IPv4-gebaseerde toegangscontrolelijst (ACL) en toegangscontrolelijst (ACE) op een switch configureren

Doel

Een toegangscontrolelijst (ACL) is een lijst van netwerkverkeersfilters en bijbehorende acties die worden gebruikt om de beveiliging te verbeteren. Het blokkeert of maakt gebruikers toegang tot specifieke bronnen. Een ACL bevat de hosts die toegang tot het netwerkapparaat is toegestaan of geweigerd.

De op IPv4 gebaseerde ACL is een lijst van bron IPv4 adressen die Layer 3 informatie gebruiken om toegang tot verkeer toe te staan of te ontkennen. IPv4 ACL's beperken IP-gerelateerd verkeer op basis van de geconfigureerde IP-filters. Een filter bevat de regels om een IP-pakket aan te passen en als de pakketovereenkomsten overeenkomen, bepaalt de regel ook of het pakket toegestaan of geweigerd moet worden.

Een Access Control Entry (ACE) bevat de eigenlijke toegangseisen. Zodra ACE wordt gecreëerd, wordt het toegepast op een ACL.

U dient toegangslijsten te gebruiken om een basisniveau van beveiliging te bieden voor de toegang tot uw netwerk. Als u geen toegangslijsten op uw netwerkapparaten vormt, kunnen alle pakketten die door de schakelaar of router worden verzonden, op alle delen van uw netwerk worden toegestaan.

Dit artikel bevat instructies hoe u op IPv4 gebaseerde ACL en ACE op uw beheerde switch kunt configureren.

Toepasselijke apparaten

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

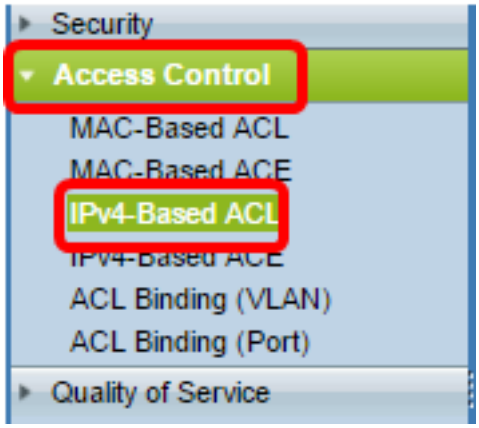
Softwareversie

- 1.4.5.02 - SX500 Series
- 2.2.5.68 - SX350 Series, SG350X Series, SX550X Series

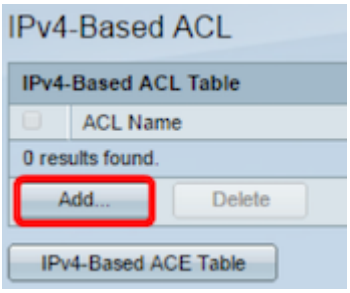
IPv4-gebaseerde ACL en ACE configureren

IPv4-gebaseerde ACL's configureren

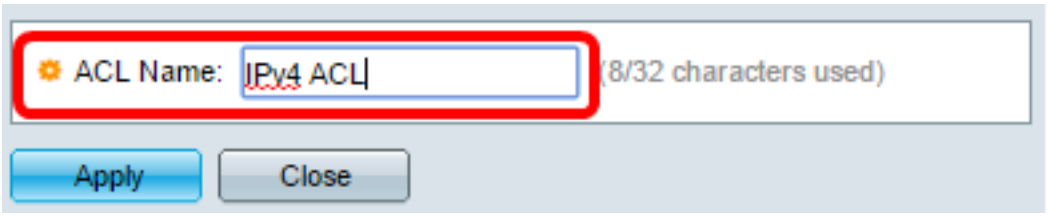
Stap 1. Meld u aan bij het webgebaseerde hulpprogramma en gaat vervolgens naar **toegangscontrole > IPv4-gebaseerde ACL**.



Stap 2. Klik op de knop **Add**.

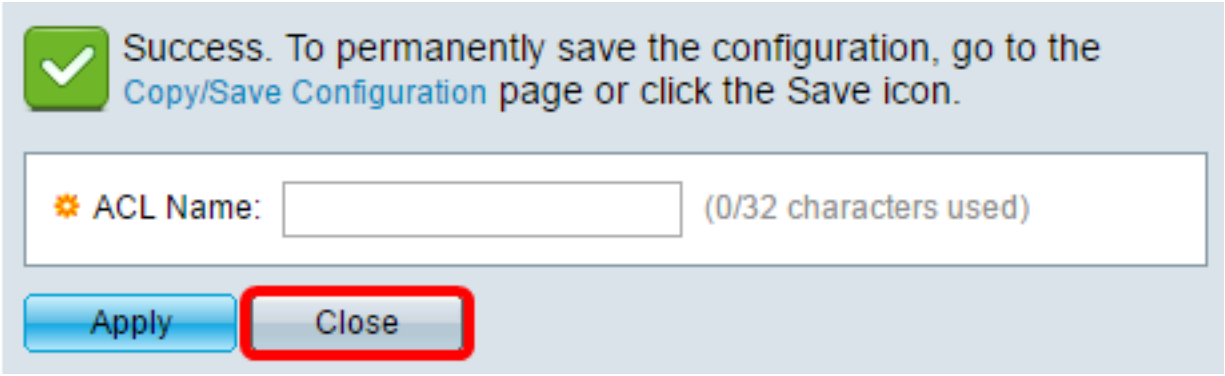


Stap 3. Voer de naam van de nieuwe ACL in het veld *ACL-naam* in.



Opmerking: In dit voorbeeld wordt IPv4 ACL gebruikt.

Stap 4. Klik op **Toepassen** en vervolgens op **Sluiten**.



Stap 5. (Optioneel) Klik op **Opslaan** om instellingen in het opstartconfiguratiebestand op te slaan.

U zou nu een op IPv4 gebaseerde ACL op uw schakelaar moeten configureren.

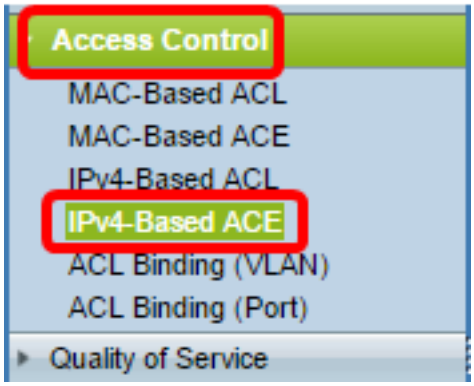
IPv4-gebaseerde ACE configureren

Wanneer een pakket op een poort wordt ontvangen, verwerkt de schakelaar het pakket door eerste ACL. Als het pakket overeenkomt met een ACE-filter van de eerste ACL, wordt de ACE-actie uitgevoerd. Als het pakket geen van de ACE filters aanpast, wordt volgende ACL verwerkt. Als er geen overeenkomst wordt gevonden met een ACE-schijf in alle relevante ACL's, komt het pakket standaard neer.

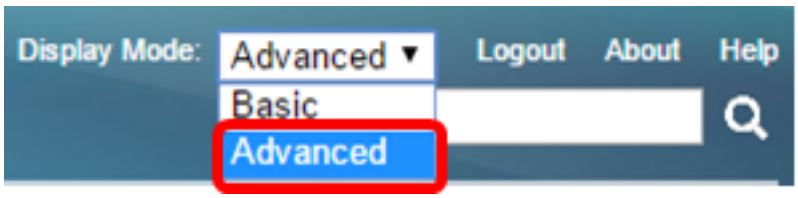
In dit scenario zal een ACE worden gecreëerd om verkeer te ontkennen dat van een specifiek door gebruiker bepaald bron IPv4 adres naar om het even welke bestemmingsadressen wordt verzonden.

Opmerking: Deze standaardactie kan worden vermeden door de creatie van een ACE met lage prioriteit die al het verkeer toestaat.

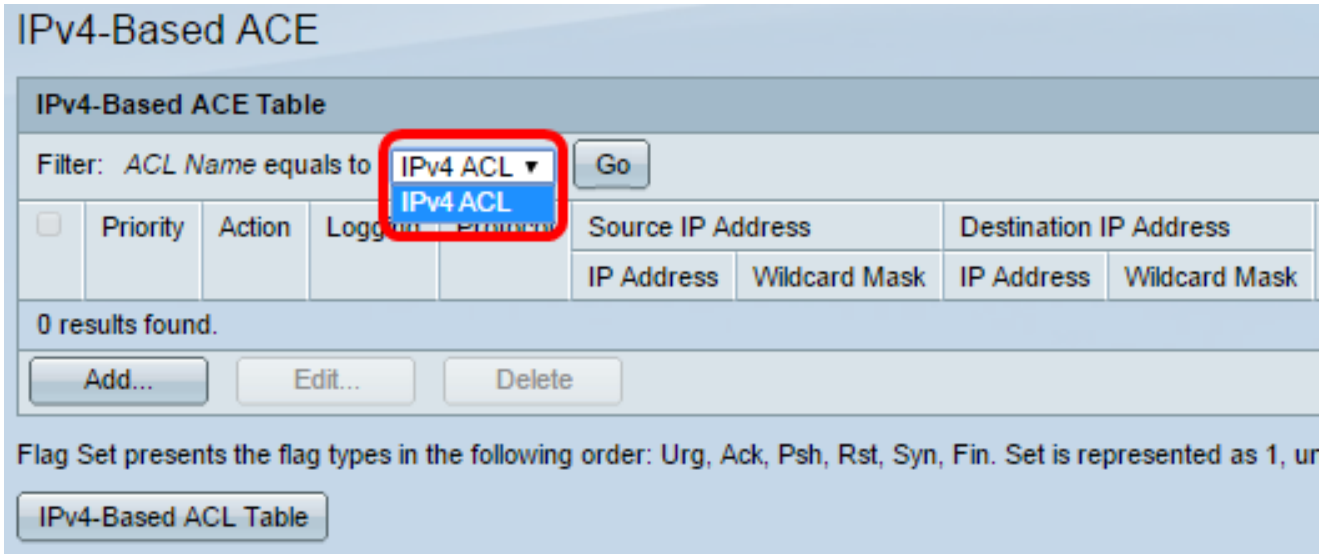
Stap 1. Ga naar **Toegangsbeheer > IPv4-gebaseerde ACE** op het web.



Belangrijk: Als u de beschikbare functies en functies van de switch volledig wilt gebruiken, verandert u deze naar de geavanceerde modus door **Geavanceerd** te kiezen in de vervolgkeuzelijst Weergave-modus in de rechterbovenhoek van de pagina.



Stap 2. Kies een ACL uit de vervolgkeuzelijst ACL-naam en klik vervolgens op **Ga**.

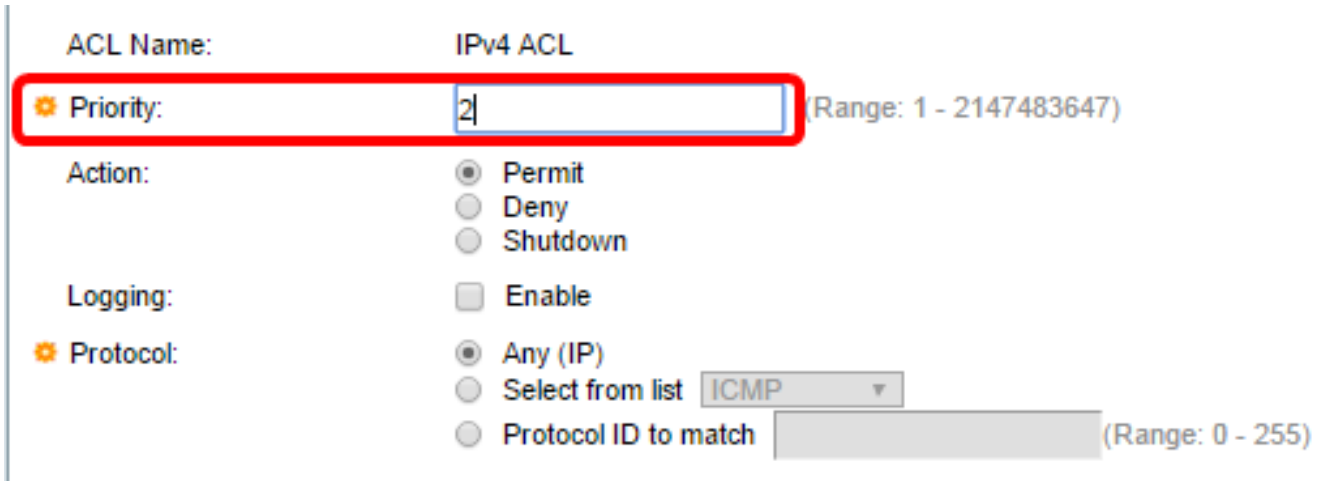


Opmerking: ACE's die al voor ACL zijn ingesteld, worden in de tabel weergegeven.

Stap 3. Klik op de knop **Add** om een nieuwe regel aan de ACL toe te voegen.

Opmerking: Het veld *ACL-naam* geeft de naam van de ACL weer.

Stap 4. Voer de prioriteitswaarde van de ACE in het veld *Prioriteit in*. ACE's met een hogere prioriteit worden eerst verwerkt. De eerste waarde is de hoogste prioriteit. Het heeft een bereik van 1 tot 2147483647.



Opmerking: In dit voorbeeld wordt 2 gebruikt.

Stap 5. Klik op de radioknop die correspondeert met de gewenste actie die wordt ondernomen wanneer een frame voldoet aan de vereiste criteria van de ACE.

Opmerking: In dit voorbeeld wordt de Vergunning gekozen.

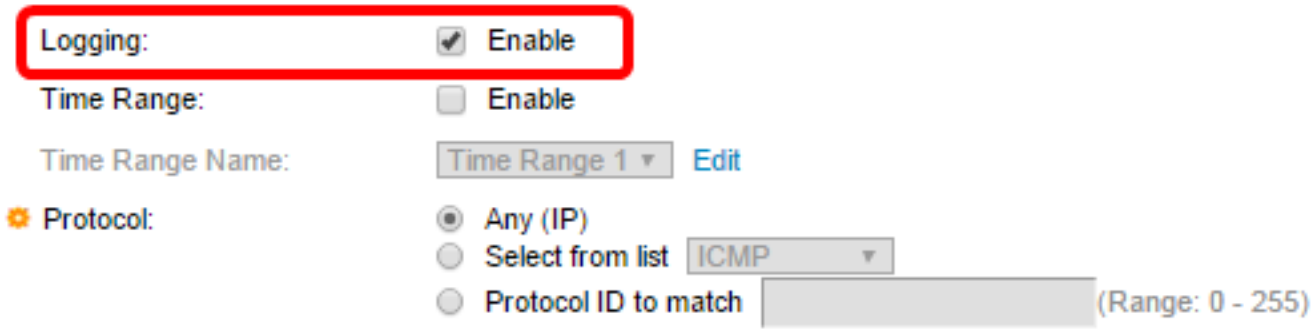
- Toestemming — De schakelaar voorwaarts pakketten die aan de vereiste criteria van

ACE voldoen.

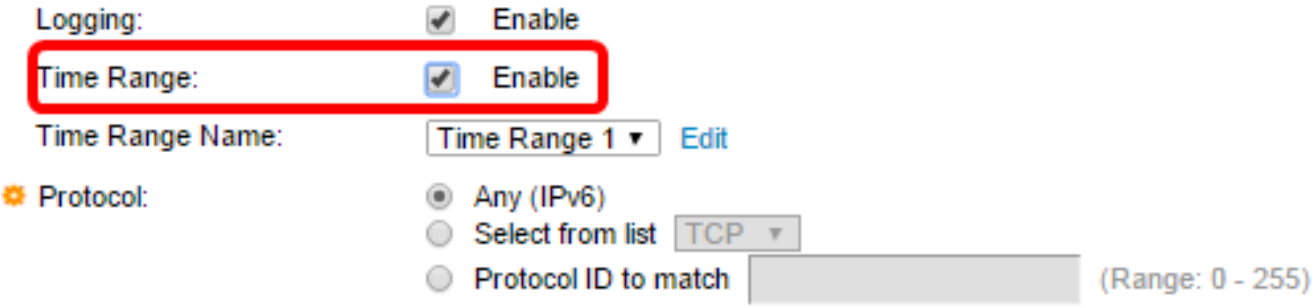
- Jeans: de schakelaar druppelt pakketten die aan de vereiste criteria van de ACE voldoen.
- Shutdown - De schakelaar druppelt pakketten die niet aan de vereiste criteria van de ACE voldoen en schakelt de haven uit waar de pakketten werden ontvangen.

Opmerking: Uitgeschakelde poorten kunnen opnieuw worden geactiveerd op de pagina Port Settings.

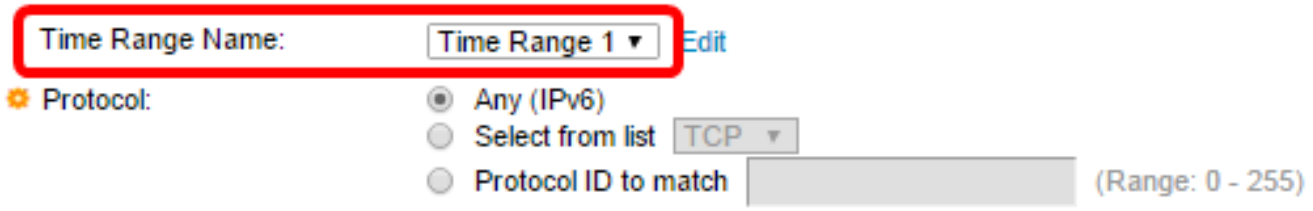
Stap 6. (Optioneel) Controleer het aanvinkvakje Aanmelden **inschakelen** om het registreren van ACL-stromen die overeenkomen met de ACL-regel mogelijk te maken.



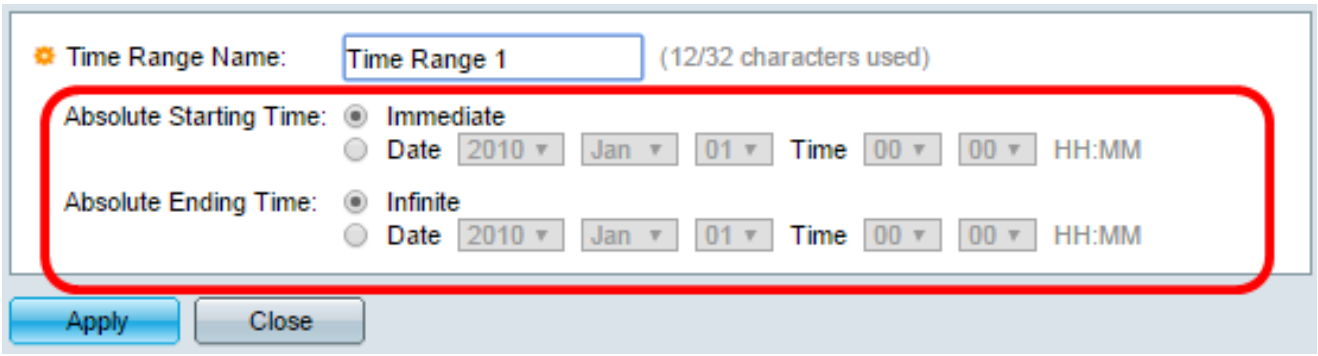
Stap 7. (Optioneel) Controleer het aankruisvakje Tijdbereik **inschakelen** om een tijdbereik in de ACE-modus te kunnen instellen. De tijdbereiken worden gebruikt om de tijd te beperken die een ACE in werking is.



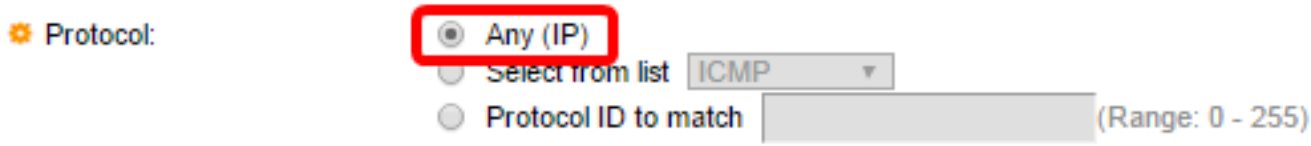
Stap 8. (Optioneel) Kies in de vervolgkeuzelijst Naam tijdbereik een tijdbereik om op de ACE toe te passen.



Opmerking: U kunt op **Bewerken** klikken om door te bladeren en een tijdbereik te maken op de pagina Tijdbereik.



Stap 9. Kies een protocoltype in het protocolgebied. De ACE wordt gemaakt op basis van een specifiek protocol of protocol-ID.

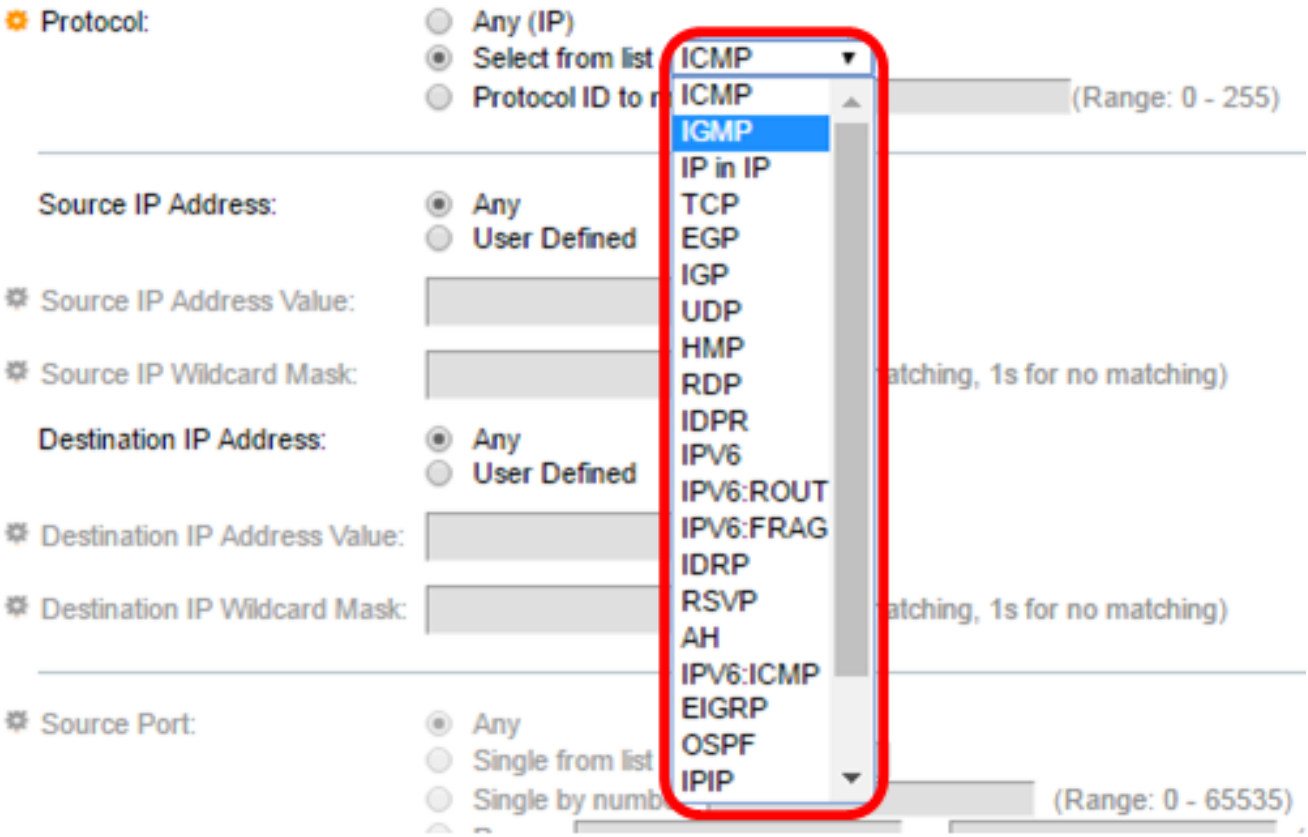


De opties zijn:

- Om het even welke (IP) — Deze optie zal de ACE configureren om alle IP protocollen te accepteren.
- Selecteer uit lijst — Met deze optie kunt u een protocol uit een vervolgkeuzelijst kiezen. Als u deze optie liever hebt, slaat u de optie over op Stap 10.
- Protocol-ID te vergelijken - Met deze optie kunt u een protocol-ID invoeren. Als u deze optie liever hebt, slaat u de optie over op Stap 11.

Opmerking: In dit voorbeeld wordt Any (IP) geselecteerd.

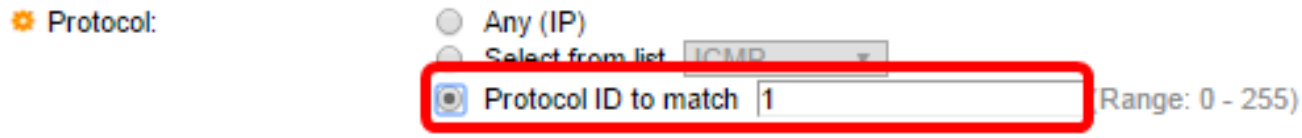
Stap 10. (Optioneel) Als u in Stap 9 Selecteren in de lijst selecteert, kiest u een protocol uit de vervolgkeuzelijst.



De opties zijn:

- ICMP — Internet Control Message Protocol
- IP in IP — IP in IP-insluiting
- TCP — Transmission Control-protocol
- EGP — Protocol voor externe gateway
- IGP — Protocol voor binnenlandse gateway
- UDP: User Datagram Protocol
- HMP — Host Mapping Protocol
- RDP: Betrouwbaar Datagram-protocol
- IDPR - routing tussen domeinen
- IPV6 — IPv6-over-IPv4-tunneling
- IPV6:ROUT — Overeenkomsten die tot de IPv6-route via een gateway behoren
- IPV6:FRAG — Overeenkomsten die behoren tot de IPv6-over-IPv4-fragmentatieheader
- IDRP — IS-IS routingprotocol voor interfaces
- RSVP — RSVP-protocol
- AH — Verificatieheader
- IPV6:ICMP — ICMP voor IPv6
- HTTP — uitgebreid routingprotocol voor binnenlandse gateway
- OSPF — Open kortstondig pad eerst
- IP — IP in IP
- PIM — Protocol onafhankelijke multicast
- L2TP-Layer 2-tunneling

Stap 11. (Optioneel) Als u Protocol-ID in stap 9 wilt koppelen, *voert* u de protocol-ID in het *veld Protocol-ID* in *die overeenkomt met het* veld *Protocol-ID*.



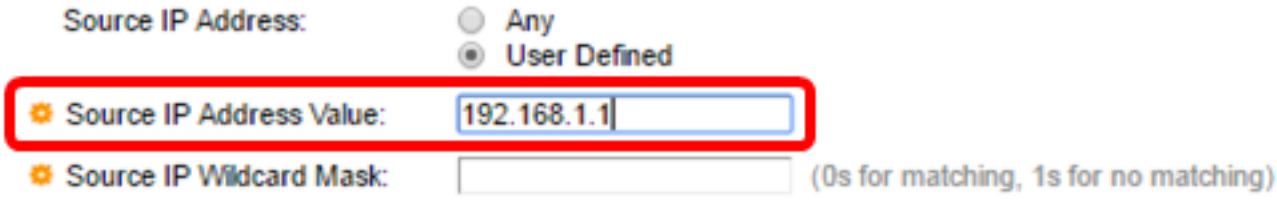
Stap 12. Klik op de radioknop die aan de gewenste criteria van ACE in het Bron IP-adresgebied voldoet.

De opties zijn:

- Alle — Alle bron IPv4 adressen zijn van toepassing op ACE.
- Gebruiker gedefinieerd - Voer een IP-adres en IP-jokermasker in dat op de ACE-waarde moet worden toegepast in de velden *Bron IP-adreswaarde* en *IP-jokermasker*. Wildcard maskers worden gebruikt om een bereik van IP adressen te definiëren.

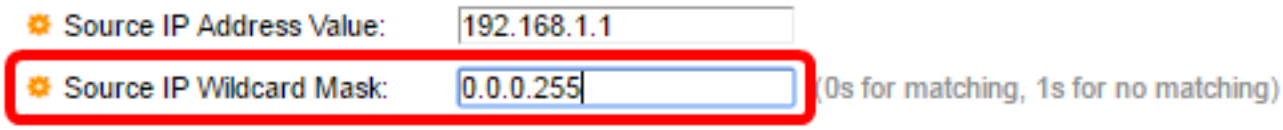
Opmerking: In dit voorbeeld wordt de gebruikersdefinitie gekozen. Als u Any selecteert, slaat u over naar Stap 15.

Stap 13. Voer het Bron-IP-adres in het veld *Source IP Address Value*.



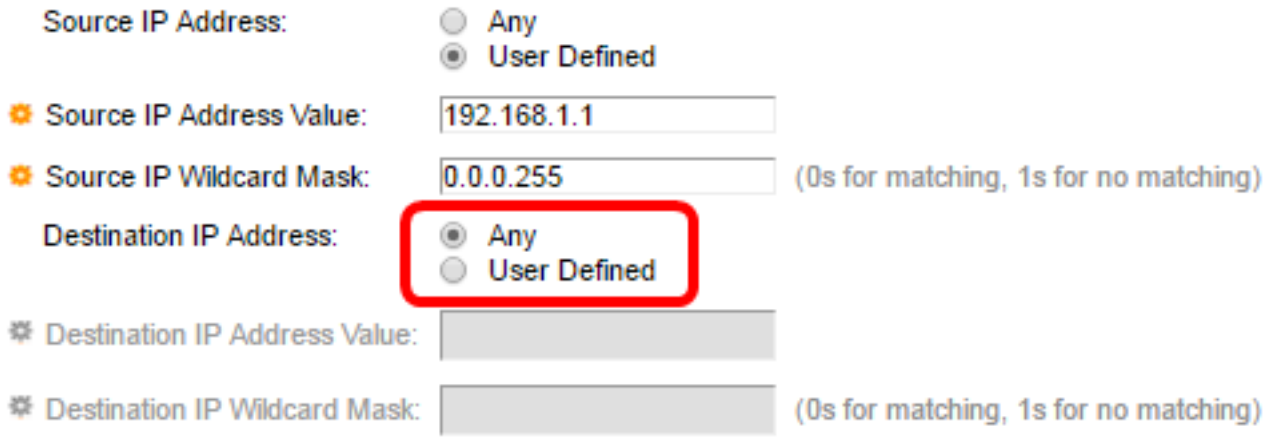
Opmerking: In dit voorbeeld wordt 192.168.1.1 gebruikt.

Stap 14. Voer het bronmasker in het veld *IP-jokermasker* in.



Opmerking: In dit voorbeeld wordt 0.0.0.255 gebruikt.

Stap 15. Klik op de radioknop die aan de gewenste criteria van ACE in het IP-adresgebied van de bestemming beantwoordt.

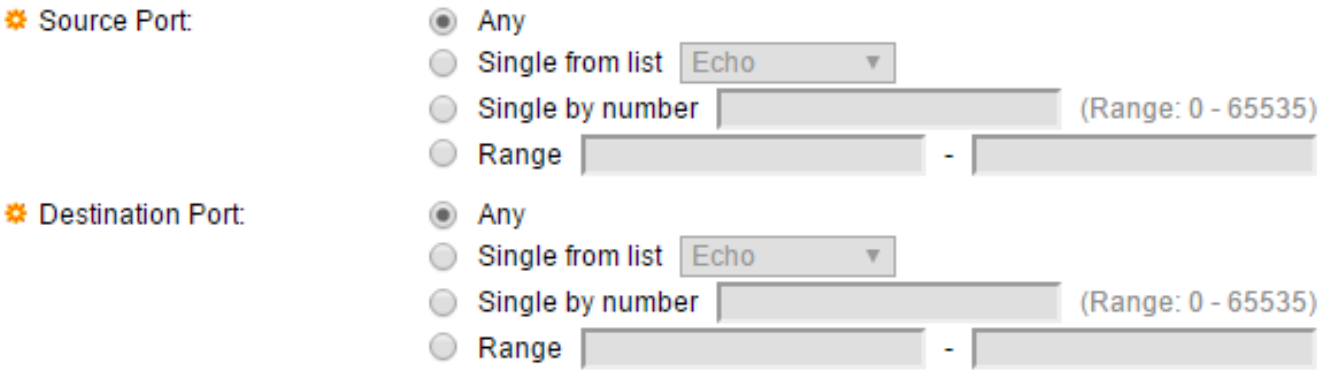


De opties zijn:

- Alle — Alle IPv4-adressen van het bestemming zijn van toepassing op de ACE.
- Gebruiker gedefinieerd - Voer een IP-adres en een IP-jokermasker in dat op de ACE-toets moet worden toegepast in de velden *IP-adreswaarde* en *IP-jokermasker* op *bestemming*. Wildcard maskers worden gebruikt om een bereik van IP adressen te definiëren.

Opmerking: In dit voorbeeld wordt AnyRes gekozen. Voor deze optie betekent de ACE-optie dat het ACE-verkeer dat van het gespecificeerde IPv4-adres naar elke bestemming komt, mogelijk is.

Stap 16. (Optioneel) Klik op een radioknop in het bronpoortgebied. De standaardwaarde is Any.



- Alle — Overeenkomend met alle bronpoorten.
- Single from list - U kunt één TCP/UDP-bronpoort kiezen waar pakketten worden aangepast. Dit veld is alleen actief als 800/6-TCP of 800/17-UDP is geselecteerd in het vervolgkeuzemenu Lijst met selecteren.
- Single by number - U kunt één TCP/UDP-bronpoort kiezen waar pakketten worden aangepast. Dit veld is alleen actief als 800/6-TCP of 800/17-UDP is geselecteerd in het vervolgkeuzemenu Lijst met selecteren.
- Bereik — U kunt een bereik van TCP/UDP-bronpoorten kiezen waaraan het pakket is aangepast. Er zijn acht verschillende poortbereiken die kunnen worden geconfigureerd (gedeeld tussen bron- en doelpoorten). TCP- en UDP-protocollen hebben elk acht poortbereik.

Stap 17. (Optioneel) Klik op een radioknop in het gebied met de bestemming. De standaardwaarde is Any.

- Alle — Overeenkomend met alle bronpoorten
- Single from list - U kunt één TCP/UDP-bronpoort kiezen waar pakketten worden aangepast. Dit veld is alleen actief als 800/6-TCP of 800/17-UDP is geselecteerd in het vervolgkeuzemenu Lijst met selecteren.
- Single by number - U kunt één TCP/UDP-bronpoort kiezen waar pakketten worden aangepast. Dit veld is alleen actief als 800/6-TCP of 800/17-UDP is geselecteerd in het vervolgkeuzemenu Lijst met selecteren.
- Bereik — U kunt een bereik van TCP/UDP-bronpoorten kiezen waaraan het pakket is aangepast. Er zijn acht verschillende poortbereiken die kunnen worden geconfigureerd (gedeeld tussen bron- en doelpoorten). TCP- en UDP-protocollen hebben elk acht poortbereik.

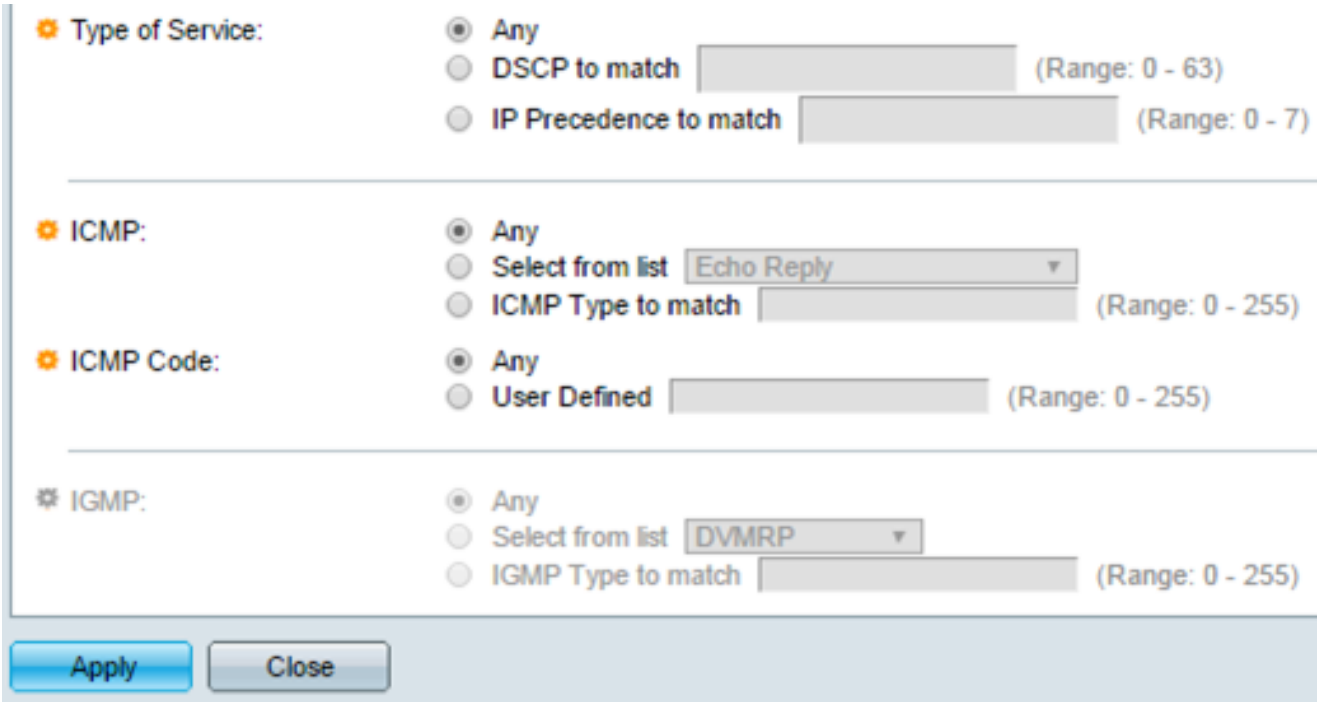
Stap 18. (Optioneel) Kies in het gebied TCP-Vlaggen een of meer TCP-vlaggen waarmee u pakketten kunt filteren. De gefilterde pakketten worden verzonden of laten vallen. Het filteren van pakketten door TCP vlaggen verhoogt pakketcontrole, wat netwerkveiligheid verhoogt.

- Instellen — Overeenkomsten als de vlag is ingesteld.
- Oningesteld - Overeenkomsten als de vlag niet is ingesteld.
- Maakt niet uit — Negeer de TCP vlag.

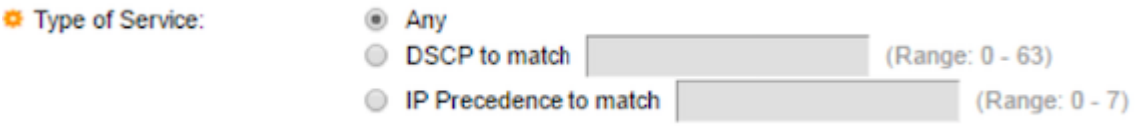
De TCP-vlaggen zijn:

- Urg — Deze vlag wordt gebruikt om binnenkomende gegevens als urgent te identificeren.
- Ack - Deze vlag wordt gebruikt om de ontvangst van pakketten met succes te bevestigen.
- Psh — Deze vlag wordt gebruikt om ervoor te zorgen dat de gegevens de prioriteit krijgen (die het verdient) en worden verwerkt op het verzendende of ontvangende eind.
- Rst — Deze vlag wordt gebruikt wanneer een segment arriveert dat niet is bedoeld voor de huidige verbinding.
- Syn — Deze vlag wordt gebruikt voor TCP-communicatie.
- Fin — Deze vlag wordt gebruikt wanneer de communicatie of gegevensoverdracht is voltooid.

Stap 19. (Optioneel) Klik op het servicetype van het IP-pakket vanuit het gedeelte Type of Service.



De opties zijn:



- Alle — Het kan elk type service zijn voor verkeersopstoppingen.
- DSCP to matching - DSCP is een mechanisme voor het classificeren en beheren van netwerkverkeer. Zes bits (0-63) wordt gebruikt om bij elk knooppunt een pakketervaring te selecteren voor het Per Hop-gedrag.
- IP-voorrang om aan elkaar te koppelen — IP-voorrang is een model van Service (TOS) die het netwerk gebruikt om de juiste QoS-verbintenissen (Quality of Service) te bieden. Dit model gebruikt de drie meest significante bits van het servicetype byte in de IP-header, zoals beschreven in RFC 791 en RFC 1349. Het sleutelwoord met IP-referentiewaarde is:

  - 0 — voor routine

  - 1 — prioriteit

  - 2 — onmiddellijk

  - 3 — flitser

  - 4 — voor flash-Override

  - 5 — voor kritische

  - 6 — voor internet

  - 7 — voor het netwerk

Stap 20. (Optioneel) Als het IP-protocol van de ACL ICMP is, klikt u op het ICMP-berichttype dat wordt gebruikt voor filterdoeleinden. Kies het berichttype op naam of voer het bericht

type nummer in:

- Alle berichttypes worden geaccepteerd.
- Selecteer uit lijst — U kunt het berichttype op naam kiezen.
- ICMP-type dat moet worden aangepast — het aantal berichten dat moet worden gebruikt voor filterdoeleinden. Het heeft een bereik van 0 tot 255.

Stap 21. (Optioneel) De ICMP-berichten kunnen een codeveld hebben dat aangeeft hoe de boodschap moet worden verwerkt. Klik op een van de volgende opties om te vormen of u in deze code wilt filteren:

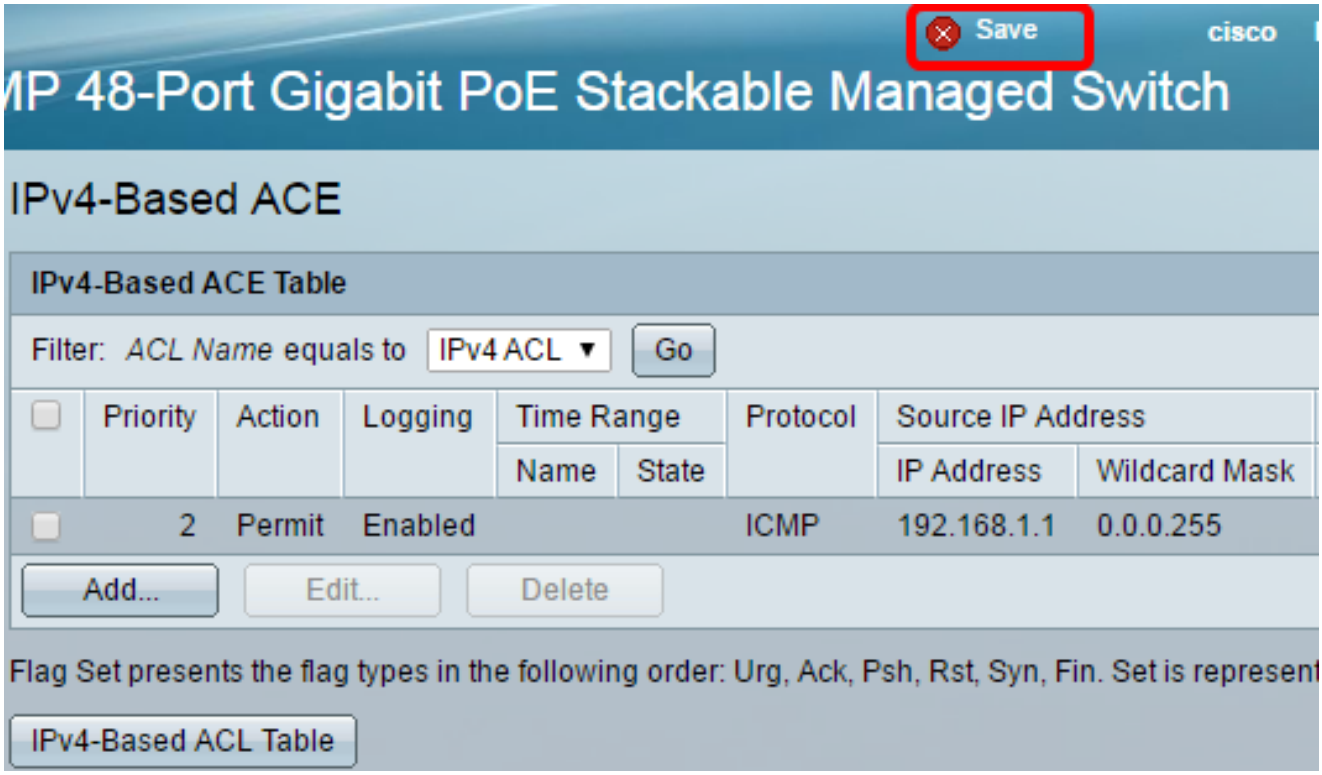
- Alle — Alle codes accepteren.
- Gebruikershandleiding — U kunt een ICMP-code invoeren voor filterdoeleinden. Het heeft een bereik van 0 tot 255.

Stap 2. (Optioneel) Als de ACL op IGMP is gebaseerd, klik dan op het IGMP-berichttype dat voor filterdoeleinden gebruikt moet worden. Kies het berichttype op naam of voer het bericht type nummer in:

- Alle berichttypes worden geaccepteerd.
- Selecteer uit lijst — U kunt een van de opties uit de vervolgkeuzelijst kiezen:
- DVMRP — Gebruikt een omgekeerde pad overstromingen techniek, waarbij een kopie van een ontvangen pakket door elke interface wordt verzonden behalve het pakket waar het pakket is aangekomen.
- Host-Query — Zorgt periodiek voor algemene host-query-berichten op elk aangesloten netwerk ter informatie.
- Host-Reactie — Het beantwoordt de vraag.
- PIM — Protocol Independent Multicast (PIM) wordt gebruikt tussen de lokale en externe multicast routers om multicast verkeer van de multicast server naar veel multicast klanten te sturen.
- Trace — Bevat informatie over het toetreden en het verlaten van de IGMP multicast groepen.
- IGMP-type dat moet worden aangepast — het aantal berichttypen dat moet worden gebruikt voor filterdoeleinden. Het heeft een bereik van 0 tot 255.

Stap 23. Klik op **Toepassen** dan op **Sluiten**. ACE wordt gecreëerd en geassocieerd met de ACL naam.

Stap 24. Klik op **Opslaan** om instellingen op te slaan in het opstartconfiguratiebestand.



U zou nu een op IPv4 gebaseerde ACE op uw schakelaar moeten hebben ingesteld.