IPv6-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 typische ACL-functie in IPv6 is vergelijkbaar met ACL's in IPv4. ACL's bepalen welk verkeer moet worden geblokkeerd en welk verkeer naar voren moet worden gebracht bij switch interfaces. ACL's staan filtering toe op basis van bron- en doeladressen, inkomende en uitgaande naar specifieke interfaces. Elke ACL heeft een impliciete ontkenningsverklaring aan het eind. De regels voor ACL's worden ingesteld in Access Control Entries (ACE's).

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 IPv6 gebaseerde ACL en ACE op een switch kunt configureren.

Toepasselijke apparaten

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

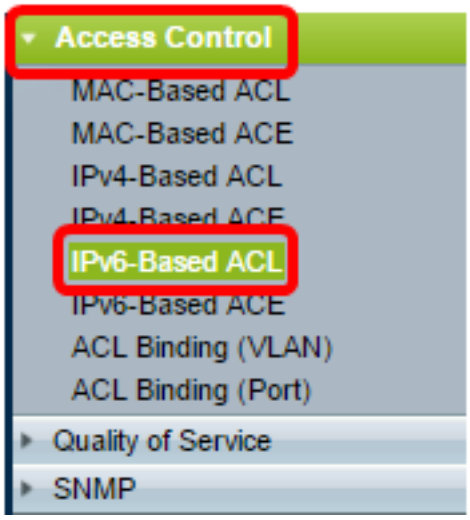
Softwareversie

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

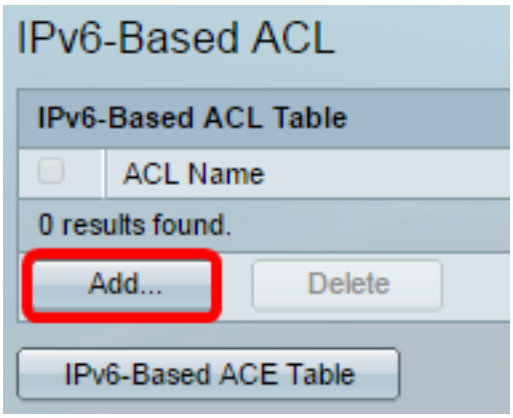
IPv6-gebaseerde ACL en ACE configureren

IPv6-gebaseerde ACL's configureren

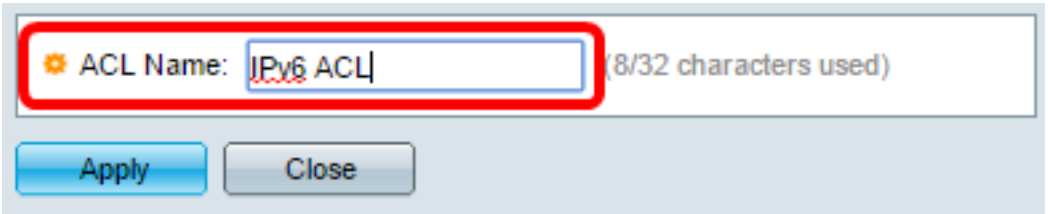
Stap 1. Meld u aan bij het op internet gebaseerde hulpprogramma. Ga vervolgens naar **toegangscontrole > IPv6 gebaseerde ACL**.



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

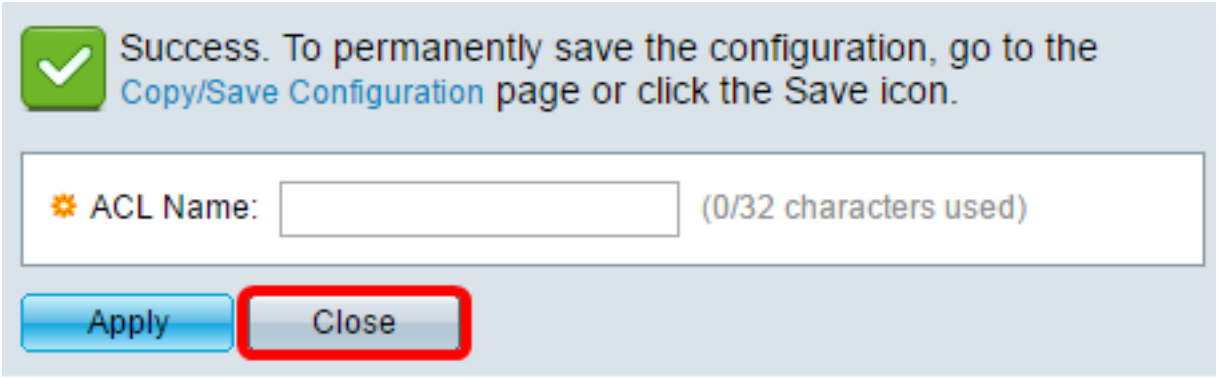


Stap 3. Voer de naam van de nieuwe ACL in het veld *ACL-naam* in.



Opmerking: In dit voorbeeld wordt IPv6 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 IPv6 gebaseerde ACL op uw schakelaar moeten configureren.

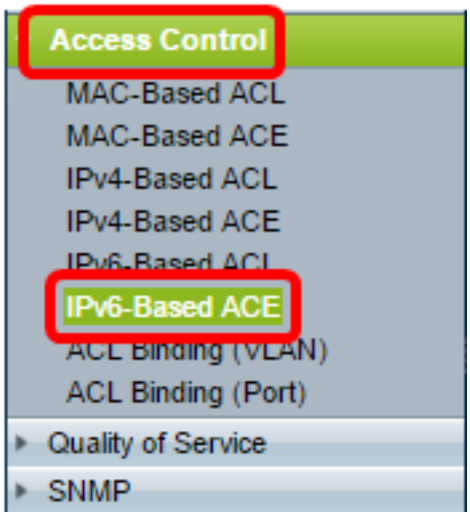
IPv6-gebaseerde ACE configureren

Wanneer een pakket op een poort wordt ontvangen, verwerkt de schakelaar het kader 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.

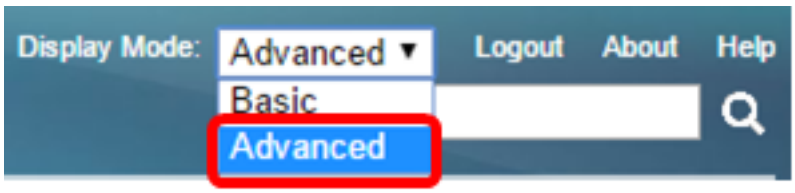
In dit scenario zal een ACE worden gecreëerd om verkeer te ontkennen dat van een specifiek door gebruiker bepaald bron IPv6 adres naar om het even welke bestemmingsadressen wordt verzonden.

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

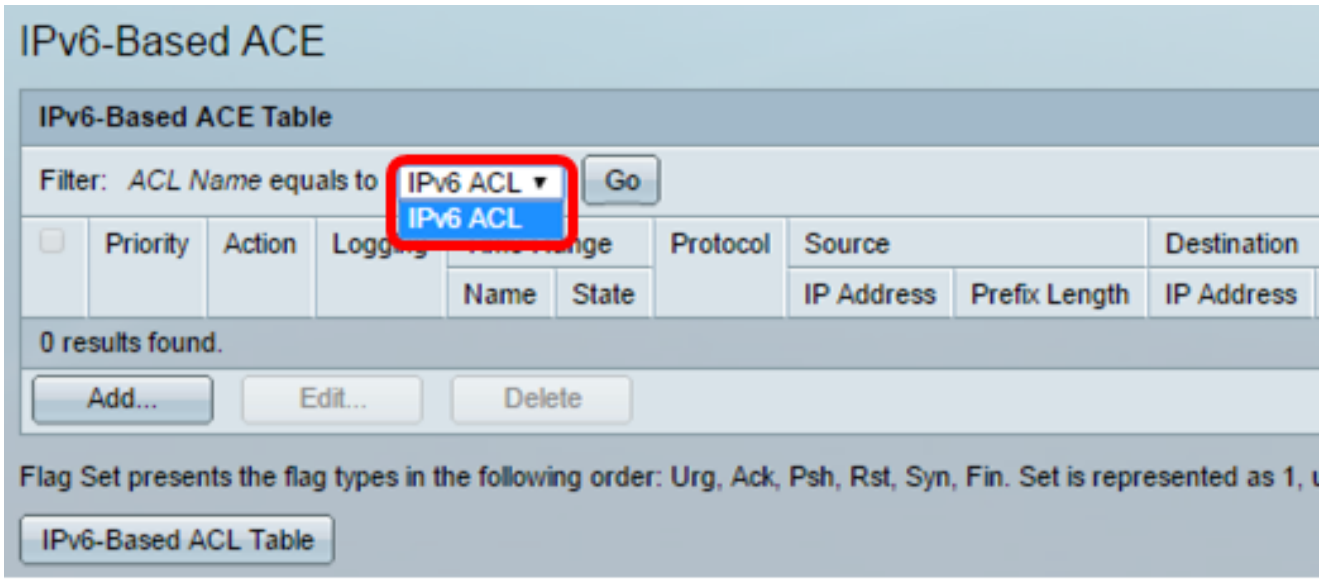
Stap 1. Ga naar **Toegangsbeheer > IPv6-gebaseerde ACE** op het web.



Belangrijk: Als u een SX350-, SG350X-, Sx550X-switch hebt, verandert u in de geavanceerde modus door **Advanced** te kiezen in de vervolgkeuzelijst Display Mode in de rechterbovenhoek van de pagina.

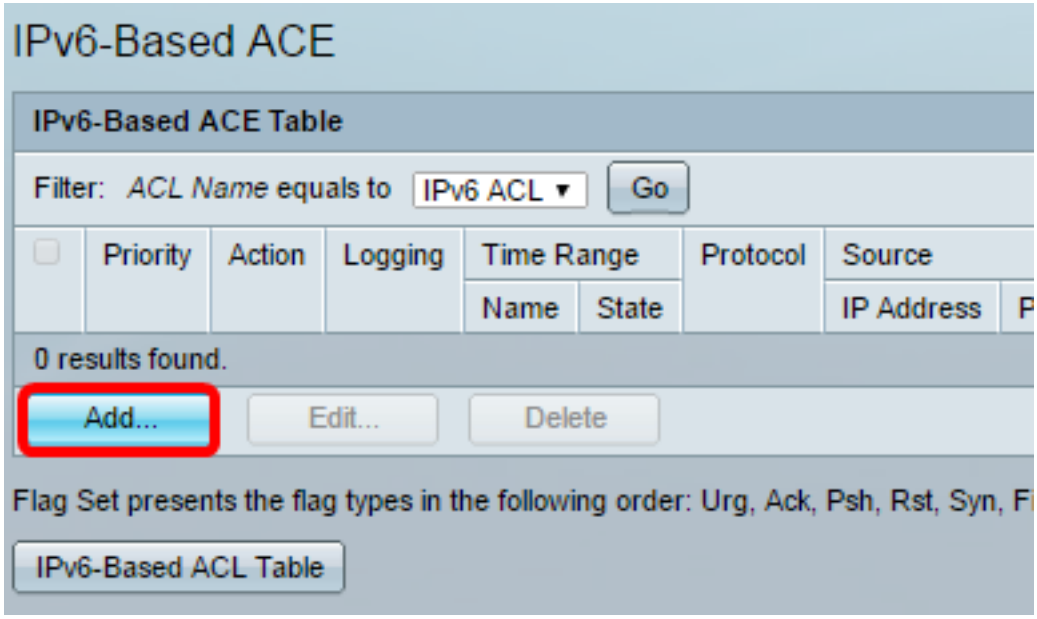


Stap 2. Kies een ACL uit de vervolgkeuzelijst ACL-naam en klik vervolgens op **Ga**.



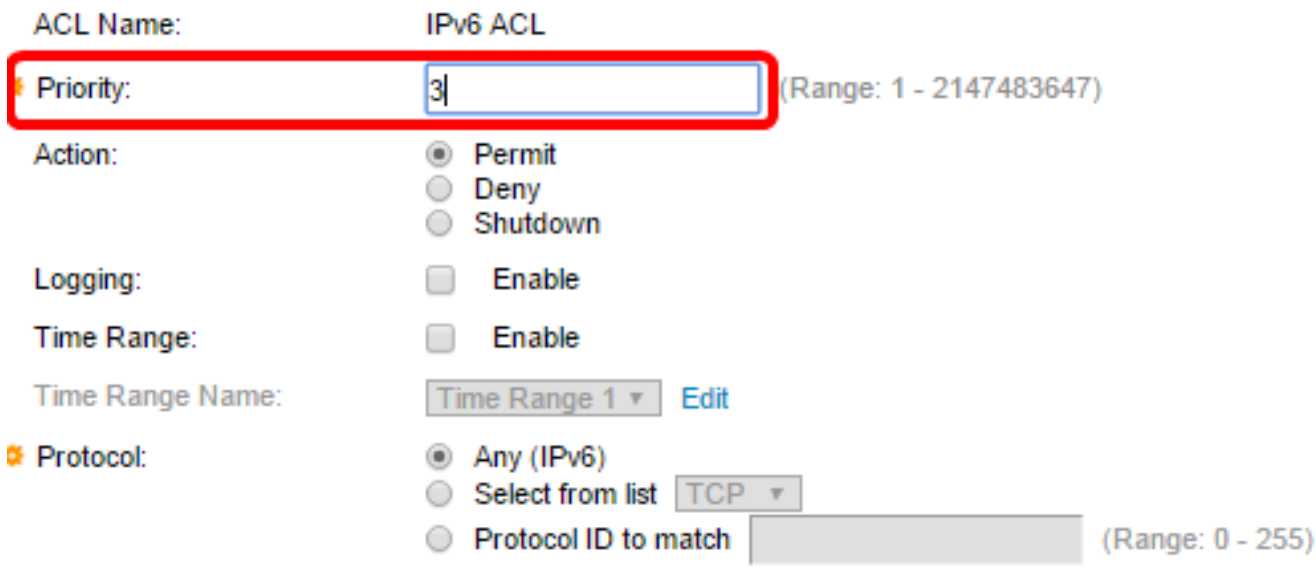
Opmerking: ACE's die al voor ACL zijn ingesteld, worden in de tabel weergegeven.

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 3 gebruikt.

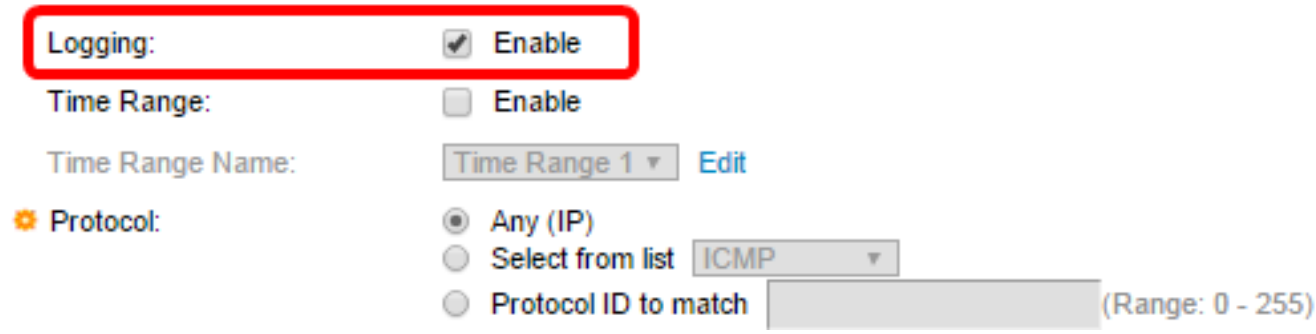
Stap 5. Klik op de radioknop die correspondeert met de gewenste actie die wordt ondernomen wanneer een frame voldoet aan de vereiste criteria van de ACE.

Opmerking: In dit voorbeeld wordt de Vergunning gekozen.

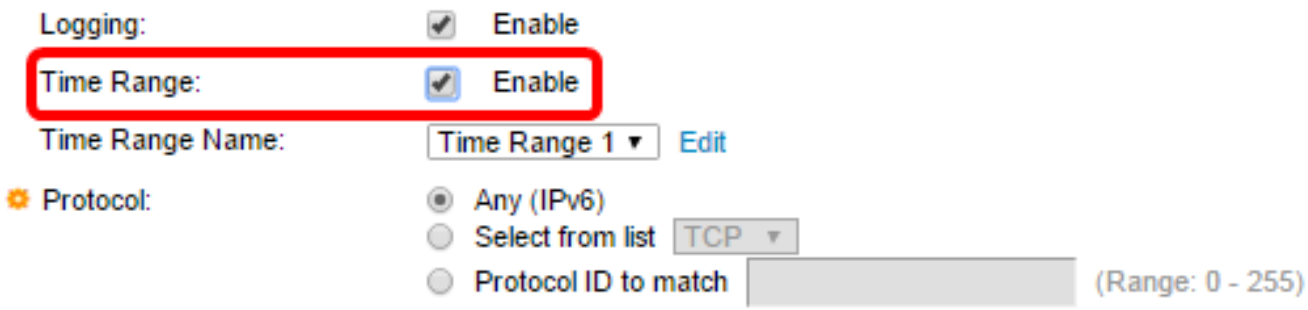
- Toestemming — De schakelaar voorwaarts pakketten die aan de vereiste criteria van ACE voldoen.
- Jeans: de schakelaar druppelt pakketten die aan de vereiste criteria van de ACE voldoen.

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

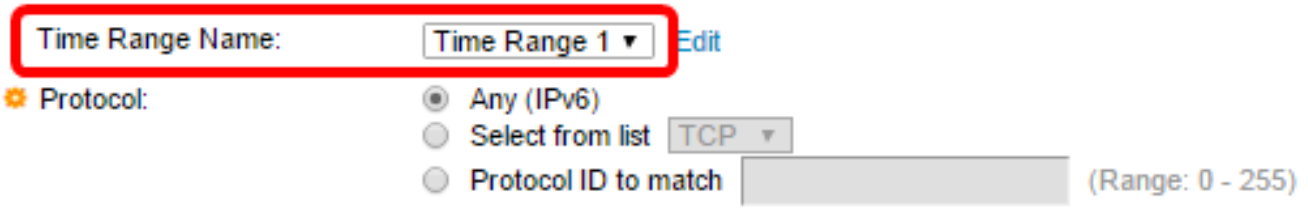
Stap 6. (Optioneel) Controleer het selectieteken voor vastlegging **inschakelen** om logstromen mogelijk te maken die overeenkomen met de ACL-regel.



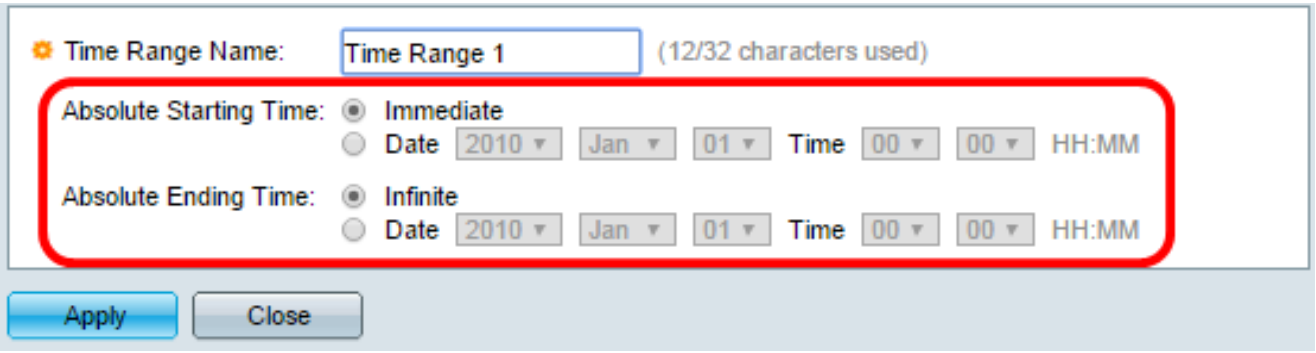
Stap 7. (Optioneel) Controleer het aankruisvakje Tijdbereik **inschakelen** om een tijdbereik in de ACE-modus te kunnen instellen. De tijdbereiken worden gebruikt om de tijd te beperken die een ACE in werking is. Als dit wordt uitgeschakeld, werkt de ACE op elk moment.



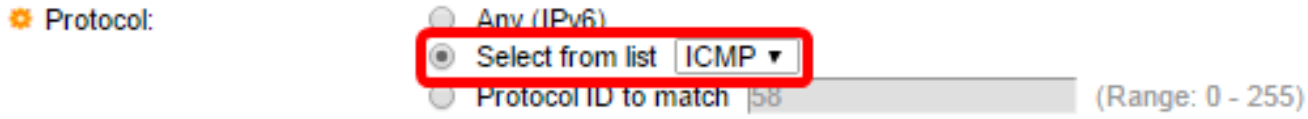
Stap 8. (Optioneel) Kies in de vervolgkeuzelijst Naam tijdbereik een tijdbereik om op de ACE toe te passen.



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.

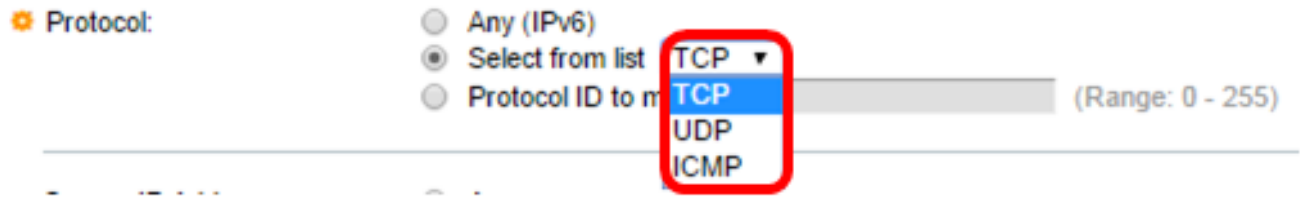


De opties zijn:

- 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 Select Van list geselecteerd.

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

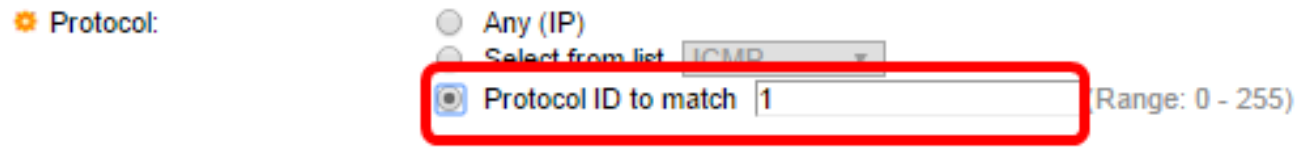


De opties zijn:

- TCP — Transmission Control Protocol (TCP) stelt twee hosts in staat te communiceren en gegevensstromen uit te wisselen. TCP garandeert pakketlevering en garandeert dat pakketten worden verzonden en ontvangen in de volgorde waarin ze werden verzonden.
- UDP — User Datagram Protocol (UDP) zendt pakketten toe, maar garandeert de levering ervan niet.
- ICMP — Overeenkomsten met het Internet Control Message Protocol (ICMP).

Opmerking: In dit voorbeeld wordt TCP gebruikt.

Stap 1. (Optioneel) Als u Protocol-ID in stap 9 wilt koppelen, voert u de protocol-ID in het veld *Protocol-ID in*.



Opmerking: In dit voorbeeld wordt 1 gebruikt.

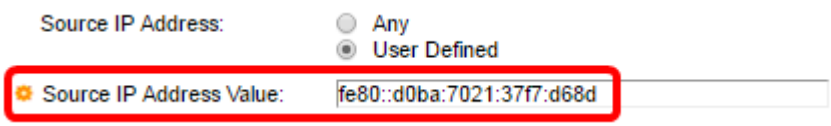
Stap 12. Klik op de radioknop die aan de gewenste criteria van ACE in het Bron IP-adresgebied voldoet.

De opties zijn:

- Alle — Alle bron IPv6-adressen zijn van toepassing op ACE.
- Gebruiker gedefinieerd - Voer een IP-adres en IP-wildkaartmasker in dat op de ACE-toets moet worden toegepast in de velden *Source IP Address Value* and *Source IP Prefix Length*.

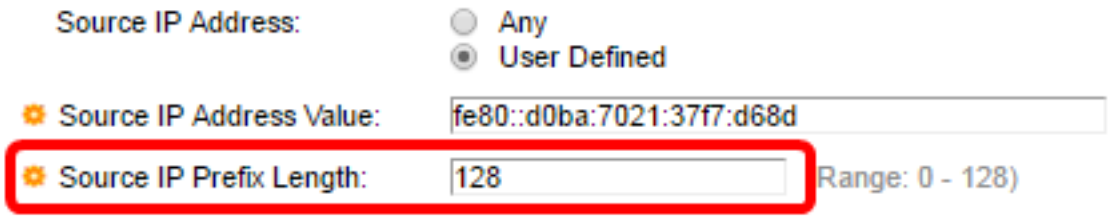
Opmerking: In dit voorbeeld wordt de gebruikersdefinitie gekozen. Als u Any selecteert, slaat u over naar Stap 15.

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



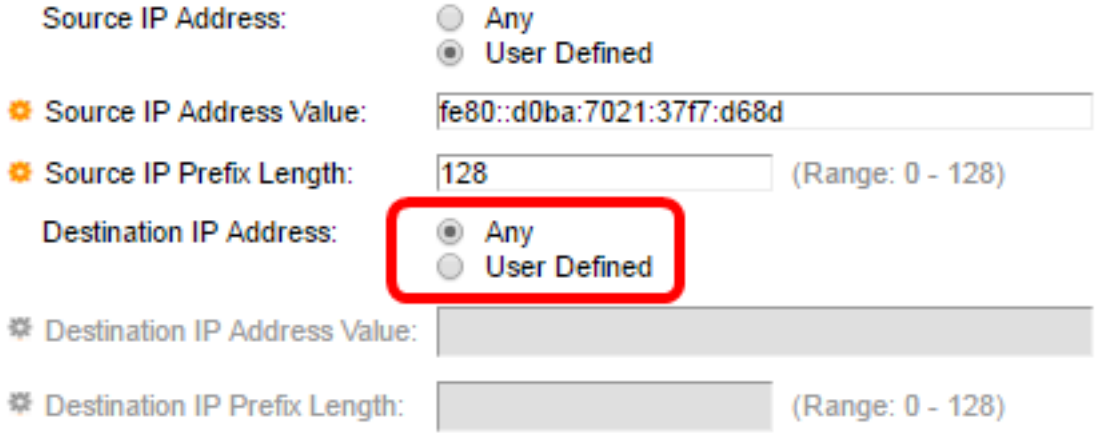
Opmerking: In dit voorbeeld wordt fe80::d0ba:7021:37f7:d68d gebruikt.

Stap 14. Voer de lengte van het bronIP-prefix in het veld *Bron IP-prefixlengte in*.



Opmerking: In dit voorbeeld wordt 128 gebruikt.

Stap 15. Klik op de radioknop die aan de gewenste criteria van ACE in het gedeelte DestinationIP Address beantwoordt.

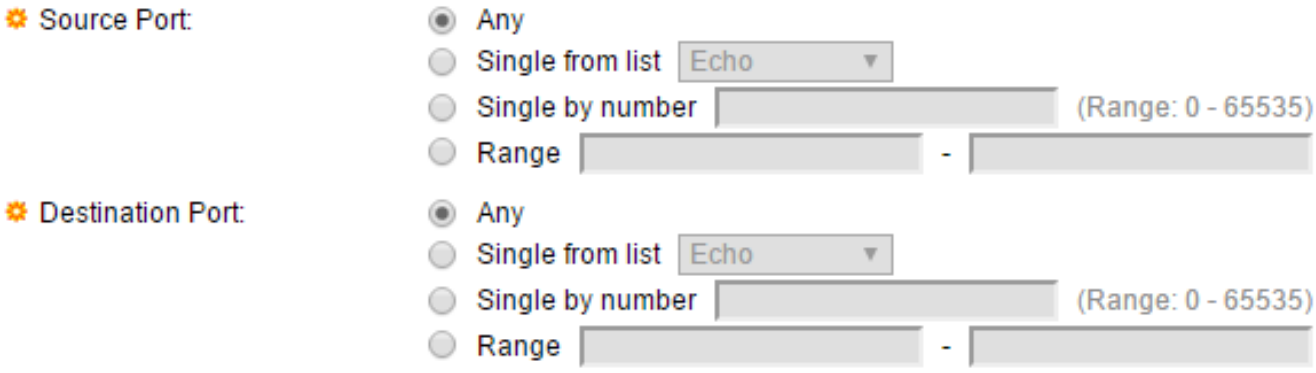


De opties zijn:

- Alle IPv6-adressen van bestemming zijn van toepassing op ACE.
- Gebruiker gedefinieerd - Voer een IP-adres en een IP-wildkaartmasker in dat op de ACE-toets moet worden toegepast in de velden *Lengte en IP-adres van bestemming*.

Opmerking: In dit voorbeeld wordt AnyRes gekozen. Als u deze optie kiest, betekent dit dat de ACE-interface die wordt aangemaakt, het ACE-verkeer dat van het gespecificeerde IPv6-adres naar elke bestemming zal toestaan.

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

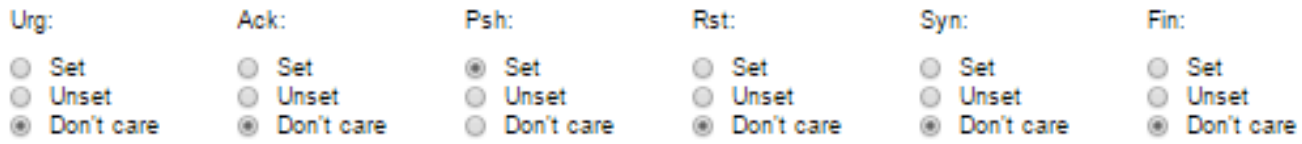
aangepast. Dit veld is alleen actief als 800/6-TCP of 800/17-UDP is geselecteerd in het vervolgkeuzemenu Lijst met selecteren.
- Bereik — U kunt een bereik van TCP/UDP-bronpoorten kiezen waaraan het pakket is aangepast. Er zijn acht verschillende poortbereiken die kunnen worden geconfigureerd (gedeeld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

Stap 17. (Optioneel) Klik op een radioknop in het gedeelte Destination Port. 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.

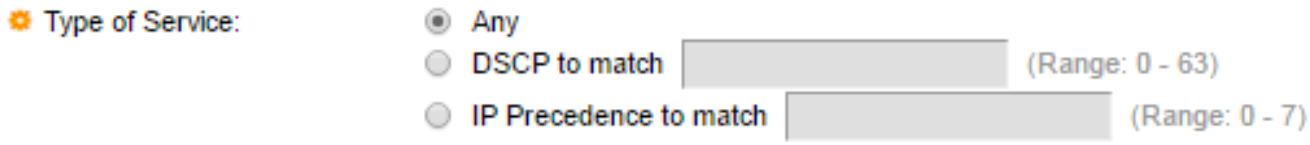
- Instellen — Overeenkomsten als de vlag is ingesteld.
- Oningesteld - Overeenkomsten als de vlag niet is ingesteld.
- Maakt niet uit — Negeer de TCP vlag.



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 — Gedifferentieerd servicescodepunt is een mechanisme voor de classificatie en het beheer 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-voorkeurswaarden is:

  - 0 — voor routine

  - 1 — prioriteit

  - 2 — onmiddellijk

  - 3 — flitser

  - 4 — voor flash-Override

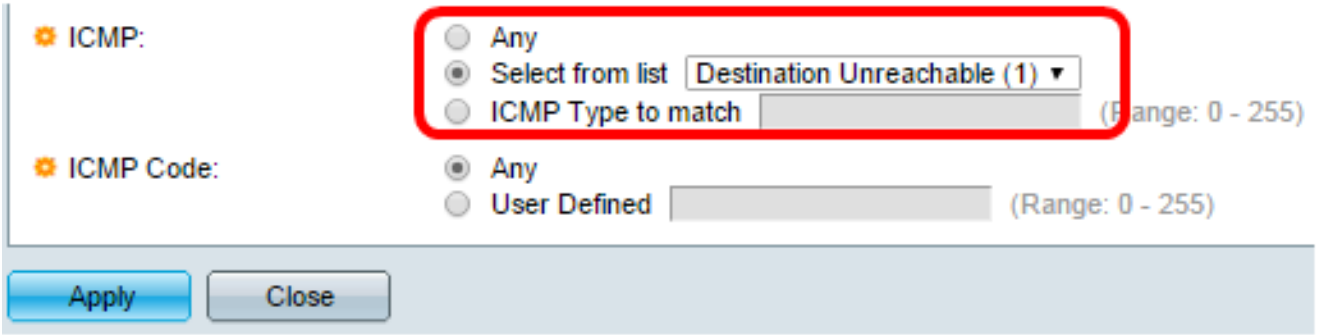
  - 5 — voor kritische

  - 6 — voor internet

  - 7 — voor het netwerk

Opmerking: In dit voorbeeld wordt AnyRes gekozen.

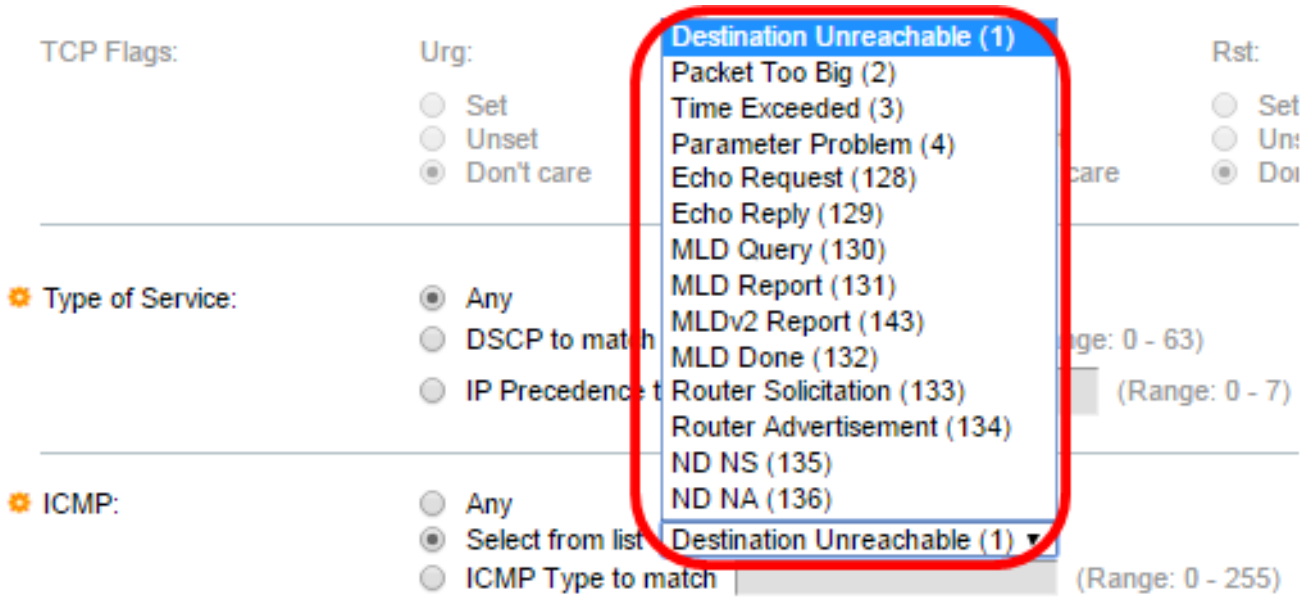
Stap 20. (Optioneel) Als het IP-protocol van de ACL ICMP is, klikt u op het ICMP-berichttype dat wordt gebruikt voor filterdoeleinden. Kies het berichttype op naam of voer het bericht type nummer in:



- 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.

Opmerking: In dit voorbeeld wordt Select Van list geselecteerd.

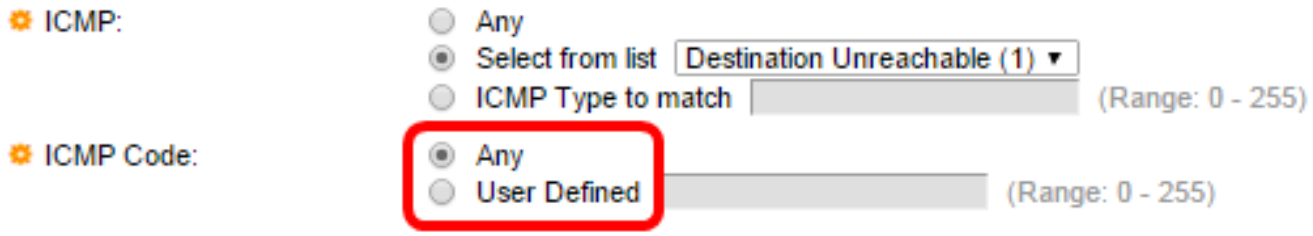
Stap 21. (Optioneel) Als u in Stap 20 uit de lijst selecteert, kiest u de controlevers om uit de mogelijke opties in de vervolgkeuzelijst te filteren:



- Doelstelling Onbereikbaar (1) — Het wordt gegenereerd door de gastheer of zijn gateway om de cliënt ervan in kennis te stellen dat de bestemming om een of andere reden onbereikbaar is (Voorbeeld: Netwerk- of hostonbereikbare fout).
- Packet Te groot (2) — De grootte van het Datagram overschrijdt de gegeven MTU.
- Tijd overschreden (3) — Het wordt gegenereerd door een poort om de bron te informeren van een afgedankte datagram vanwege de tijd om het veld onder nul te zetten.
- Parameter Probleem (4) — Het wordt gegenereerd als een reactie voor elke fout die niet specifiek door een ander ICMP-bericht wordt bestreken.
- Echo-aanvraag (128) — Het is een ping, waarvan de data naar verwachting teruggestuurd zullen worden in een echo-antwoord.
- Echo-antwoord (129) — Het wordt gegenereerd in antwoord op een echo-verzoek.
- MLD Query (130) — Het wordt gebruikt om te leren welke multicast-adressen luisteraars hebben op een aangesloten link. Type 130 in decimale volgorde.
- MPLD-rapport (131) — Het wordt gegenereerd wanneer IPv6-multicast adres waarnaar de bericht-zender luistert.
- MLD v2 Report (143) — Het is hetzelfde als MLD Report met versie 2.
- MPLS Gereed (132) — Wanneer de host een groep verlaat, stuurt ze een multicast luisteraar via een e-mailbericht naar multicast routers op het netwerk.
- Routeraanvraag (133) - Het is een bericht dat de router ontdekt. De hosts ontdekken de adressen van hun naburige routers eenvoudig wanneer zij naar advertenties luisteren. Standaard is 224.0.0.2 voor multicast, anders is het 255.255.255.255.
- Router Advertisement (134) — De router multicast periodiek een routeradvertentie van elk van zijn multicast interfaces, en kondigt de IP-adressen van die interface aan.
- ND NS (135) — Berichten worden gegenereerd door knooppunten om het adres van de verbindingslaag van een ander knooppunt te vragen en ook voor functies zoals dubbele adresdetectie en onbereikbaarheidsdetectie van de buren.
- ND NA (136) — Berichten worden verstuurd als antwoord op NS-berichten. Als een knooppunt zijn link-laagadres wijzigt, kan het een ongevraagd netwerk verzenden om het nieuwe adres bekend te maken.

Stap 2. (Optioneel) De ICMP-berichten kunnen een codeveld hebben dat aangeeft hoe u het

bericht wilt verwerken. Dit is ingeschakeld als u in Stap 10 het ICMP-protocol kiest. Klik op een van de volgende opties om te configureren of u een filter in deze code wilt uitvoeren:

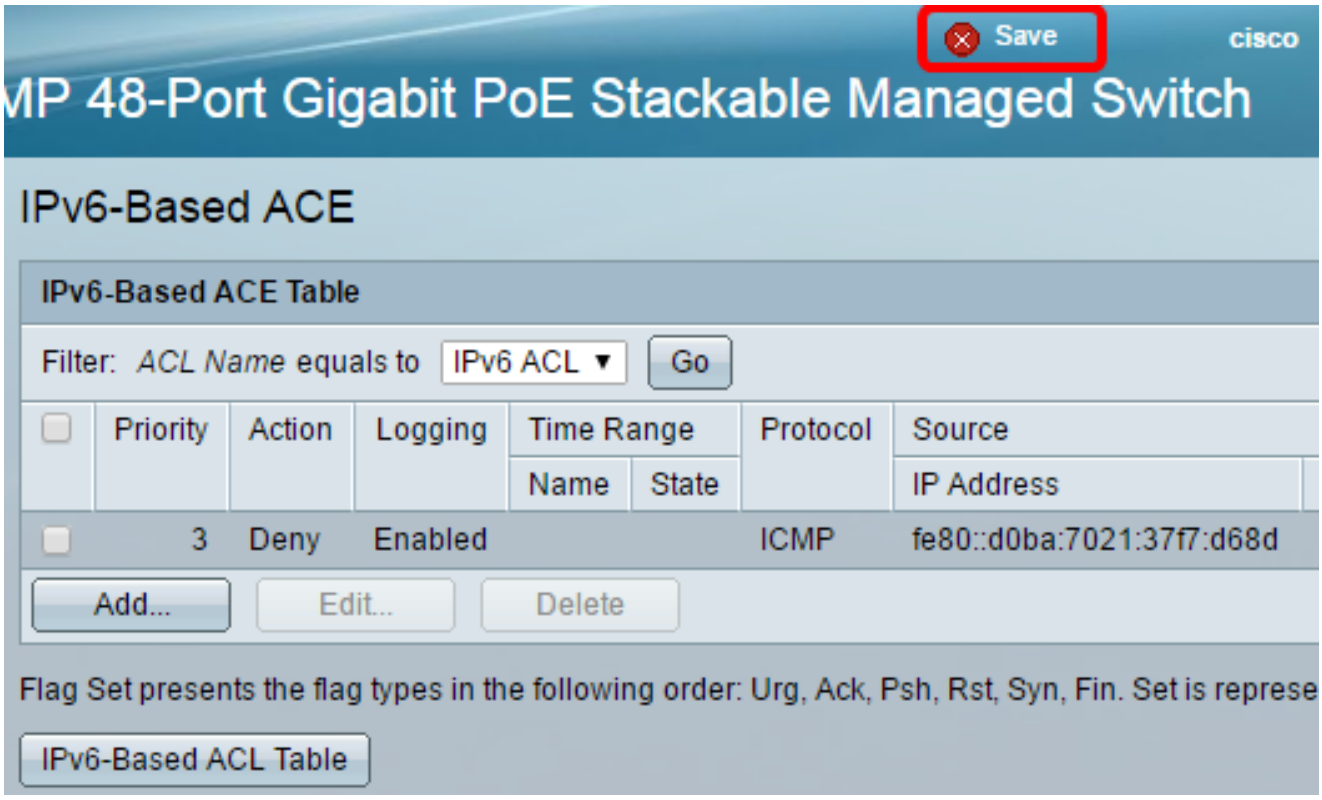


- Alle — Alle codes accepteren.
- Gebruikershandleiding — U kunt een ICMP-code invoeren voor filterdoeleinden.

Opmerking: In dit voorbeeld wordt AnyRes gekozen.

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 IPv6 gebaseerde ACE op uw schakelaar moeten hebben ingesteld.