Configure la lista de control de acceso (ACL) basada en IPv4 y la Entrada de control de acceso (ACE) en un conmutador

Objetivo

Una lista de control de acceso (ACL) es filtros de tráfico de una lista de redes y acciones correlacionadas usados para mejorar la Seguridad. Bloquea o permite que los usuarios tengan acceso a los recursos específicos. Un ACL contiene los host se permiten que o acceso negado al dispositivo de red.

El ACL basado en IPv4 es una lista de direccionamientos de la fuente IPv4 que utilicen la información de la capa 3 para permitir que o para negar el acceso trafique. IPv4 ACL restringen el tráfico IP-relacionado basado en los filtros configurados IP. Un filtro contiene las reglas para hacer juego un paquete IP, y si el paquete hace juego, la regla también estipula si se permite o se niega el paquete.

Una Entrada de control de acceso (ACE) contiene los criterios reales de la regla de acceso. Una vez que se crea ACE, se aplica a un ACL.

Usted debe utilizar las Listas de acceso para proporcionar a un nivel de seguridad básico para tener acceso a su red. Si usted no configura las Listas de acceso en sus dispositivos de red, todos los paquetes que pasaban a través del conmutador o del router se podrían permitir sobre todas las partes de su red.

Este artículo proporciona a las instrucciones en cómo configurar el ACL basado en IPv4 y ACE en su conmutador manejado.

Dispositivos aplicables

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

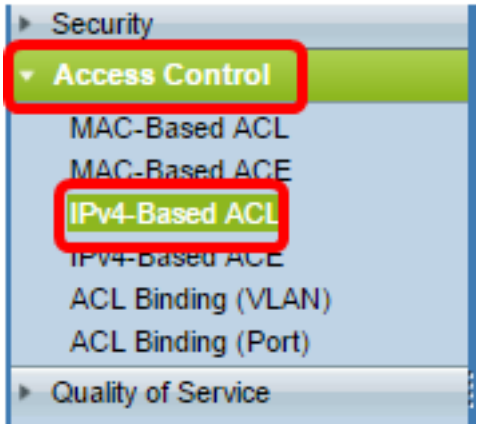
Versión de software

- 1.4.5.02 – Sx500 Series
- 2.2.5.68 – Sx350 Series, serie SG350X, serie Sx550X

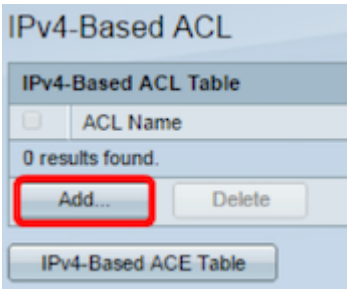
Configure el ACL basado en IPv4 y ACE

Configure el ACL basado en IPv4

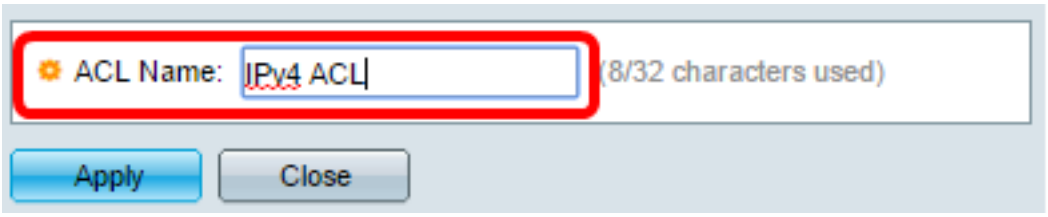
Paso 1. La clave a la utilidad en Internet entonces va al **control de acceso > ACL basado en IPv4**.



Paso 2. Haga clic el **botón Add**.

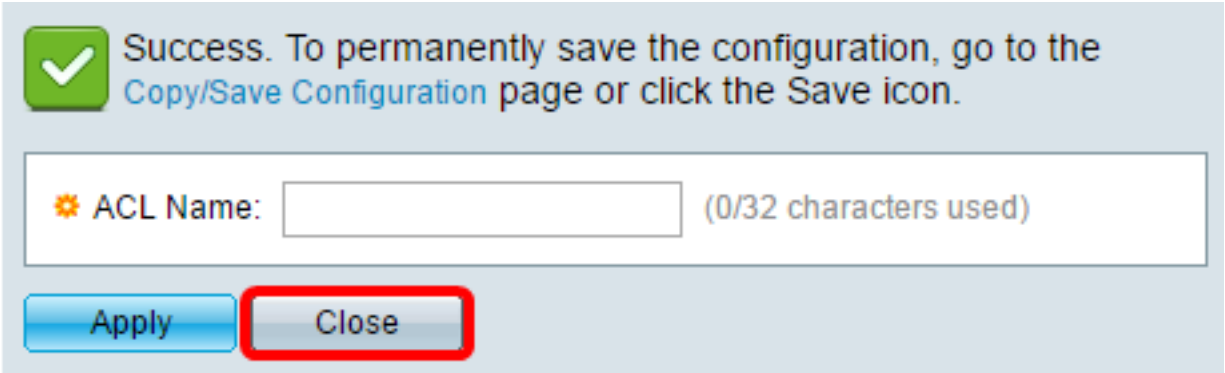


Paso 3. Ingrese el nombre del nuevo ACL en el *campo de nombre ACL*.



Nota: En este ejemplo, se utiliza IPv4 ACL.

Paso 4. El tecleo **se aplica** entonces hace clic **cerca**.



Salvaguardia (opcional) del tecleo del paso 5. para salvar las configuraciones en el fichero de configuración de inicio.

Usted debe ahora haber configurado un ACL basado en IPv4 en su conmutador.

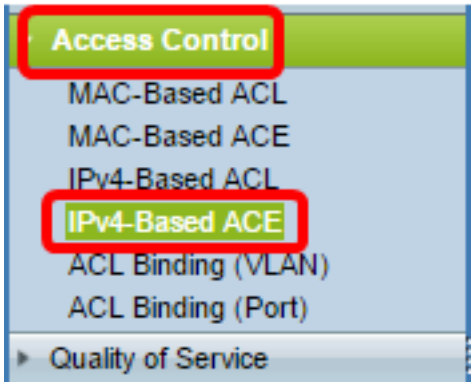
Configure ACE basado en IPv4

Cuando un paquete se recibe en un puerto, el conmutador procesa el paquete con el primer ACL. Si el paquete hace juego un filtro de ACE del primer ACL, la acción de ACE ocurre. Si el paquete no hace juego ningunos de los filtros de ACE, se procesa el ACL siguiente. Si no se encuentra ninguna coincidencia a ningún ACE en todos los ACL relevantes, el paquete se cae por abandono.

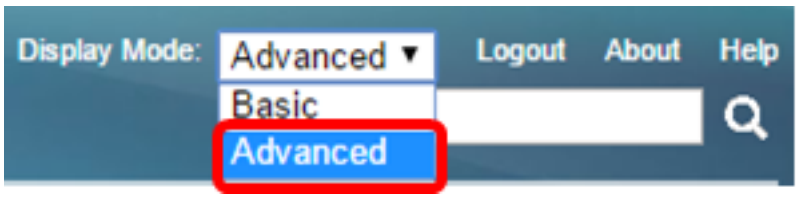
En este decorado, ACE será creado para negar el tráfico que se envía de un direccionamiento definido por el usario específico de la fuente IPv4 a cualquier direccionamiento de destino.

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

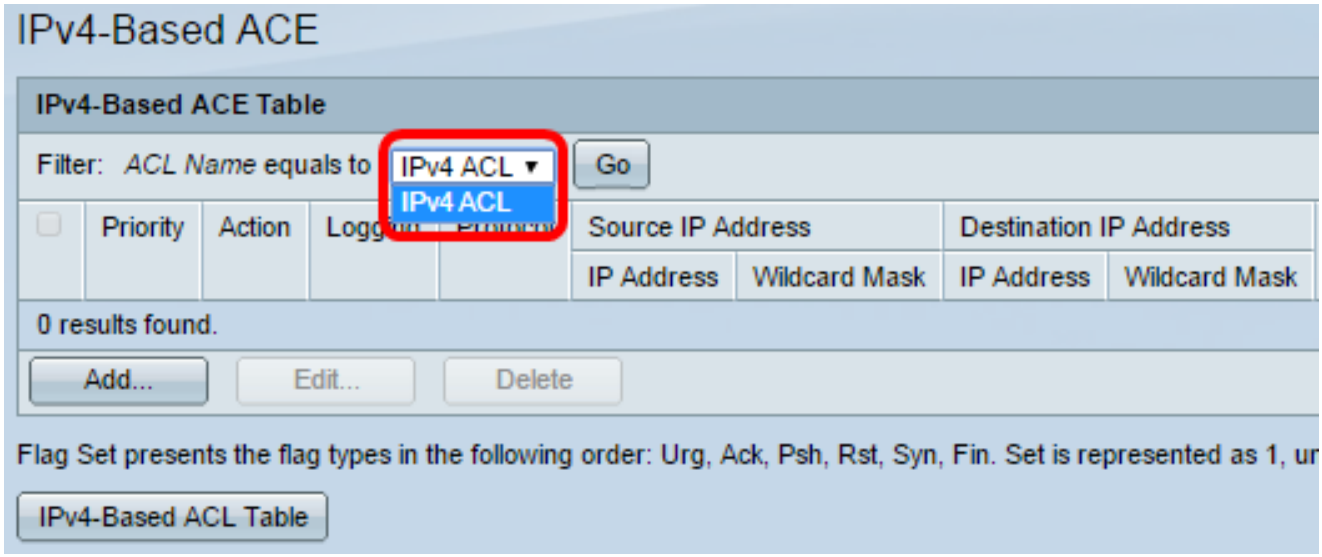
Paso 1. En la utilidad en Internet, va al **control de acceso > ACE basado en IPv4**.



Importante: Para utilizar completamente las características y las funciones disponibles del conmutador, cambie al modo avanzado eligiendo **avanzado de la** lista desplegable del modo de visualización en la esquina superior derecha de la página.



Paso 2. Elija un ACL de la lista desplegable del nombre ACL después haga clic **van**.

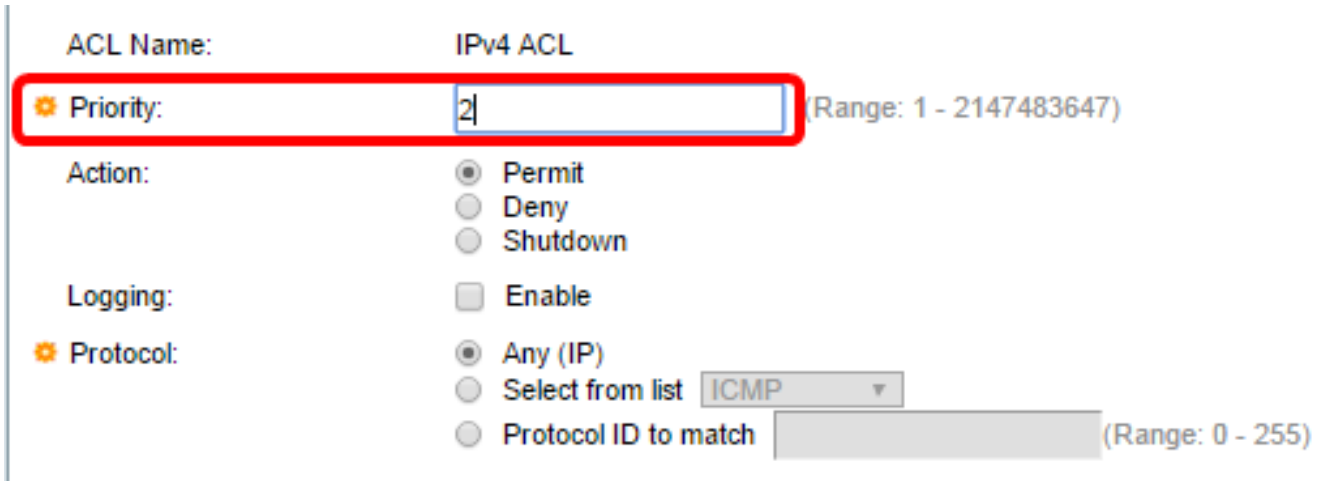


Nota: Los as que se configuran ya para el ACL serán visualizados en la tabla.

Paso 3. Haga clic el **botón Add** para agregar una nueva regla al ACL.

Nota: *El campo de nombre ACL* visualiza el nombre del ACL.

Paso 4. Ingrese el valor de prioridad para el AS en el *campo de prioridad*. Los as con un valor más prioritario se procesan primero. El valor 1 es la prioridad más alta. Tiene un rango de 1 a 2147483647.



Nota: En este ejemplo, se utiliza 2.

Paso 5. Haga clic el botón de radio que corresponde a la acción deseada se toma que cuando un marco cumple los criterios requeridos de ACE.

Nota: En este ejemplo, se elige el permiso.

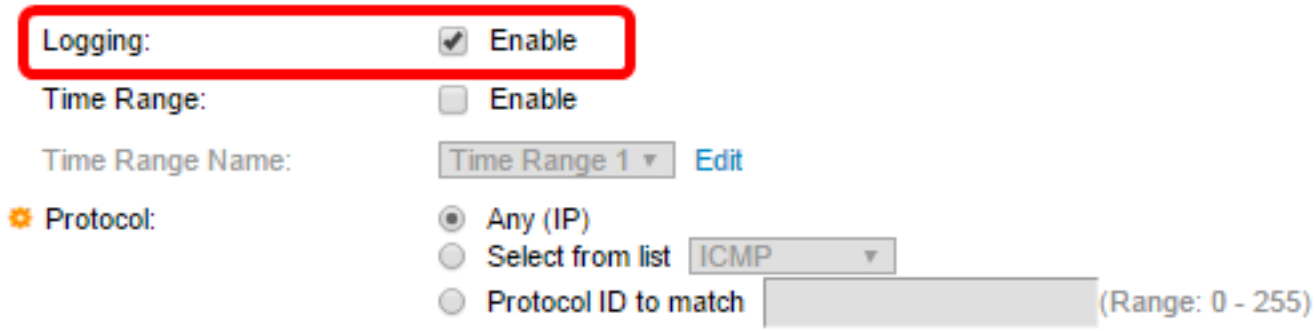
- Permiso — Del conmutador los paquetes adelante que cumplen los criterios requeridos

de ACE.

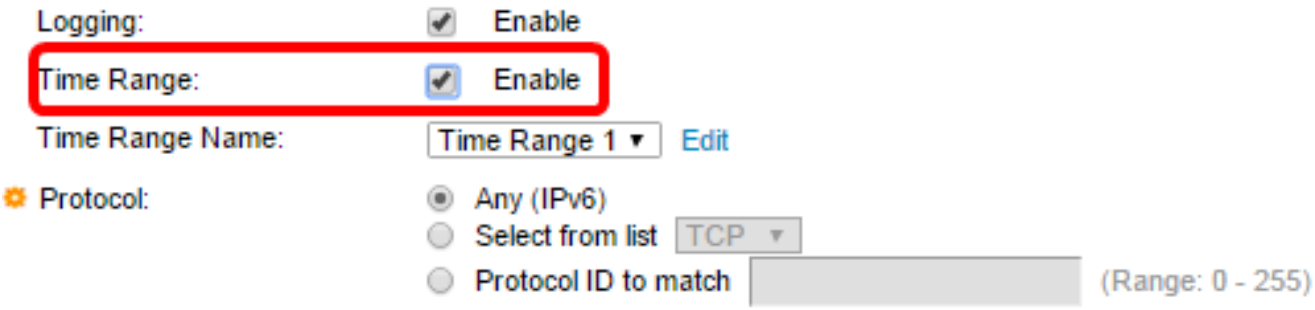
- Niegue — El conmutador cae los paquetes que cumplen los criterios requeridos de ACE.
- Parada normal — El conmutador cae los paquetes que no cumplen los criterios requeridos de ACE y inhabilita el puerto donde los paquetes fueron recibidos.

Nota: Los puertos discapacitados se pueden reactivar en la página de las configuraciones de puerto.

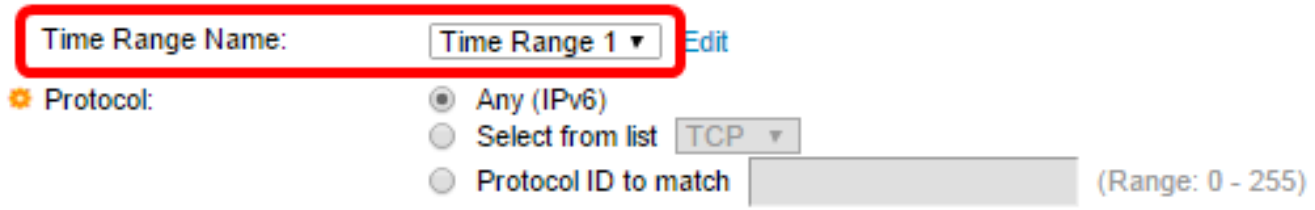
Control (opcional) del paso 6. la casilla de verificación del registro del **permiso** para activar el registro de los flujos ACL que hacen juego la regla ACL.



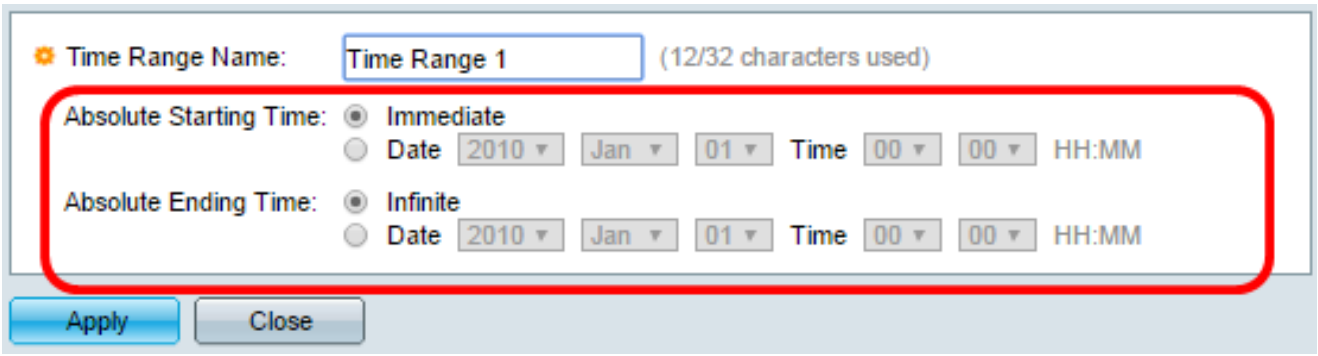
Control (opcional) del paso 7. **Enable time (Habilitar tiempo) la** casilla de verificación del rango para permitir que un rango de tiempo sea configurado a ACE. Los rangos de tiempo se utilizan para limitar la cantidad de tiempo que ACE está en efecto.



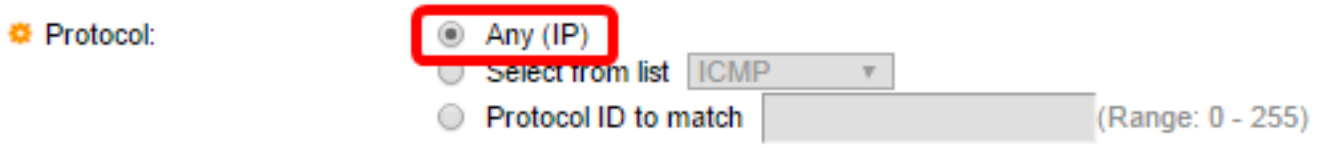
El paso 8. (opcional) de la lista desplegable del nombre del rango de tiempo, elige un rango de tiempo para aplicarse a ACE.



Nota: Usted puede hacer clic **corrige** para navegar y para crear un rango de tiempo en la página del rango de tiempo.



Paso 9. Elija un Tipo de protocolo en el área del protocolo. ACE será creado sobre la base de un protocolo o de un ID del protocolo específico.

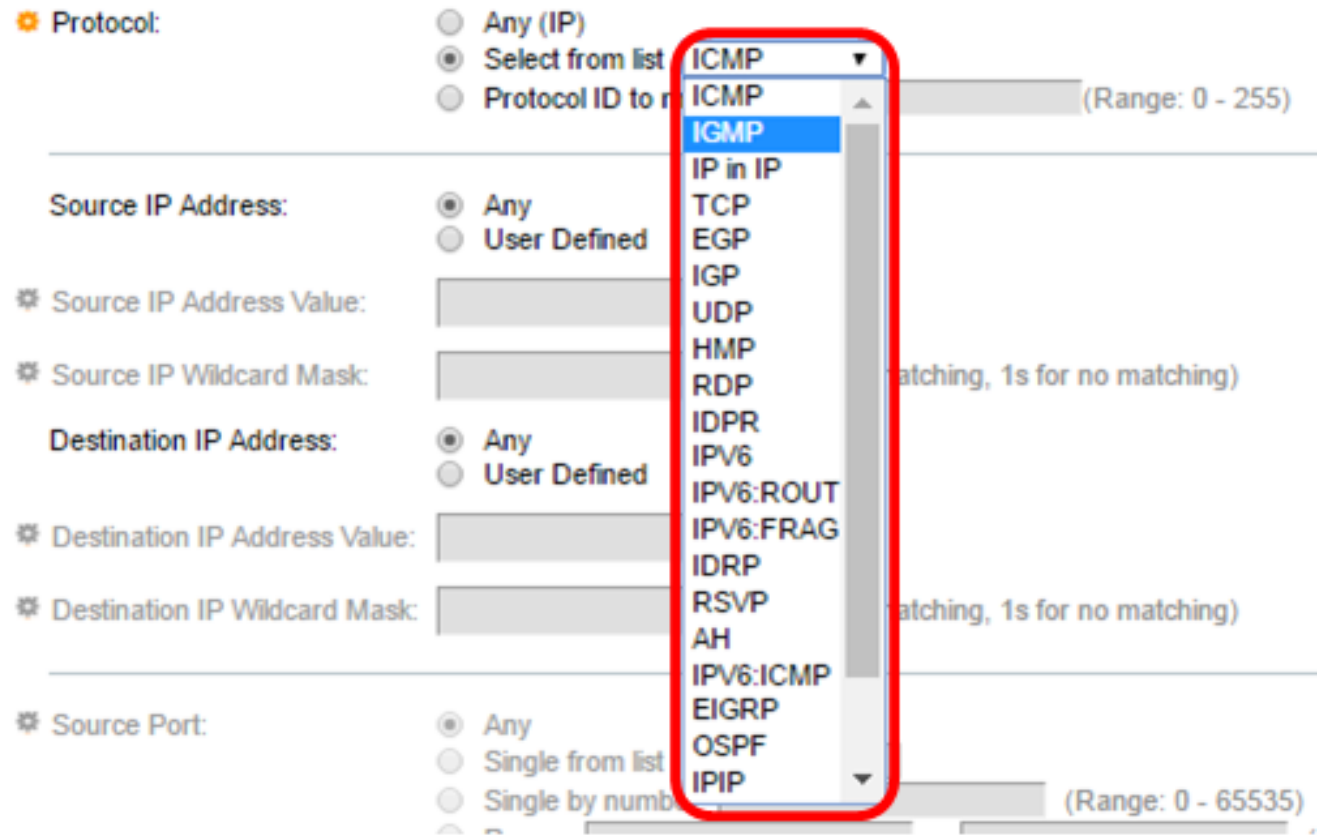


Las opciones son:

- Ningunos (IP) — Esta opción configurará ACE para validar todos los protocolos IP.
- Seleccione de la lista — Esta opción permitirá que usted elija un protocolo de una lista desplegable. Si usted prefiere esta opción, salte al paso 10.
- ID del protocolo a corresponder con — Esta opción permitirá que usted ingrese un ID del protocolo. Si usted prefiere esta opción, salte al paso 11.

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

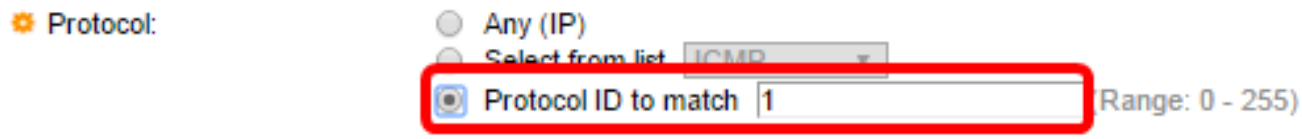
El paso 10. (opcional) si usted eligió selecciona de la lista en el paso 9, elige un protocolo de la lista desplegable.



Las opciones son:

- ICMP — Protocolo Protocolo de control de mensajes de Internet (ICMP)
- IP en IP — Encapsulación del IP en IP
- TCP — Protocolo Protocolo de control de transmisión (TCP)
- EGP — Exterior Gateway Protocol
- IGP — Protocolo Interior Gateway Protocols
- UDP — Protocolo UDP
- HMP — Protocolo de la asignación del host
- RDP — Protocolo confiable del datagrama
- IDPR — Encaminamiento de la directiva de Interdomain
- IPV6 — IPv6 sobre el Tunelización IPv4
- IPV6:ROUT — Paquetes de las coincidencias que pertenecen al IPv6 sobre la ruta IPv4 a través de un gateway
- IPV6:FRAG — Hace juego los paquetes que pertenecen al IPv6 sobre la encabezado del fragmento IPv4
- IDRP — Protocolo de la encaminamiento IS-IS Interdomain
- Protocolo de la Reservación RSVP
- AH — Encabezado de autenticación
- IPV6:ICMP — ICMP para el IPv6
- EIGRP — Protocolo de ruteo de gateway interior mejorado
- OSPF — Abra el trayecto más corto primer
- IPIP — IP en IP
- PIM — Multidifusión independiente de protocolo
- L2TP — Protocolo Layer 2 Tunneling Protocol

El paso 11 (opcional) si usted eligió el ID del protocolo para corresponder con en el paso 9, ingresa el ID del protocolo en el *ID del protocolo para corresponder con el* campo.



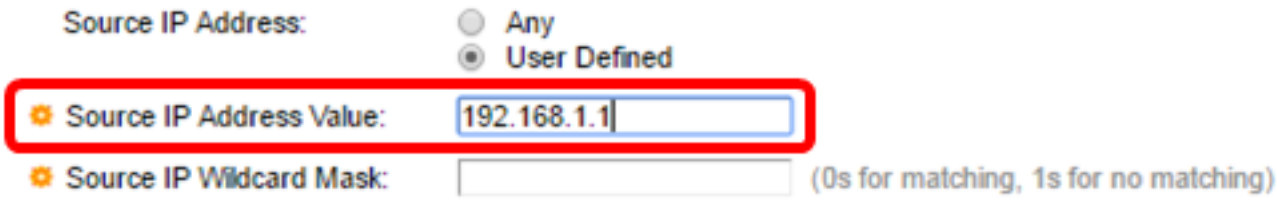
Paso 12. Haga clic el botón de radio que corresponde a los criterios deseados de ACE en el área de la dirección IP de la fuente.

Las opciones son:

- Ningunos — Todos los direccionamientos de la fuente IPv4 se aplican a ACE.
- Definido por el usario — Ingrese a una máscara comodín del IP address y IP que deba ser aplicada al AS en los campos de la *máscara comodín de la fuente del IP address IP del valor* y de la *fuente*. Utilizan a las máscaras comodín para definir un rango de los IP Addresses.

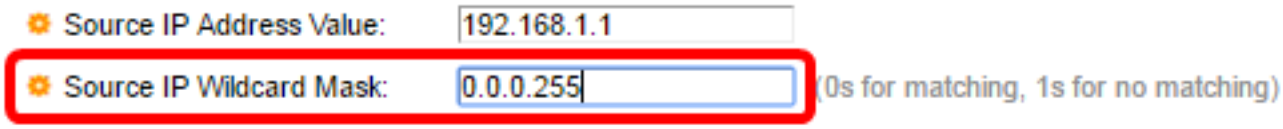
Nota: En este ejemplo, definido por el usario se elige. Si usted eligió ningunos, salte al paso 15.

Paso 13. Ingrese el IP address de la fuente en el *campo de valor del IP address de la fuente* .



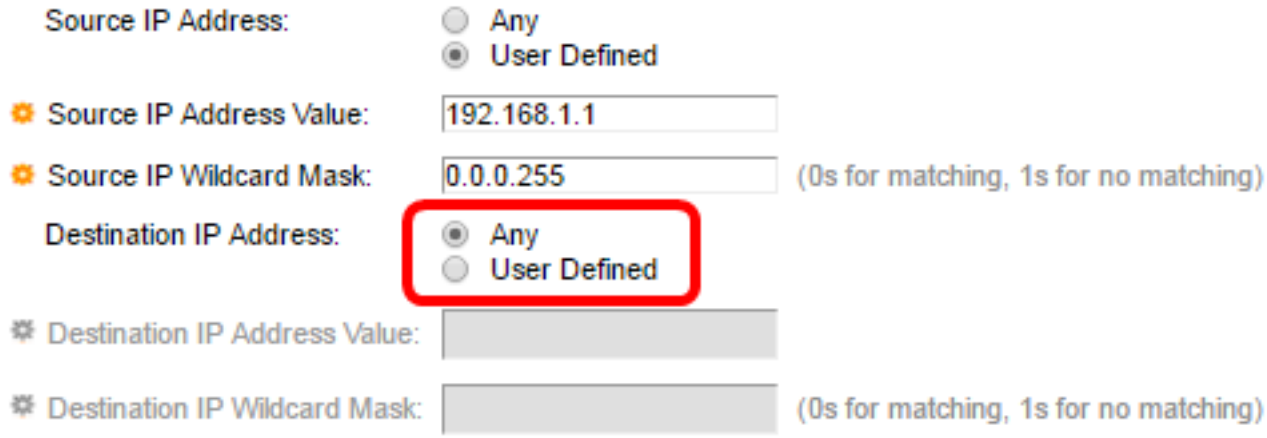
Nota: En este ejemplo, se utiliza 192.168.1.1.

Paso 14. Ingrese a la máscara comodín de la fuente en el campo de la *máscara comodín IP de la fuente*.



Nota: En este ejemplo, se utiliza 0.0.0.255.

Paso 15. Haga clic el botón de radio que corresponde a los criterios deseados de ACE en el área de la dirección IP del destino.

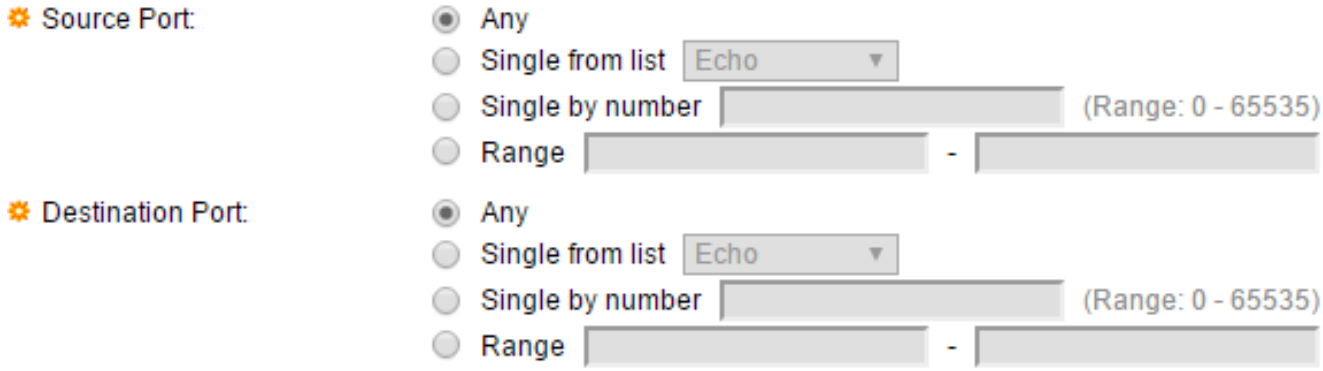


Las opciones son:

- Ningunos — Todos los direccionamientos del destino IPv4 se aplican a ACE.
- Definido por el usario — Ingrese a una máscara comodín del IP address y IP que deba ser aplicada al AS en los campos de la *máscara comodín del destino del IP address IP del valor* y del *destino*. Utilizan a las máscaras comodín para definir un rango de los IP Addresses.

Nota: En este ejemplo, se elige ninguno. Elegir esta opción significa que ACE que se creará permitirá ACE trafica venir del direccionamiento especificado IPv4 a cualquier destino.

Paso 16. (Opcional) haga clic un botón de radio en el área del puerto de origen. El valor predeterminado es ninguno.



- Ningunos — Coincidencia a todos los puertos de origen.
- Escoja de la lista — Usted puede elegir un solo puerto de origen TCP/UDP al cual se correspondan con los paquetes. Este campo es activo solamente si 800/6-TCP o 800/17-UDP se elige en la selección del menú desplegable de la lista.
- Escoja por el número — Usted puede elegir un solo puerto de origen TCP/UDP al cual se correspondan con los paquetes. Este campo es activo solamente si 800/6-TCP o 800/17-UDP se elige en la selección del menú desplegable de la lista.
- Rango — Usted puede elegir un rango de los puertos de origen TCP/UDP a los cuales se corresponde con el paquete. Hay ocho diversos rangos del puerto que pueden ser configurados (compartido entre los puertos de origen y de destino). El TCP y los protocolos UDP cada uno tienen ocho rangos del puerto.

Paso 17. (Opcional) haga clic un botón de radio en la zona portuaria de destino. El valor predeterminado es ninguno.

- Ningunos — Coincidencia a todos los puertos de origen
- Escoja de la lista — Usted puede elegir un solo puerto de origen TCP/UDP al cual se correspondan con los paquetes. Este campo es activo solamente si 800/6-TCP o 800/17-UDP se elige en la selección del menú desplegable de la lista.
- Escoja por el número — Usted puede elegir un solo puerto de origen TCP/UDP al cual se correspondan con los paquetes. Este campo es activo solamente si 800/6-TCP o 800/17-UDP se elige en la selección del menú desplegable de la lista.
- Rango — Usted puede elegir un rango de los puertos de origen TCP/UDP a los cuales se corresponde con el paquete. Hay ocho diversos rangos del puerto que pueden ser configurados (compartido entre los puertos de origen y de destino). El TCP y los protocolos UDP cada uno tienen ocho rangos del puerto.

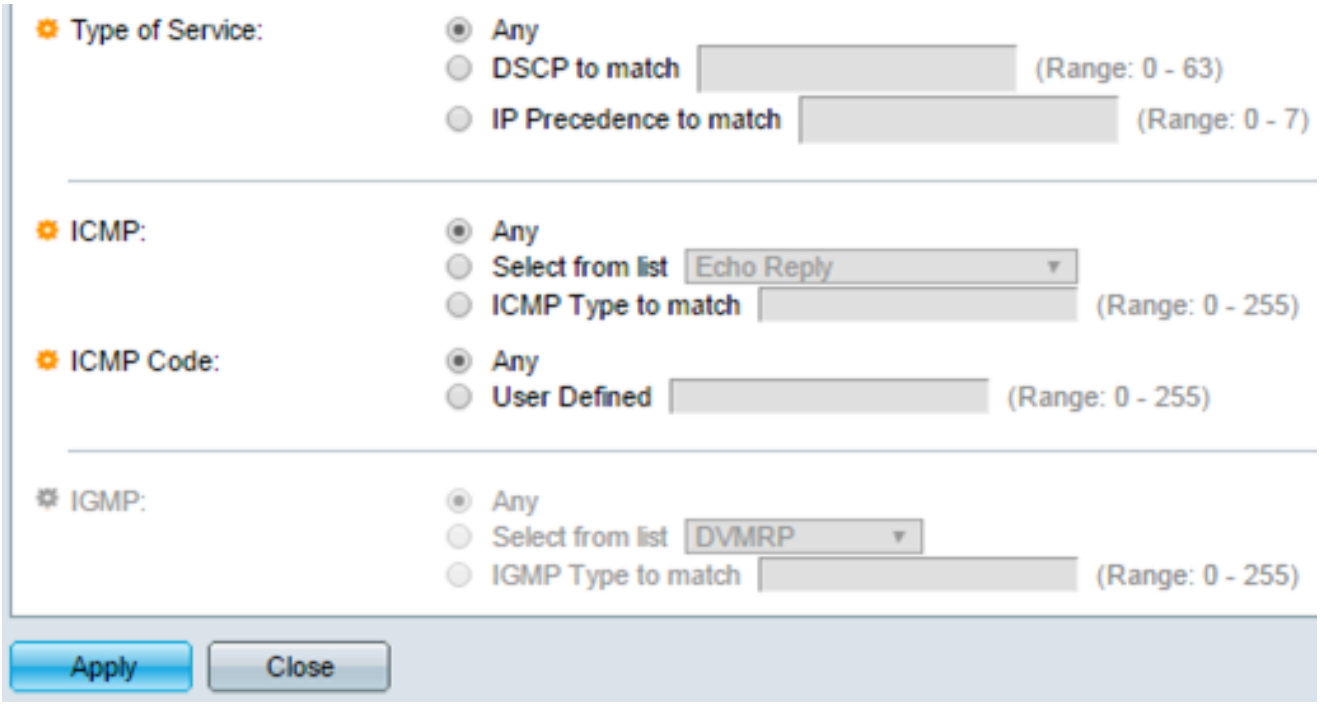
Paso 18. (Opcional) en el TCP señala el área por medio de una bandera, eligen uno o más indicadores TCP con los cuales filtrar los paquetes. Se remiten o se caen los paquetes filtrados. La filtración de los paquetes por los indicadores TCP aumenta el control del paquete, que aumenta la seguridad de la red.

- Conjunto — Haga juego si se fija el indicador.
- Unset — Haga juego si el indicador no se fija.
- No cuide — Ignore el indicador TCP.

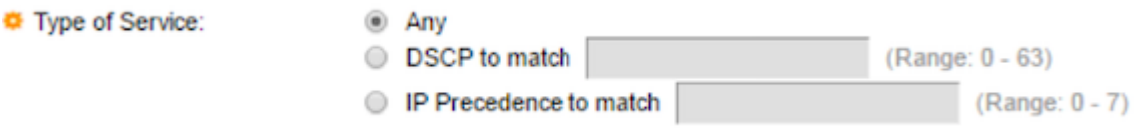
Los indicadores TCP son:

- Urg — Este indicador se utiliza para identificar los datos entrantes como urgentes.
- Ack — Este indicador se utiliza para reconocer el recibo exitoso de los paquetes.
- Psh — Este indicador se utiliza para asegurarse de que los datos están dados la prioridad (esa merecen) y procesados en el envío o el extremo receptor.
- Rst — Se utiliza este indicador cuando llega un segmento que no se piensa para la conexión actual.
- Syn — Este indicador se utiliza para las comunicaciones TCP.
- Aleta — Se utiliza este indicador cuando se acaba la comunicación o la Transferencia de datos.

Paso 19. (Opcional) haga clic el tipo de servicio del paquete IP del área de tipo de servicio.



Las opciones son:



- Ningunos — Puede ser cualquier tipo de servicio para la congestión de tráfico.
- DSCP a hacer juego — DSCP es un mecanismo para clasificar y manejo del tráfico de la red. Seis bits (0-63) se utilizan para seleccionar por el comportamiento del salto las experiencias de un paquete en cada nodo.
- Prioridad IP a hacer juego — La Prioridad IP es un modelo del Tipo de servicio (ToS) que los usos de la red de ayudar a proporcionar a las consolidaciones apropiadas del Calidad de Servicio (QoS). Este modelo utiliza tres la mayoría de los bits significativos del byte del tipo de servicio en la encabezado IP, según lo descrito en el RFC 791 y el RFC 1349. La palabra clave con el valor de preferencia IP es los siguientes:

  – 0 — para la rutina

– 1 — para la prioridad

– 2 — para inmediato

– 3 — para el flash

– 4 — para la flash-invalidación

– 5 — para crítico

– 6 — para Internet

– 7 — para la red

Paso 20. (Opcional) si protocolo IP del ACL es el ICMP, haga clic el tipo de mensaje de ICMP usado para filtrar los propósitos. Elija el Tipo de mensaje por nombre o ingrese el número del Tipo de mensaje:

- Ningunos — Validan a todos los Tipos de mensaje.
- Seleccione de la lista — Usted puede elegir el Tipo de mensaje por nombre.
- El ICMP pulsa para hacer juego — El número de Tipo de mensaje que se utilizará para filtrar purposes. Tiene un rango de 0 a 255.

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

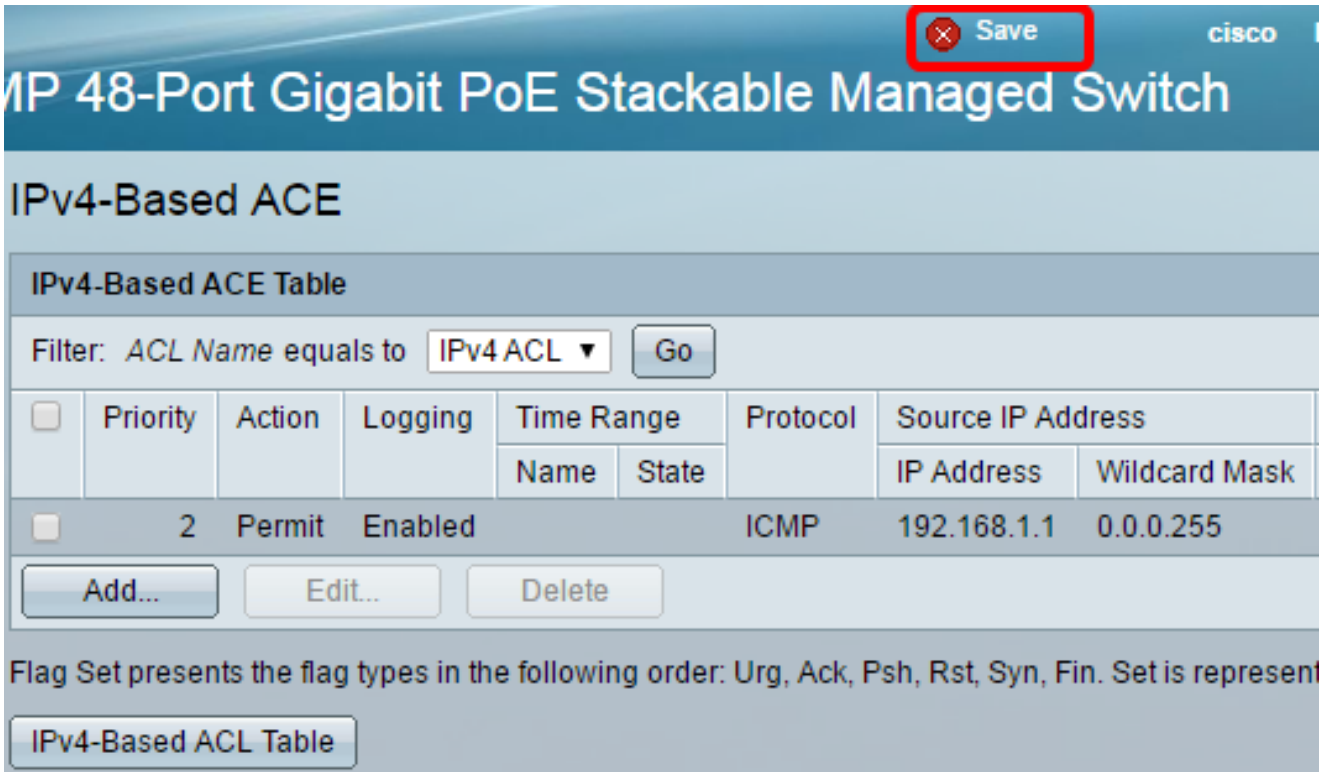
- Ningunos — Valide todos los códigos.
- Definido por el usario — Usted puede ingresar un código ICMP para los propósitos de filtración. Tiene un rango de 0 a 255.

Paso 22. (Opcional) si el ACL se basa en IGMP, haga clic el tipo de mensaje IGMP que se utilizará para filtrar los propósitos. Elija el Tipo de mensaje por nombre o ingrese el número del Tipo de mensaje:

- Ningunos — Validan a todos los Tipos de mensaje.
- Seleccione de la lista — Usted puede elegir las opciones unas de los de la lista desplegable:
- DVMRP — Utiliza una técnica de la inundación del trayecto inverso, mandando una copia de un paquete recibido a través de cada interfaz excepto el cual el paquete llegó.
- Host-interrogación — Envía periódicamente los mensajes generales de la host-interrogación en cada red conectada para la información.
- Host-contestación — Contesta a la interrogación.
- PIM — La multidifusión independiente de protocolo (PIM) se utiliza entre el Routers local y remoto del Multicast para dirigir el tráfico Multicast del servidor de multidifusión a muchos clientes del Multicast.
- Rastro — Provee información sobre unirse a y dejar los grupos de multidifusión IGMP.
- Tipo IGMP a hacer juego — El número de Tipo de mensaje que deba ser utilizado para filtrar purposes. Tiene un rango de 0 a 255.

Paso 23. El tecleo **se aplica** entonces hace clic **cerca**. ACE se crea y se asocia al nombre ACL.

Paso 24. **Salvaguardia del** tecleo para salvar las configuraciones al fichero de configuración de inicio.



Usted debe ahora haber configurado ACE basado en IPv4 en su conmutador.