplegable Nombre de ACL y haga clic en Ir.

IPv4-Based ACE

IPv4-Based ACE Table

Filter: ACL Name equals to **IPv4 ACL** Go

<input type="checkbox"/>	Priority	Action	Logging	Source IP Address	Destination IP Address
				IP Address Wildcard Mask	IP Address Wildcard Mask
0 results found.					

Add... Edit... Delete

Flag Set presents the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represented as 1, ur

IPv4-Based ACL Table

Nota: Las ACE que ya están configuradas para la ACL se mostrarán en la tabla.

Paso 3. Haga clic en el botón Add para agregar una nueva regla a la ACL.

Nota: El campo Nombre de ACL muestra el nombre de la ACL.

Paso 4. Introduzca el valor de prioridad para la ACE en el campo Priority. Las ACE con un valor de prioridad más alto se procesan primero. El valor 1 es la prioridad más alta. Tiene un rango de 1 a 2147483647.

ACL Name: IPv4 ACL

Priority: (Range: 1 - 2147483647)

Action: Permit Deny Shutdown

Logging: Enable

Protocol: Any (IP) Select from list Protocol ID to match (Range: 0 - 255)

Nota: En este ejemplo, se utiliza 2.

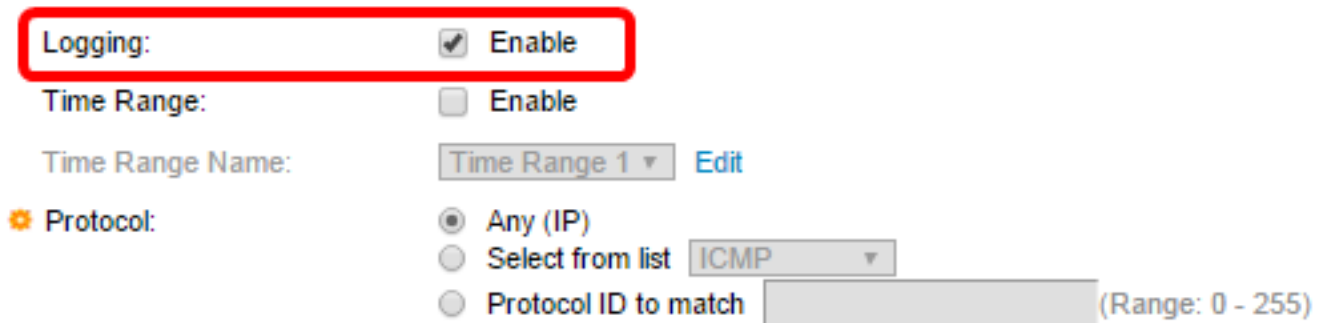
Paso 5. Haga clic en el botón de opción correspondiente a la acción deseada que se realiza cuando una trama cumple los criterios requeridos de la ACE.

Nota: En este ejemplo, se elige Permitir.

- Permitir: el switch reenvía paquetes que cumplen los criterios requeridos de la ACE.
- Deny: el switch descarta paquetes que cumplen con los criterios requeridos de la ACE.
- Apagar: el switch descarta paquetes que no cumplen los criterios requeridos de la ACE e inhabilita el puerto donde se recibieron los paquetes.

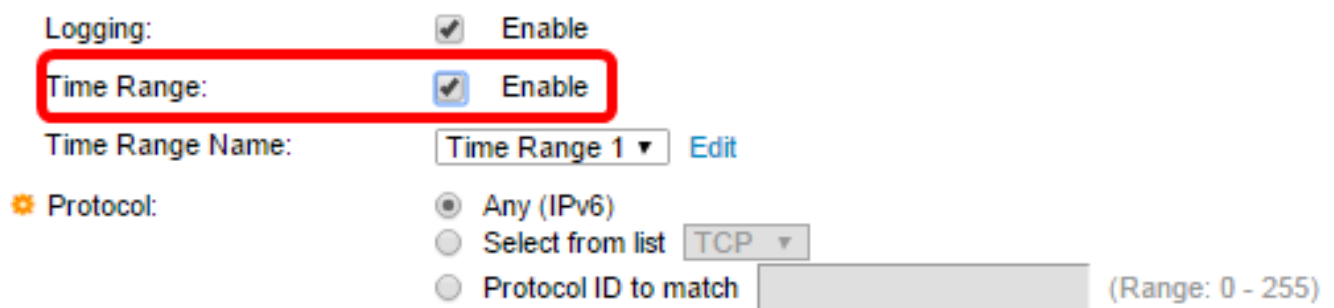
Nota: Los puertos desactivados se pueden reactivar en la página Port Settings (Configuración de puertos).

Paso 6. (Opcional) Marque la casilla de verificación EnableLogging para habilitar el registro de flujos ACL que coincidan con la regla ACL.



The screenshot shows the configuration interface for an ACL rule. The 'Logging' option is checked and labeled 'Enable', highlighted with a red box. Below it, 'Time Range' is unchecked. The 'Time Range Name' is set to 'Time Range 1' with an 'Edit' link. Under 'Protocol', 'Any (IP)' is selected. Other options include 'Select from list' (set to ICMP) and 'Protocol ID to match' (with a range of 0-255).

Paso 7. (Opcional) Marque la casilla de verificación Enable Time Range (Activar rango de tiempo) para permitir que se configure un rango de tiempo para la ACE. Los intervalos de tiempo se utilizan para limitar la cantidad de tiempo que una ACE está en vigor.



The screenshot shows the configuration interface for an ACL rule. The 'Time Range' option is checked and labeled 'Enable', highlighted with a red box. 'Logging' is also checked. The 'Time Range Name' is 'Time Range 1' with an 'Edit' link. Under 'Protocol', 'Any (IPv6)' is selected. Other options include 'Select from list' (set to TCP) and 'Protocol ID to match' (with a range of 0-255).

Paso 8. (Opcional) En la lista desplegable Nombre del rango de tiempo, seleccione un rango de tiempo para aplicarlo a la ACE.

Time Range Name: [Edit](#)

Protocol: Any (IPv6) Select from list Protocol ID to match (Range: 0 - 255)

Nota: Puede hacer clic en Editar para navegar y crear un rango de tiempo en la página Rango de Tiempo.

Time Range Name: (12/32 characters used)

Absolute Starting Time: Immediate Date Time HH:MM

Absolute Ending Time: Infinite Date Time HH:MM

Paso 9. Elija un tipo de protocolo en el área Protocolo. La ACE se creará en función de un protocolo o ID de protocolo específico.

Protocol: Any (IP) Select from list Protocol ID to match (Range: 0 - 255)

Las opciones son:

- Any (IP): esta opción configurará la ACE para que acepte todos los protocolos IP.
- Seleccionar de la lista: esta opción le permitirá elegir un protocolo de una lista desplegable. Si prefiere esta opción, vaya directamente al [paso 10](#).
- Protocol ID to match (ID de protocolo que coincide): esta opción le permitirá introducir un ID de protocolo. Si prefiere esta opción, vaya directamente al [paso 11](#).

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

Paso 10. (Opcional) Si selecciona Seleccionar de la lista en el Paso 9, elija un protocolo de la lista desplegable.

- L2TP: protocolo de tunelización de capa 2

Paso 11. (Opcional) Si selecciona Protocol ID (Identificador de protocolo) para que coincida en el Paso 9, ingrese el ID de protocolo en el campo Protocol ID to match (Identificador de protocolo para que coincida).

Protocol: Any (IP) Select from list ICMP Protocol ID to match 1 (Range: 0 - 255)

Paso 12. Haga clic en el botón de opción que corresponda a los criterios deseados de la ACE en el área Dirección IP de origen.

Source IP Address:

Any User Defined

Las opciones son:

- Cualquiera: todas las direcciones IPv4 de origen se aplican a la ACE.
- Definido por el usuario: introduzca una dirección IP y una máscara comodín IP que se aplicarán a la ACE en los campos Source IP Address Value y Source IP Wildcard Mask. Las máscaras comodín se utilizan para definir un intervalo de direcciones IP.

Nota: En este ejemplo, se elige Definido por el usuario. Si selecciona Any (Cualquiera), vaya al [paso 15](#).

Paso 13. Introduzca la dirección IP de origen en el campo Source IP Address Value.

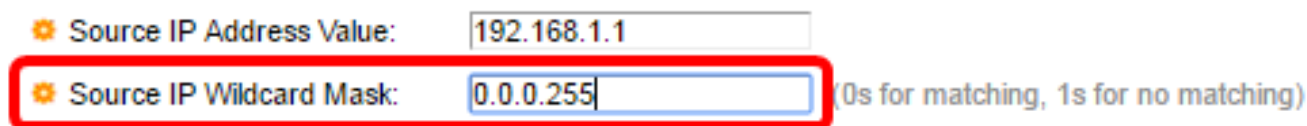
Source IP Address: Any User Defined

Source IP Address Value: 192.168.1.1

Source IP Wildcard Mask: (0s for matching, 1s for no matching)

Nota: En este ejemplo, se utiliza 192.168.1.1.

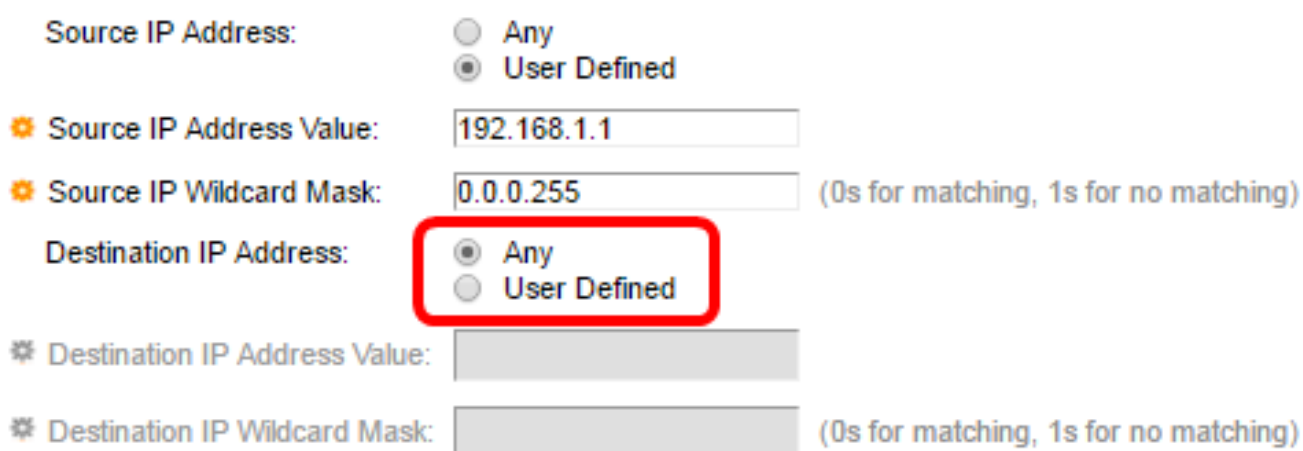
Paso 14. Introduzca la máscara comodín de origen en el campo Máscara comodín IP de origen.



Source IP Address Value: 192.168.1.1
Source IP Wildcard Mask: 0.0.0.255 (0s for matching, 1s for no matching)

Nota: En este ejemplo, se utiliza 0.0.0.255.

Paso 15. Haga clic en el botón de opción que corresponda a los criterios deseados de la ACE en el área Dirección IP de destino.



Source IP Address: Any User Defined
Source IP Address Value: 192.168.1.1
Source IP Wildcard Mask: 0.0.0.255 (0s for matching, 1s for no matching)
Destination IP Address: Any User Defined
Destination IP Address Value: [disabled]
Destination IP Wildcard Mask: [disabled] (0s for matching, 1s for no matching)

Las opciones son:

- Cualquiera: todas las direcciones IPv4 de destino se aplican a la ACE.
- Definido por el usuario: introduzca una dirección IP y una máscara comodín IP que se aplicarán a la ACE en los campos Valor de dirección IP de destino y Máscara comodín de IP de destino. Las máscaras comodín se utilizan para definir un intervalo de direcciones IP.

Nota: En este ejemplo, se elige Any (Cualquiera). Al elegir esta opción, la ACE que se creará permitirá el tráfico ACE procedente de la dirección IPv4 especificada a cualquier destino.

Paso 16. (Opcional) Haga clic en un botón de opción del área Puerto de origen. El valor predeterminado es Any.

Source Port:
 Any
 Single from list
 Single by number (Range: 0 - 65535)
 Range -

Destination Port:
 Any
 Single from list
 Single by number (Range: 0 - 65535)
 Range -

- Cualquiera: coincide con todos los puertos de origen.
- Único de la lista: puede elegir un único puerto de origen TCP/UDP con el que se comparan los paquetes. Este campo solo está activo si se selecciona 800/6-TCP o 800/17-UDP en el menú desplegable Select from List (Seleccionar de la lista).
- Único por número: puede elegir un único puerto de origen TCP/UDP con el que coincidan los paquetes. Este campo solo está activo si se selecciona 800/6-TCP o 800/17-UDP en el menú desplegable Select from List (Seleccionar de la lista).
- Rango: puede elegir un rango de puertos de origen TCP/UDP con los que se hace coincidir el paquete. Se pueden configurar ocho intervalos de puertos diferentes (compartidos entre los puertos de origen y de destino). Los protocolos TCP y UDP tienen ocho intervalos de puertos cada uno.

Paso 17. (Opcional) Haga clic en un botón de opción del área Puerto de destino. El valor predeterminado es Any.

- Cualquiera: coincidencia con todos los puertos de origen
- Único de la lista: puede elegir un único puerto de origen TCP/UDP con el que se comparan los paquetes. Este campo solo está activo si se selecciona 800/6-TCP o 800/17-UDP en el menú desplegable Select from List (Seleccionar de la lista).
- Único por número: puede elegir un único puerto de origen TCP/UDP con el que coincidan los paquetes. Este campo solo está activo si se selecciona 800/6-TCP o 800/17-UDP en el menú desplegable Select from List (Seleccionar de la lista).
- Rango: puede elegir un rango de puertos de origen TCP/UDP con los que se hace coincidir el paquete. Se pueden configurar ocho intervalos de puertos diferentes (compartidos entre los puertos de origen y de destino). Los protocolos TCP y UDP tienen ocho intervalos de puertos cada uno.

Paso 18. (Opcional) En el área Indicadores TCP, elija uno o más indicadores TCP con los que filtrar paquetes. Los paquetes filtrados se reenvían o se descartan. Filtrar paquetes mediante indicadores TCP aumenta el control de paquetes, lo que aumenta la seguridad de la red.

- Definir: coincidencia si el indicador está definido.
- Desactivado: Coincidir si el indicador no está definido.

- No importa: ignore el indicador TCP.

Urg:	Ack:	Psh:	Rst:	Syn:	Fin:
<input type="radio"/> Set	<input type="radio"/> Set	<input checked="" type="radio"/> Set	<input type="radio"/> Set	<input type="radio"/> Set	<input type="radio"/> Set
<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset	<input type="radio"/> Unset
<input checked="" type="radio"/> Don't care	<input checked="" type="radio"/> Don't care	<input type="radio"/> Don't care	<input checked="" type="radio"/> Don't care	<input checked="" type="radio"/> Don't care	<input checked="" type="radio"/> Don't care

Los indicadores TCP son:

- Urg: este indicador se utiliza para identificar los datos entrantes como Urgente.
- Ack: este indicador se utiliza para confirmar la recepción correcta de paquetes.
- Psh: este indicador se utiliza para garantizar que los datos tienen la prioridad (que merecen) y se procesan en el extremo de envío o recepción.
- Rst: este indicador se utiliza cuando llega un segmento que no está pensado para la conexión actual.
- Syn: este indicador se utiliza para las comunicaciones TCP.
- Fin: este indicador se utiliza cuando la comunicación o la transferencia de datos ha finalizado.

Paso 19. (Opcional) Haga clic en el tipo de servicio del paquete IP en el área Tipo de servicio.

Type of Service:

Any

DSCP to match (Range: 0 - 63)

IP Precedence to match (Range: 0 - 7)

ICMP:

Any

Select from list

ICMP Type to match (Range: 0 - 255)

ICMP Code:

Any

User Defined (Range: 0 - 255)

IGMP:

Any

Select from list

IGMP Type to match (Range: 0 - 255)

Las opciones son:

• Type of Service:

- Any
- DSCP to match (Range: 0 - 63)
- IP Precedence to match (Range: 0 - 7)

- Cualquiera: puede ser cualquier tipo de servicio para la congestión del tráfico.
- DSCP para igualar: DSCP es un mecanismo para clasificar y administrar el tráfico de red. Se utilizan seis bits (0-63) para seleccionar el comportamiento por salto que un paquete experimenta en cada nodo.
- Precedencia de IP a igualar: la precedencia de IP es un modelo de tipo de servicio (TOS) que la red utiliza para ayudar a proporcionar los compromisos de calidad de servicio (QoS) adecuados. Este modelo utiliza los tres bits más significativos del byte de tipo de servicio en el encabezado IP, como se describe en RFC 791 y RFC 1349. La palabra clave con el valor de Preferencia IP es la siguiente:

- 0: para la rutina

- 1 — para prioridad

- 2 — para uso inmediato

- 3 — para flash

- 4 — para flash-override

- 5 — para los

- 6 — para Internet

- 7 — para la red

Paso 20. (Opcional) Si el protocolo IP de la ACL es ICMP, haga clic en el tipo de mensaje ICMP utilizado para filtrar. Elija el tipo de mensaje por nombre o introduzca el número de tipo de mensaje:

- Cualquiera: se aceptan todos los tipos de mensajes.
- Seleccionar de la lista: puede elegir el tipo de mensaje por nombre.
- Tipo ICMP de coincidencia: el número de tipo de mensaje que se utilizará para fines de filtrado. Tiene un rango de 0 a 255.

Paso 21. (Opcional) Los mensajes ICMP pueden tener un campo de código que indica cómo manejar el mensaje. Haga clic en una de las opciones siguientes para configurar si desea filtrar por este código:

- Cualquiera: acepte todos los códigos.
- Definido por el usuario: puede introducir un código ICMP con fines de filtrado. Tiene un rango de 0 a 255.

Paso 22. (Opcional) Si la ACL se basa en IGMP, haga clic en el tipo de mensaje IGMP que se utilizará para filtrar. Elija el tipo de mensaje por nombre o introduzca el número de tipo de mensaje:

- Cualquiera: se aceptan todos los tipos de mensajes.
- Seleccionar de la lista: puede elegir cualquiera de las opciones de la lista desplegable:
- DVMRP: utiliza una técnica de inundación de trayectoria inversa, que envía una copia de un paquete recibido a través de cada interfaz, excepto la interfaz a la que llegó el paquete.
- Consulta de host: envía periódicamente mensajes generales de consulta de host en cada red conectada para obtener información.
- Host-Reply — Responde a la consulta.
- PIM: Protocol Independent Multicast (PIM) se utiliza entre los routers multicast locales y remotos para dirigir el tráfico multicast desde el servidor multicast a muchos clientes multicast.
- Seguimiento: proporciona información sobre cómo unirse y salir de los grupos de multidifusión IGMP.
- Tipo de IGMP coincidente: el número de tipos de mensajes que se utilizarán para filtrar. Tiene un rango de 0 a 255.

Paso 23. Haga clic en Apply y luego en Close. La ACE se crea y se asocia al nombre de la ACL.

Paso 24. Haga clic en Guardar para guardar los parámetros en el archivo de configuración de inicio.

cisco

IPv4-Based ACE

IPv4-Based ACE Table

Filter: *ACL Name* equals to

<input type="checkbox"/>	Priority	Action	Logging	Time Range		Protocol	Source IP Address	
				Name	State		IP Address	Wildcard Mask
<input type="checkbox"/>	2	Permit	Enabled			ICMP	192.168.1.1	0.0.0.255

Flag Set presents the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represent

Ahora debería haber configurado un ACE basado en IPv4 en su switch.

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).