Een MAC-gebaseerde ACL op basis van SG350XG en SG550XG

Doel

Een toegangscontrolelijst (ACL) is een verzameling regels die kan worden gemaakt om pakketten te manipuleren, afhankelijk van of ze aan bepaalde criteria voldoen. Deze criteria kunnen bron- of doeladressen, veldnamenvelden en andere verschillende onderdelen van een pakket zijn. Als een pakket aan de gespecificeerde criteria van ACL voldoet, wordt het ingetrokken of toegestaan om verder te gaan. Een MAC-Based ACL gebruikt regels die Layer 2 van een pakket analyseren voor deze criteria, zoals MAC-adressen, VLAN-ID's en EtherType-waarden. Het implementeren van een MAC-Based ACL staat u toe om pakketten die over de switch reizen op Laag 2 niveau te controleren.

Het doel van dit document is om u te tonen hoe u een MAC-gebaseerde ACL kunt maken en configureren op de SG350XG en SG550XG switches.

Toepasselijke apparaten

- SG350XG router
- SG550XG router

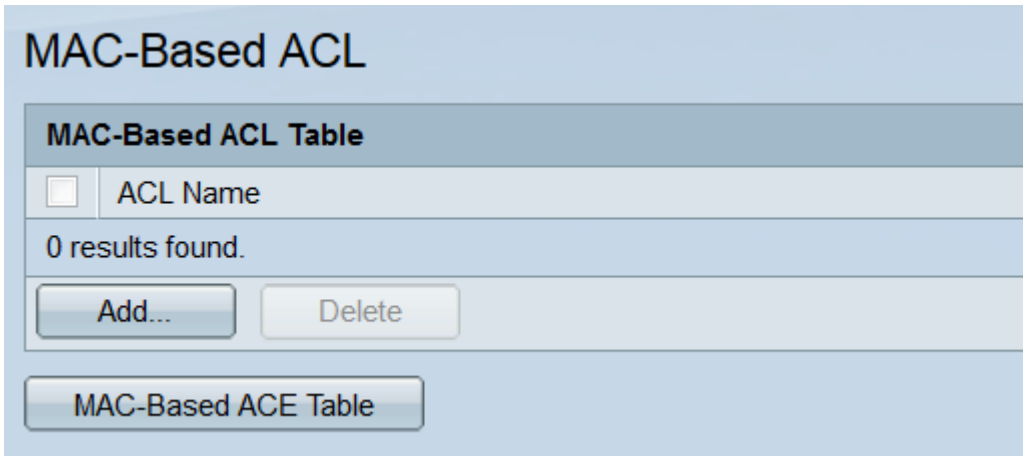
Softwareversie

- v2.0.0.73

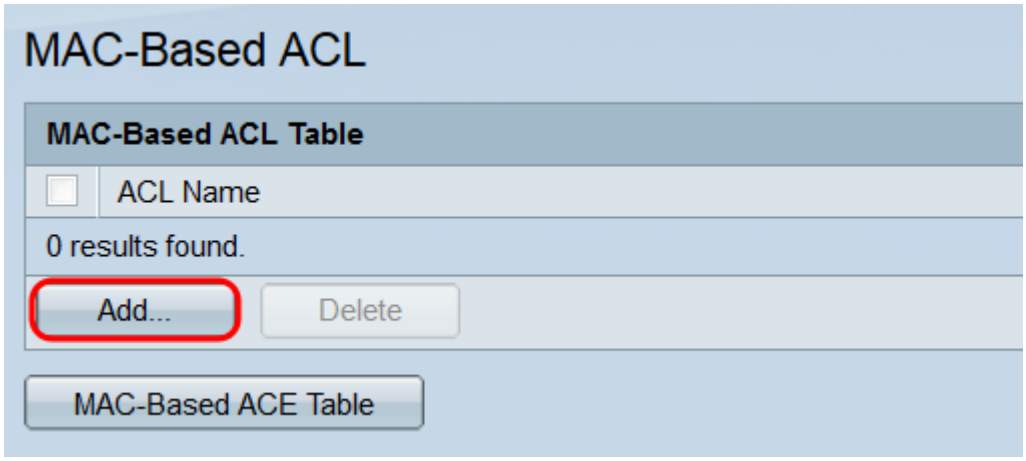
Configuratie MAC-gebaseerde ACL's

Creëren een ACL en regels

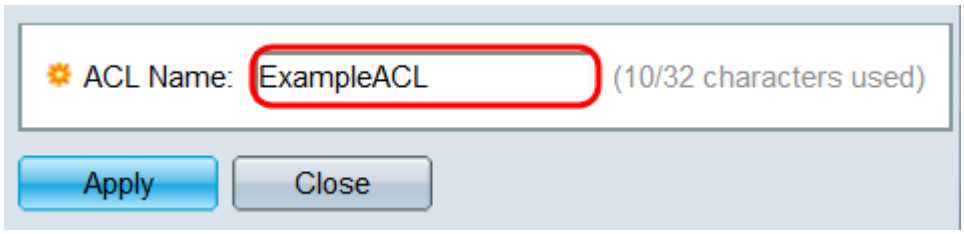
Stap 1. Meld u aan bij het web configuratie hulpprogramma en kies **toegangscontrole > MAC-gebaseerde ACL**. De *MAC-gebaseerde ACL*-pagina wordt geopend.



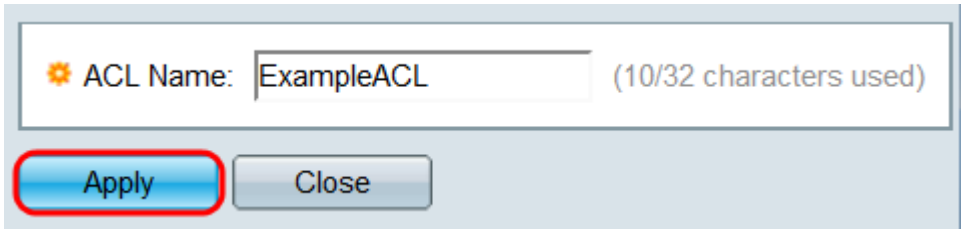
Stap 2. De *MAC-gebaseerde ACL-tabel* zal alle MAC-gebaseerde ACL's op de switch weergeven. Klik op de knop **Toevoegen** om een nieuwe ACL te maken. Het *Add MAC-Based ACL* wordt geopend.



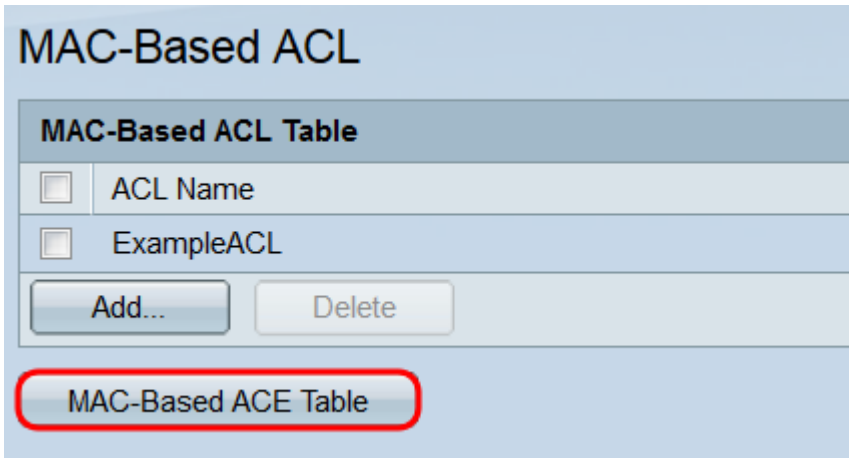
Stap 3. Voer in het veld *ACL-naam* in de naam van de nieuwe ACL. Deze naam heeft geen invloed op de functie van ACL en is alleen bedoeld voor identificatiedoeleinden.



Stap 4. Klik op **Toepassen**. De nieuwe ACL wordt toegevoegd aan de *MAC-gebaseerde ACL-tabel*. Klik op **Close** om naar de *MAC-gebaseerde ACL*-pagina terug te keren of een andere ACL te maken door de vorige stap te herhalen.

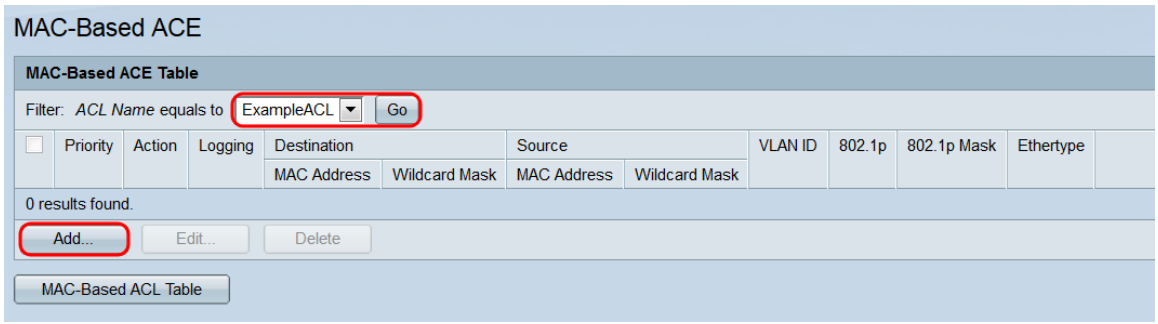


Stap 5. Alle nieuw gemaakte ACL's zijn leeg; Dat wil zeggen, het zal geen regels bevatten om pakketten te blokkeren of toe te staan gebaseerd op de adressen van MAC. Om deze regels te maken moet een ingang van de toegangscontrole (ACE) aan ACL worden toegevoegd. Om dit te doen, klik op de **MAC-Based ACE-**knop om naar de *MAC-Based ACE*-pagina te gaan.

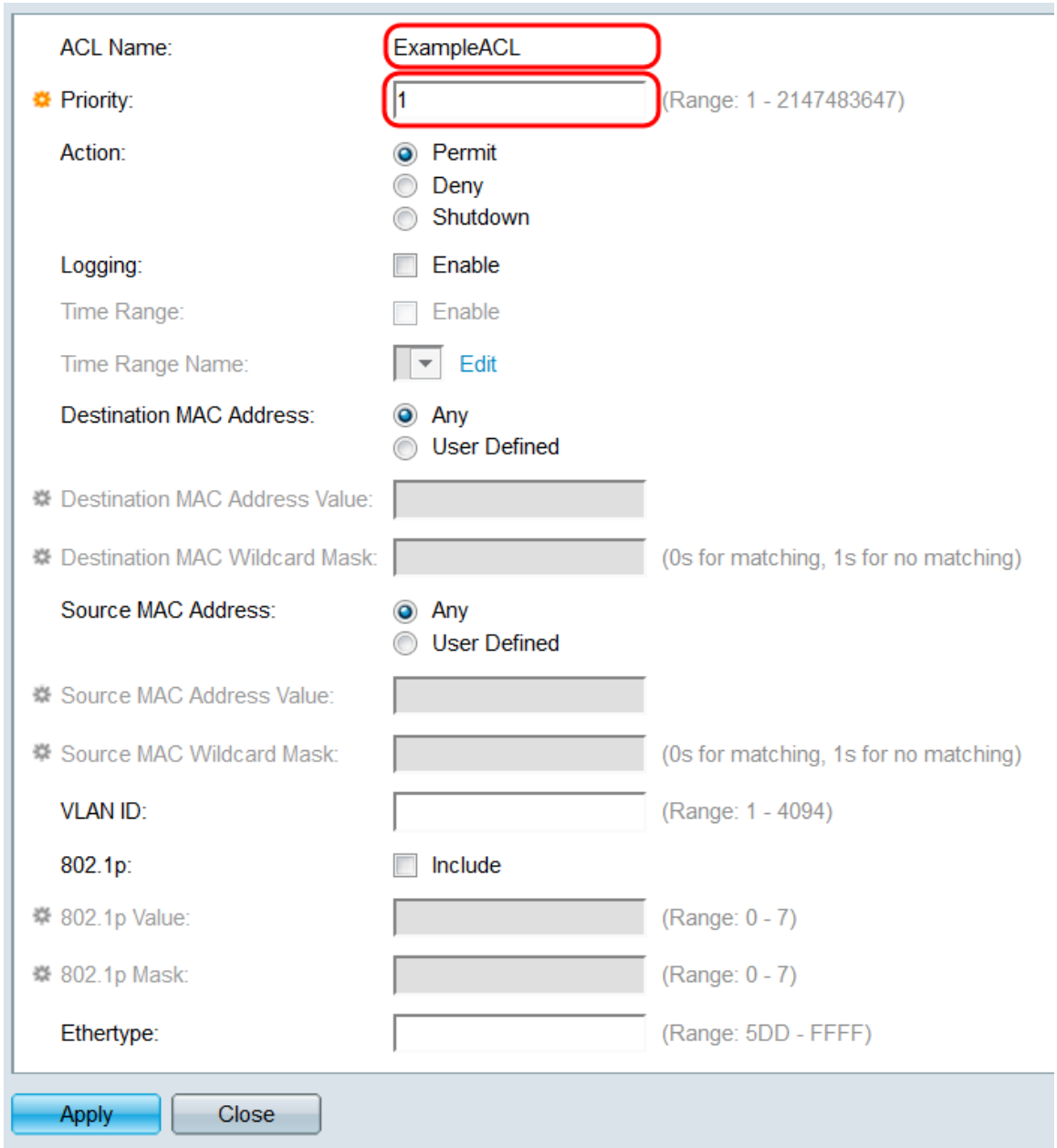


Stap 6. Selecteer op de *MAC-Based ACE*-pagina de ACL die u aan een ACE wilt toevoegen via de vervolgkeuzelijst boven in de *MAC-Based ACE-tabel* en klik op **Ga**. De tabel toont

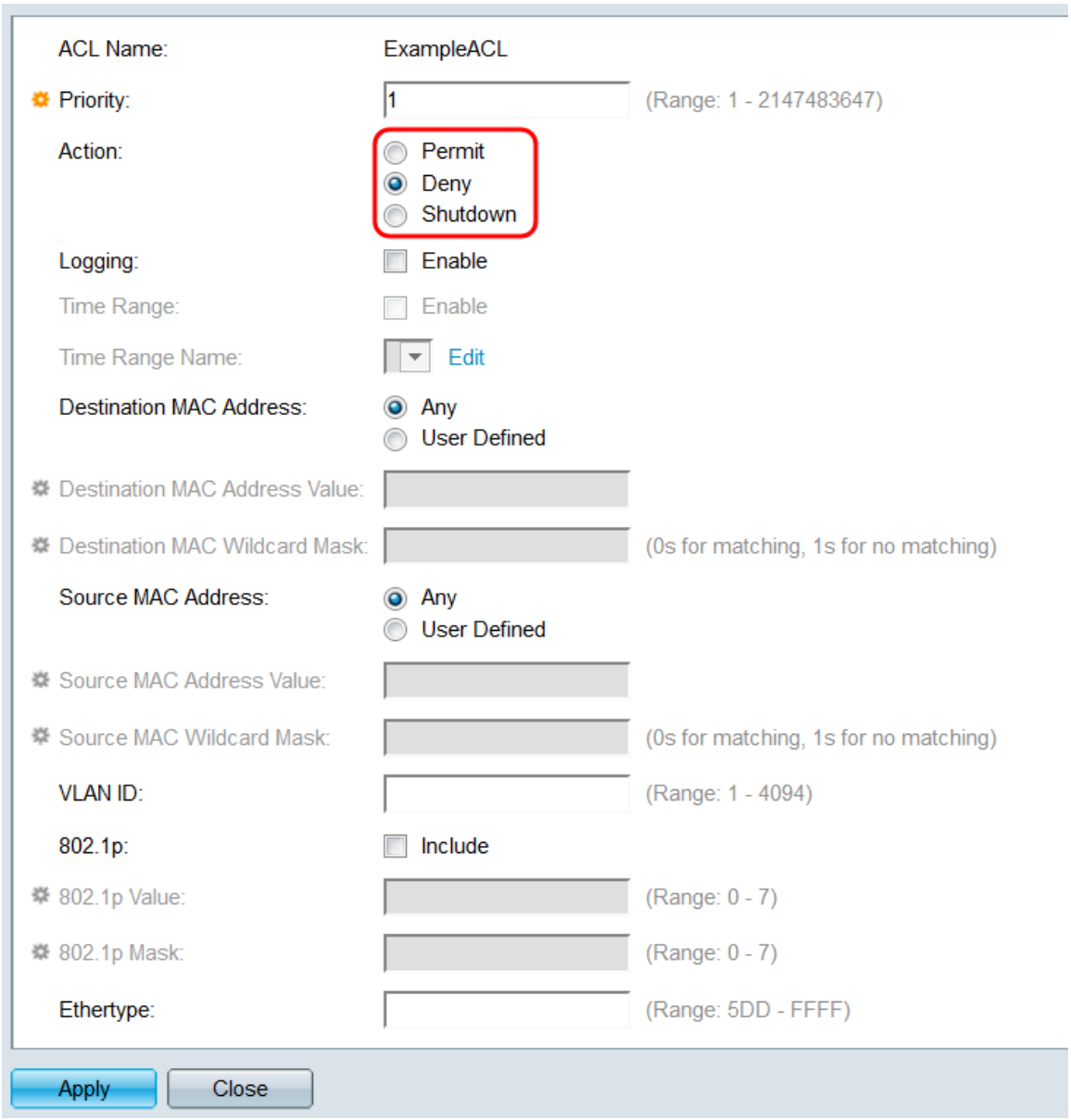
ACE's die momenteel met de geselecteerde ACL zijn geassocieerd. Als u een ACE wilt toevoegen, klikt u op de knop **Toevoegen...**. Het *Add MAC-Based ACE* venster wordt geopend.



Stap 7. Het veld *ACL-naam* toont de naam van de ACL waaraan u een ACE toevoegt. Voer in het *prioriteitsveld* een prioriteitsnummer in voor het ACE. Hoe hoger de prioriteit van een ACE, hoe sneller het zal worden verwerkt. De marge loopt van 1 tot 2147483647, waarvan 1 de hoogste prioriteit heeft.



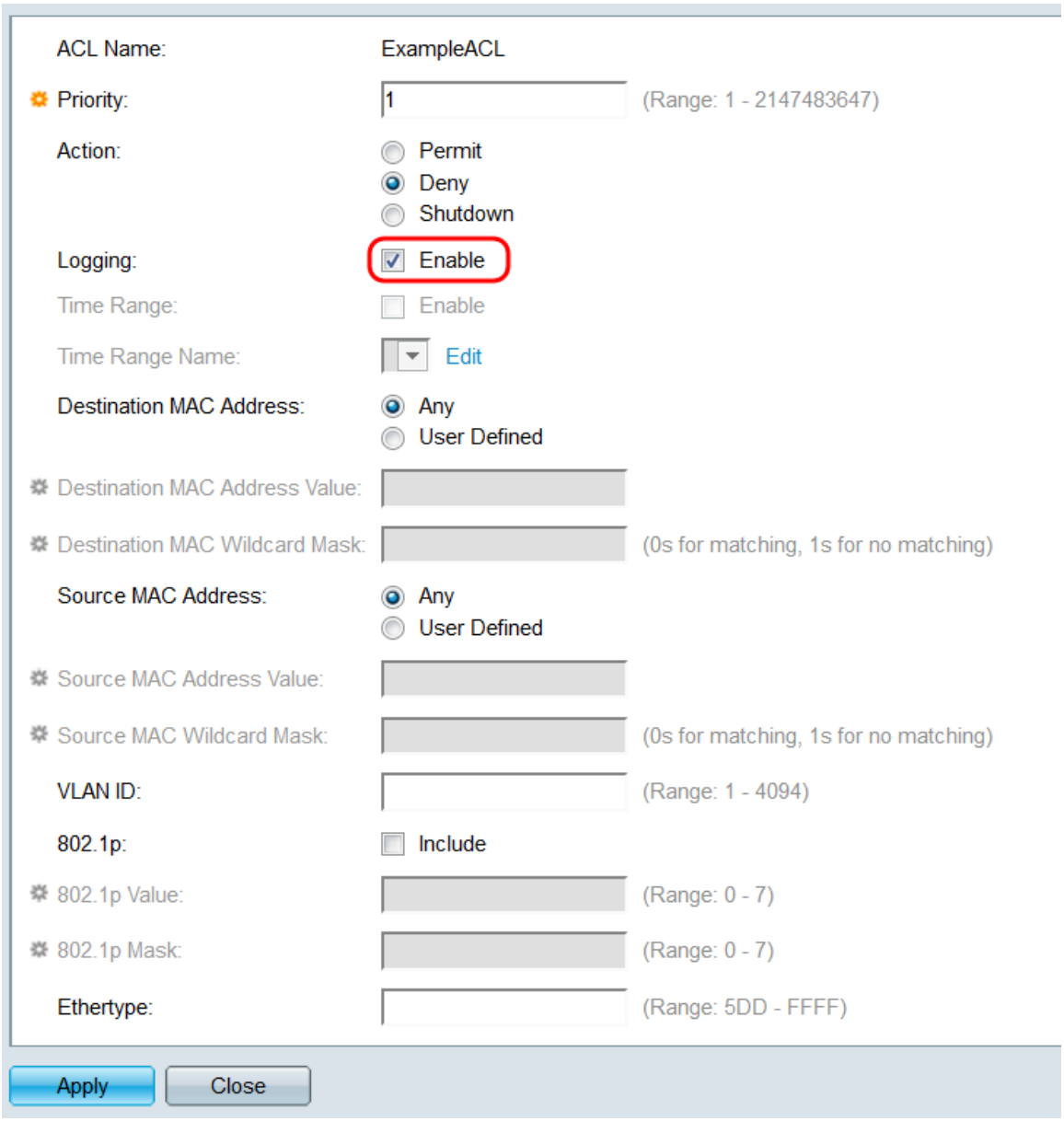
Stap 8. Selecteer in het veld *Action* een radioknop om te bepalen wat er zal gebeuren wanneer aan de criteria van ACE wordt voldaan.



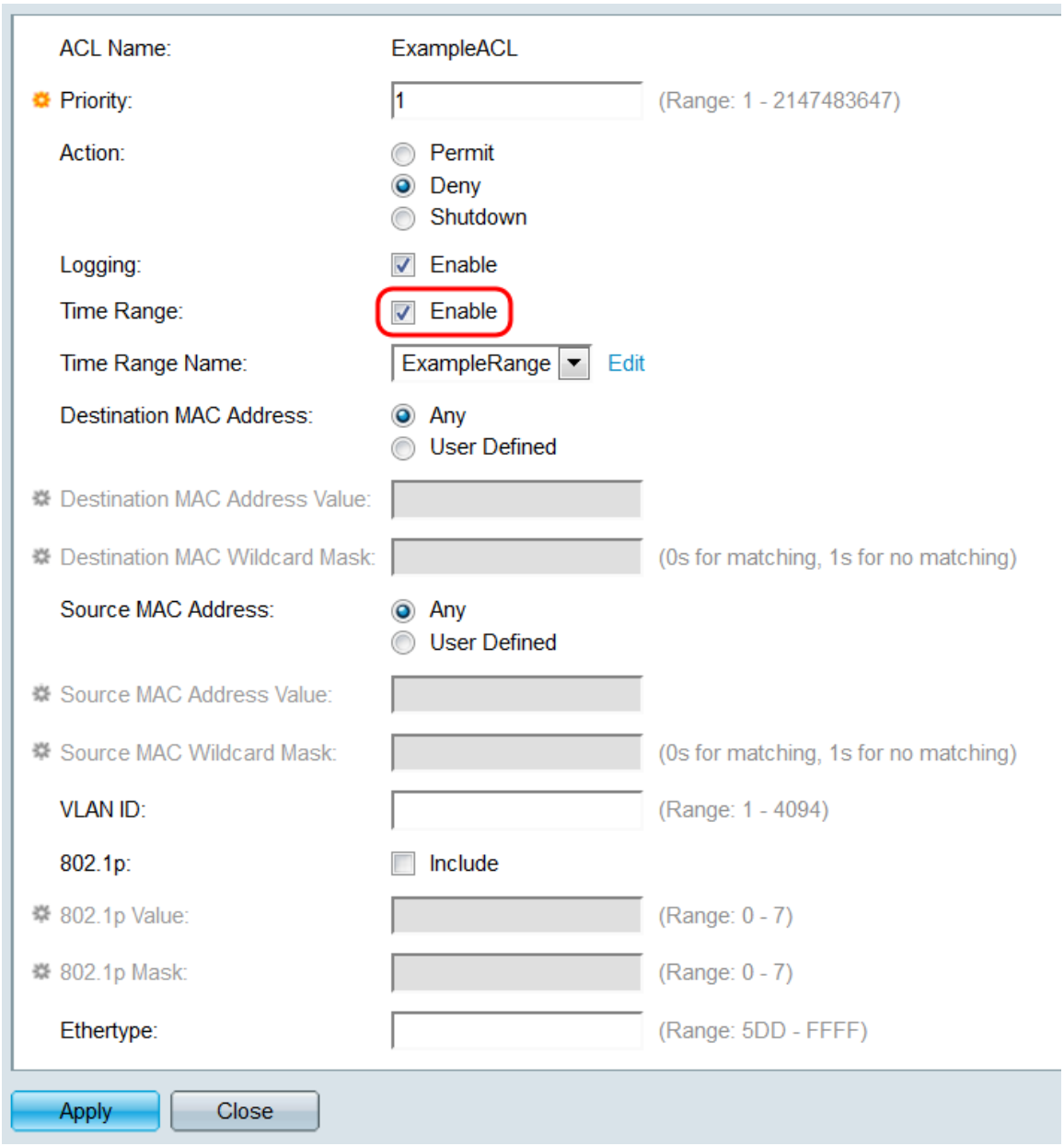
De opties zijn:

- Vergunning - Verzenden van pakketten die aan de criteria voldoen.
- Jeans - neer pakketten die aan de criteria voldoen.
- Sluiten - Stalen pakketten die aan de criteria voldoen, en dan de poort uitschakelen.

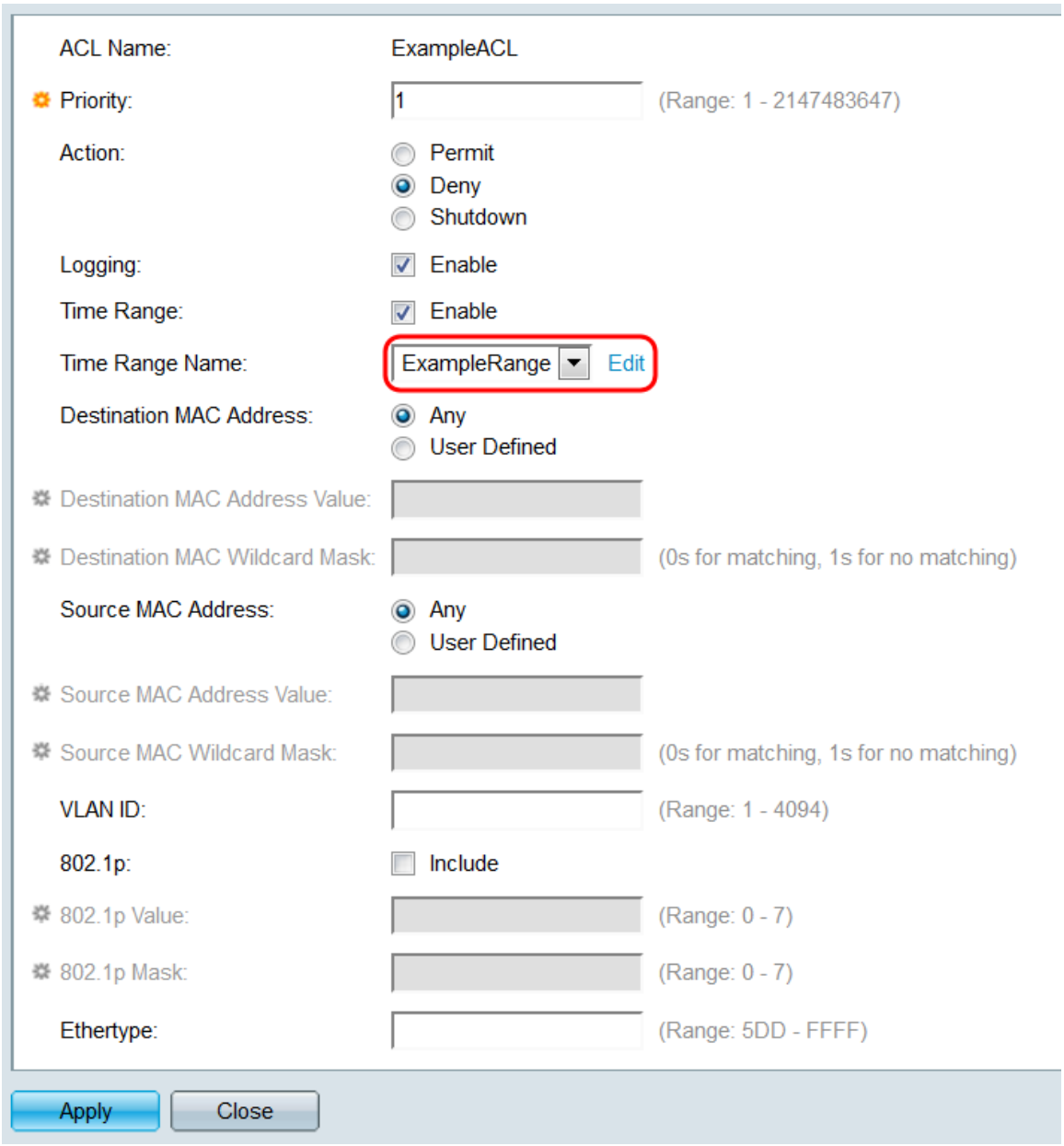
Stap 9. In het veld *Vastlegging*, controleert u het selectieteken Enable om ACL-stromen die overeenkomen met de ACE-regel in te schakelen. Als u de Basis-weergavemodus gebruikt, slaat u de CIP over naar Stap 12. De weergavemodus kan worden gewijzigd via de vervolgkeuzelijst rechtsboven in het webprogramma.



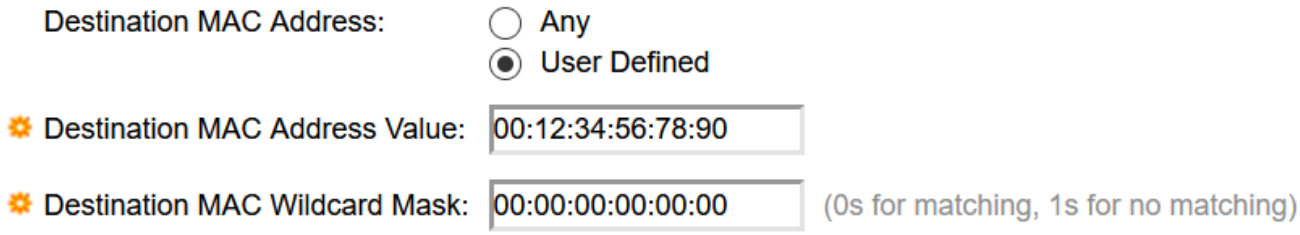
Stap 10. In het veld *Tijdbereik* controleert u het selectieteken **Inschakelen** om te zien dat de ACE alleen actief is binnen een gespecificeerd tijdbereik. Als er geen bestaande tijdbereiken op de switch zijn ingesteld, is dit veld niet beschikbaar.



Stap 1. Als u een tijdbereik voor deze ACE hebt geactiveerd, is het veld *Naam tijdbereik* beschikbaar. Gebruik de vervolgkeuzelijst om een tijdbereik te selecteren dat al in de switch is ingesteld om op de ACE toe te passen. Als er geen tijdbereiken op de switch bestaan, is dit veld niet beschikbaar. Klik op de koppeling **Bewerken** om naar de pagina *Tijdbereik te gaan* om tijdbereiken te maken of aan te passen. Raadpleeg voor meer informatie het artikel *Een tijdbereik instellen op SG350XG en SG550XG*.



Stap 12. In het veld *MAC-adres van de bestemming* selecteert u een radioknop om te bepalen welke MAC-adressen van de bestemming overeenkomen. Selecteer **Any** om een doeladres als overeenkomend te hebben, of **door gebruiker** gedefinieerd om een adres of bereik van adressen op te geven.



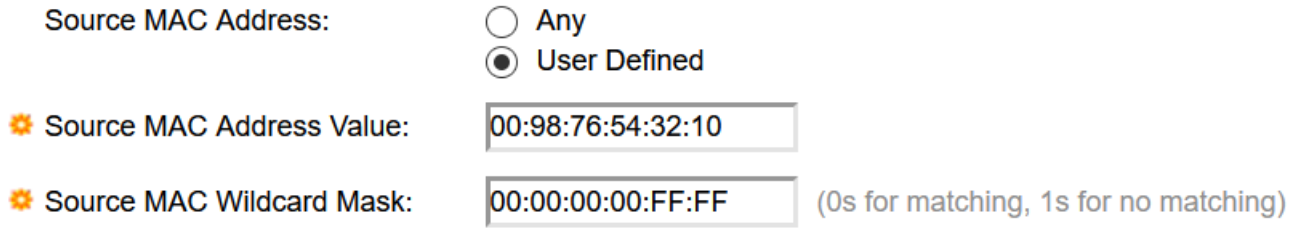
Als u **Gebruiker** heeft geselecteerd, vult u de volgende velden in:

- MAC-adreswaarde van bestemming - Voer het MAC-adres van de bestemming in. Als een pakket dit doeladres bevat, beschouwt de ACE-band het als een overeenkomst.
- MAC Wildcard-masker van de bestemming - Voer een masker in om een bereik van adressen te definiëren. Wanneer u een beetje instelt als 1, wordt het corresponderende bit in het MAC-

adres genegeerd en 0's worden bits bijgesneden.

Opmerking: Met een masker van 0000 0000 0000 000 000 000 000 000 000 000 000 000 000 000 1111111 (dat betekent dat je daar op de bits aansluit 0 en niet op de bits waar er 1 s is). Je moet de 1's vertalen naar een hexadecimale waarde en je schrijft 0 voor elke vier nullen. In dit voorbeeld sinds 1111 1111 = FF wordt het masker geschreven: 12:00:00:00:00

Stap 13. In het veld *Bron-MAC-adres* selecteert u een radioknop om te bepalen welke bron-MAC-adressen overeenkomen. Selecteer **Any** om een bronadres als overeenkomend te hebben, of **door gebruiker gedefinieerd** om een adres of een bereik van adressen op te geven.



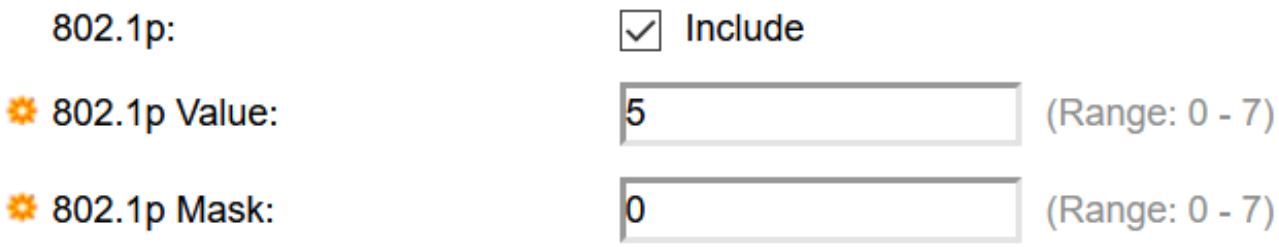
Als u **Gebruiker** heeft geselecteerd, vult u de volgende velden in:

- Bron MAC-adreswaarde - Voer het bron-MAC-adres in. Als een pakket dit bronadres bevat, overweegt ACE het een overeenkomst.
- Bron: MAC Wildcard masker - Voer een masker in om een bereik van adressen te definiëren. Wanneer u een bit als 1 instelt, wordt het corresponderende bit in het MAC-adres genegeerd en worden 0's bits bijgesteld (bijv. 00:00:00:00:11).

Opmerking: Met een masker van 0000 0000 0000 000 000 000 000 000 000 000 000 000 000 000 1111111 (dat betekent dat je daar op de bits aansluit 0 en niet op de bits waar er 1 s is). Je moet de 1's vertalen naar een hexadecimale waarde en je schrijft 0 voor elke vier nullen. In dit voorbeeld sinds 1111 1111 = FF wordt het masker geschreven: 12:00:00:00:00

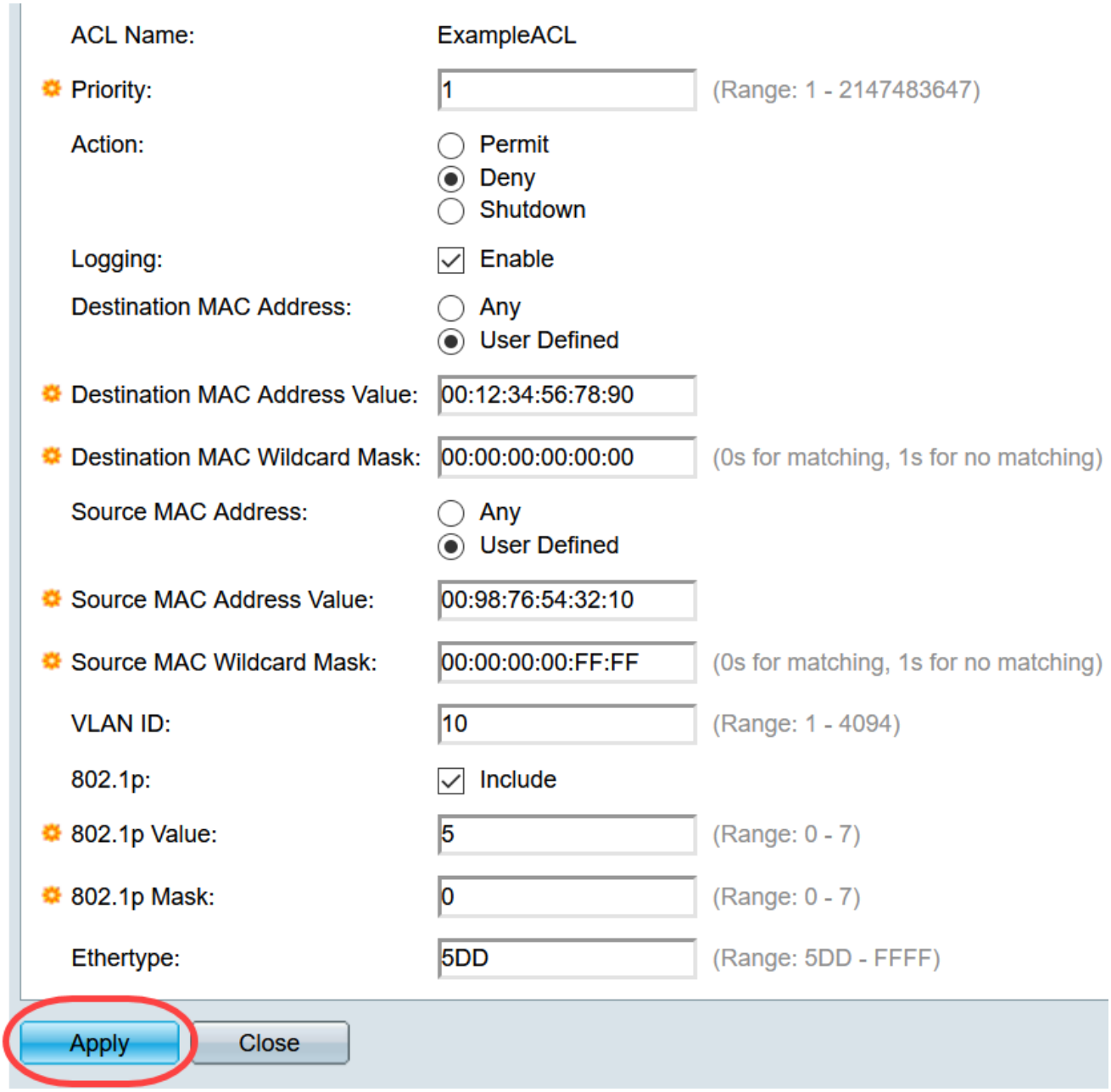
Stap 14. Voer in het veld *VLAN-id* een VLAN-id in uit 1-4094. Als een pakket dit VLAN-id bevat, overweegt ACE het een overeenkomst. Dit veld is niet vereist. Als u het leeg laat, hoeft u geen VLAN-ID's te overwegen bij het controleren van pakketten.

Stap 15. In het veld *802.1p*, controleer het selectieteken **Inclusief** om de ACE-toets 802.1p te laten bevatten. Als u 802.1p-criteria hebt meegeleverd, voert u een 802.1p-waarde en een masker in respectievelijk *802.1p-waarde* en *802.1p-masker* in. Het bereik voor beide velden is 0-7. Als een pakket de corresponderende 802.1p waarde bevat en het masker past, beschouwt de ACE het als een overeenkomst.



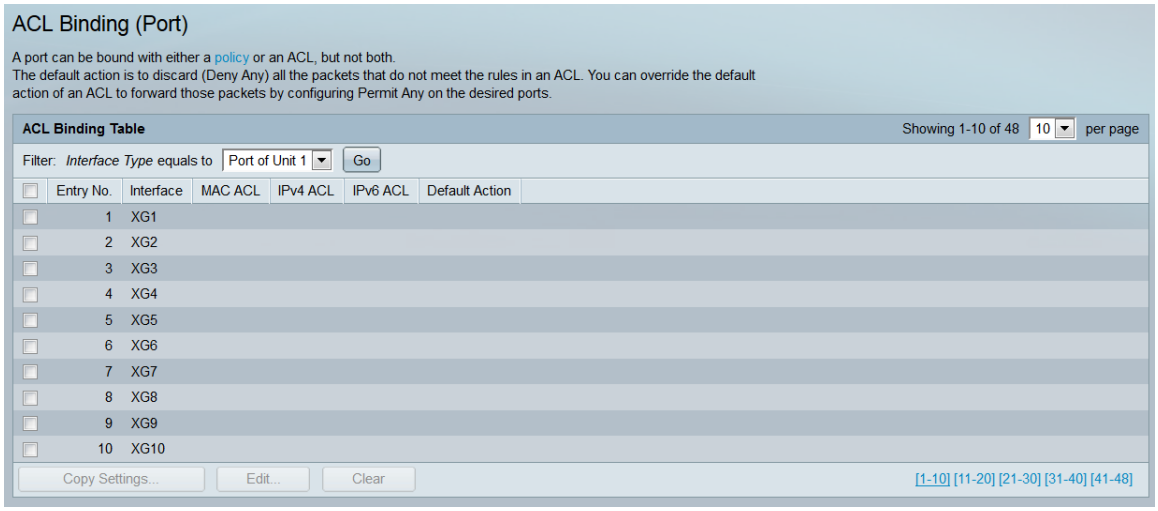
Stap 16. Voer in het veld *EtherType* een waarde in die u tegenover inkomende pakketten kunt vergelijken. EtherType is een veld met twee letters in een kader dat aangeeft welk protocol in het pakket is ingesloten. Het bereik is 5DD- FFFF. Als een pakket de gespecificeerde EtherType-waarde bevat, zal ACE het een overeenkomst overwegen. U vindt een lijst met EtherSwitch-waarden op deze pagina met IEEE-standaarden.

Stap 17. Klik op **Toepassen**. ACE wordt toegevoegd aan de gespecificeerde ACL. Klik op **Close** om terug te keren naar de *MAC-gebaseerde ACE*-pagina.

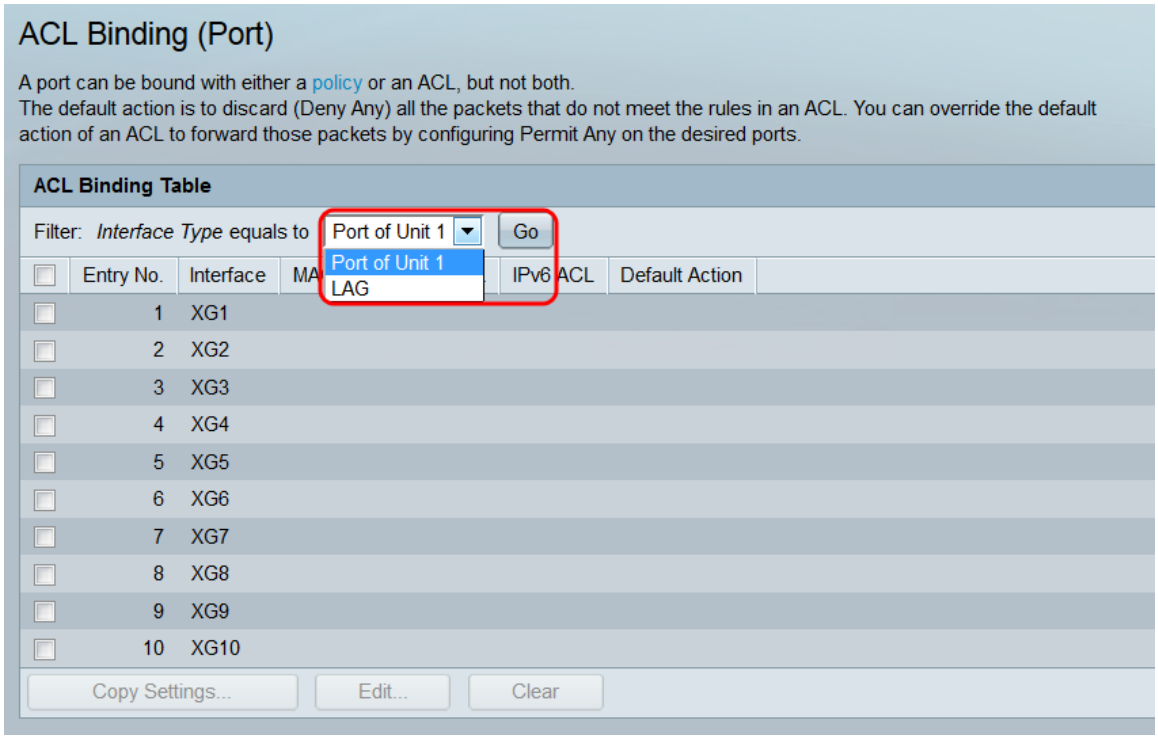


Toewijzing van een MAC-gebaseerde ACL naar poorten

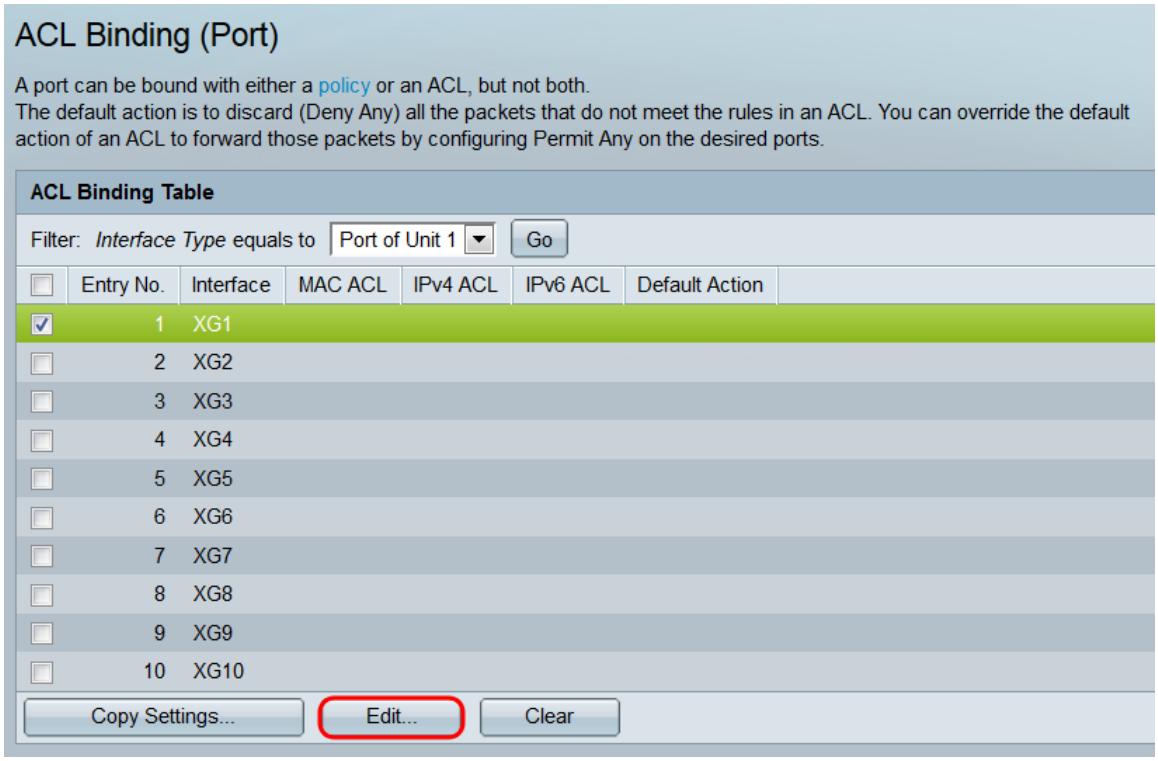
Stap 1. ACL kan aan of poorten of VLAN's worden toegewezen. Om een MAC-Based ACL aan een poort of poorten in kaart te brengen, navigeer naar **toegangscontrole > ACL-binding (poort)**. De *ACL*-pagina *(Poort)* wordt geopend.



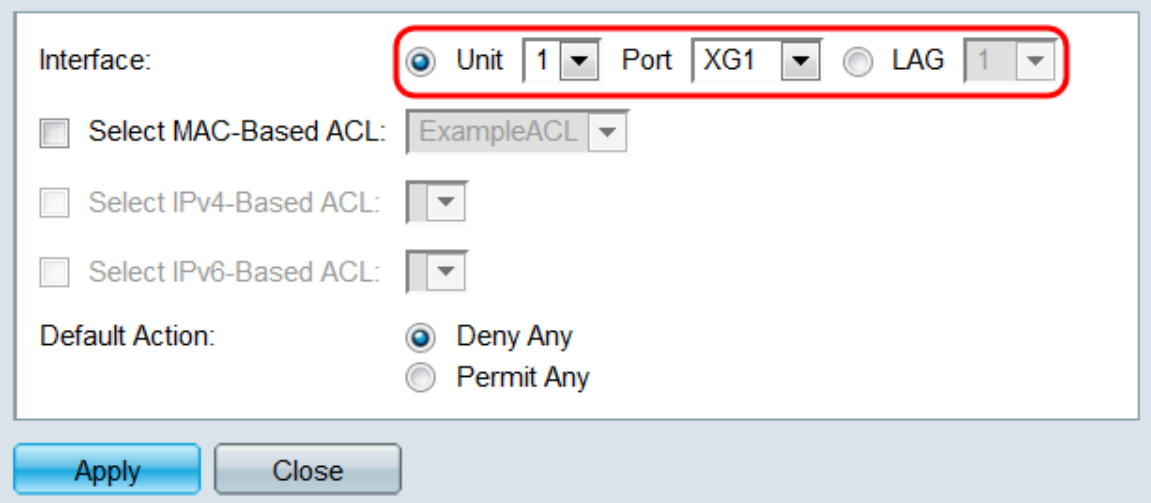
Stap 2. In de vervolgkeuzelijst boven in de *ACL-bindende tabel* selecteert u poorten of LAG (groep voor aggregatie van link) als interfacetype. Als de switch deel uitmaakt van een stapel, kunnen poorten van andere eenheden worden geselecteerd. Klik op **Ga** om een lijst van het gespecificeerde interfacetype weer te geven.



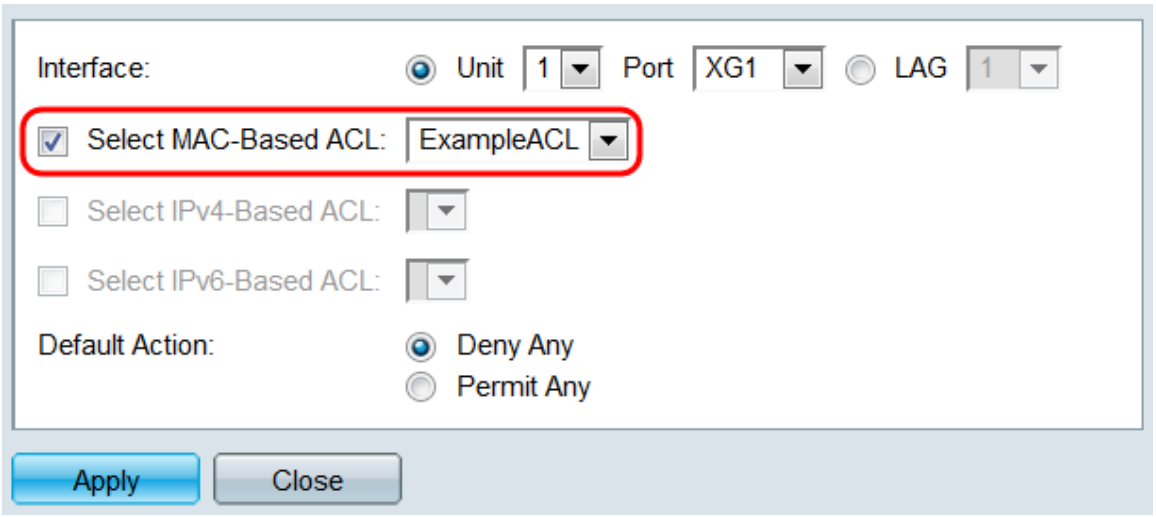
Stap 3. Selecteer het selectieteken van een interface en klik vervolgens op de knop **Bewerken...**. Het venster *ACL-binding bewerken* wordt geopend.



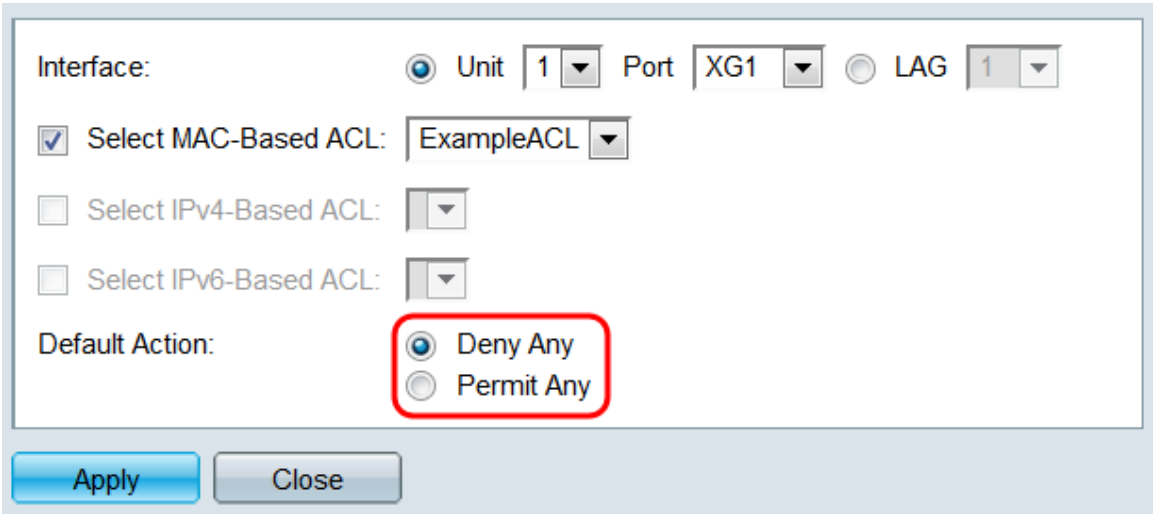
Stap 4. Het veld *Interface* geeft de poort of LAG weer die op dit moment wordt geconfigureerd. Het zal automatisch de interface tonen die in de *ACL Bindende Tabel* wordt geselecteerd. Dit veld kan worden gebruikt om snel tussen verschillende interfaces te switches zonder naar de *ACL*-pagina *(Poort)* terug te keren.



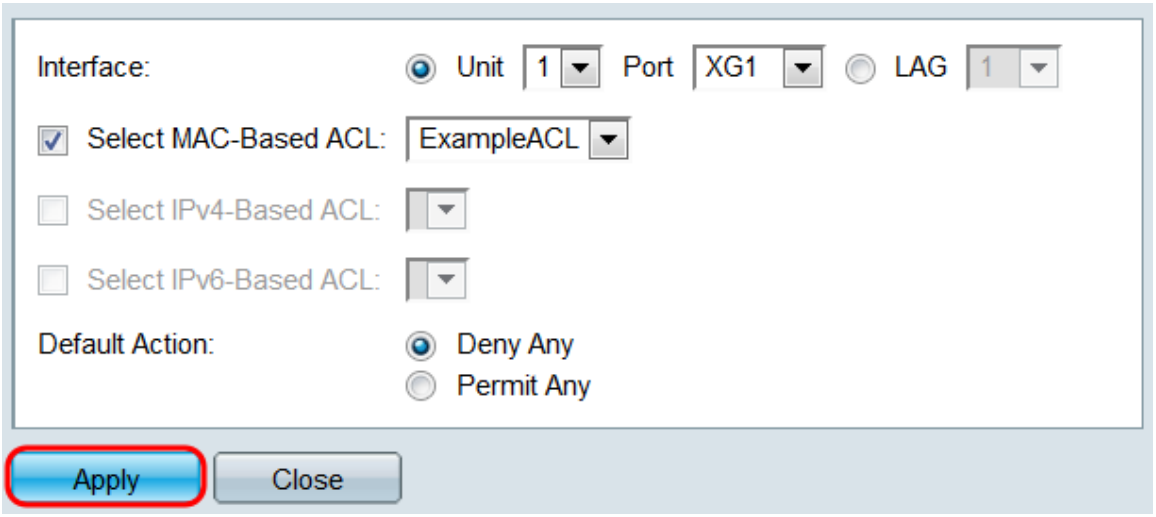
Stap 5. Controleer het selectieteken **MAC-Based ACL** en gebruik de vervolgkeuzelijst om een ACL te selecteren om naar de gespecificeerde interface te tekenen.



Stap 6. In het veld *Default Action* selecteert u een radioknop om te bepalen hoe pakketten die niet overeenkomen met de criteria van ACL worden verwerkt. De standaardinstelling is **Deny Any**, waardoor alle pakketten die niet aan de criteria van ACL beantwoorden, worden weggelaten; **Geef** toe dat **Any** andere pakketten worden verzonden.

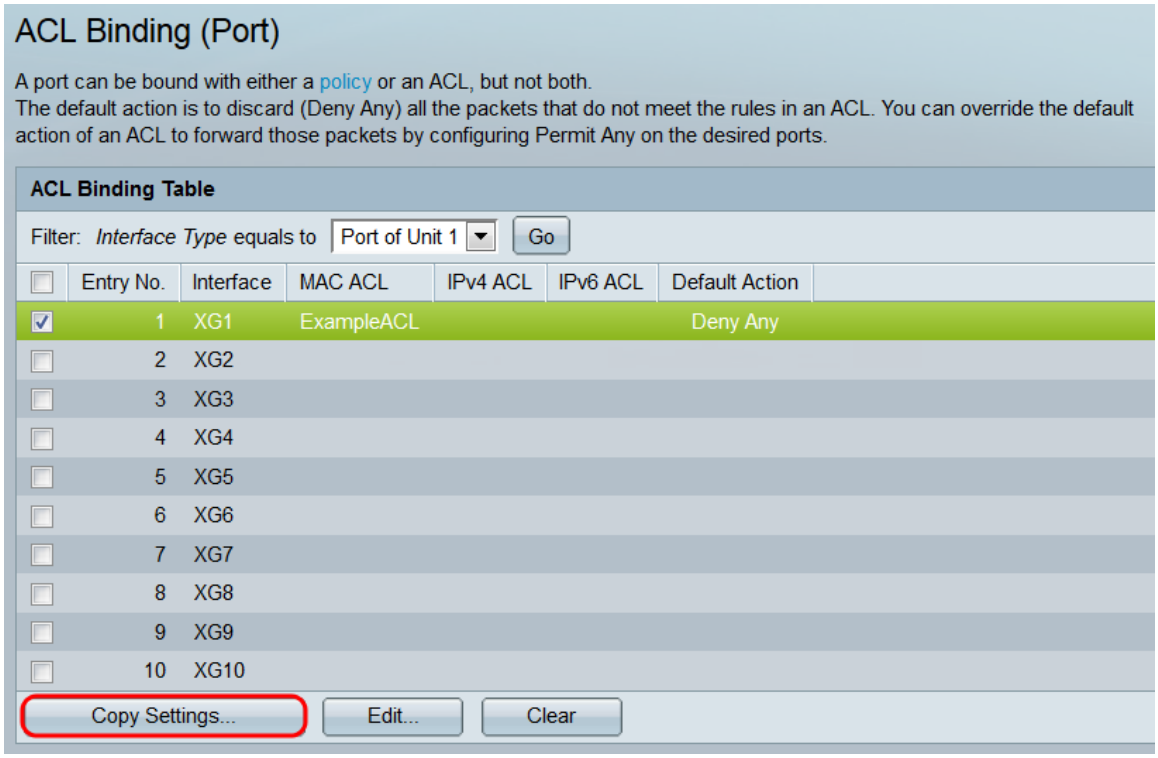


Stap 7. Klik op **Toepassen**. ACL wordt in kaart gebracht aan de gespecificeerde interface. U kunt het veld *Interface* gebruiken om een andere interface te selecteren om te configureren of op **Close** klikken om terug te keren naar de *ACL*-pagina *(poort)*.

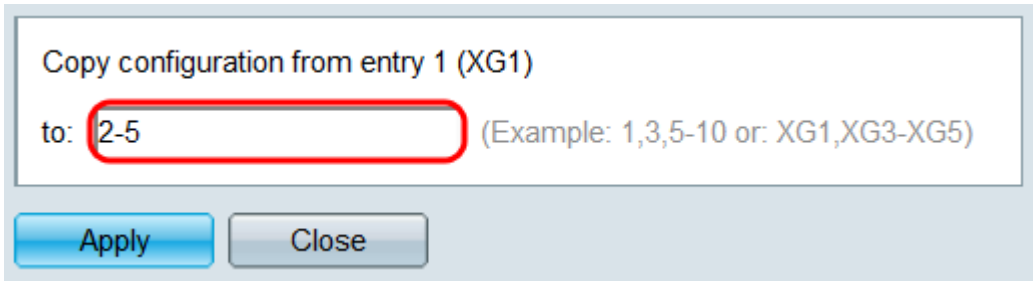


Stap 8. Als u de instellingen van een interface snel naar andere interfaces wilt kopiëren, selecteert u het selectieteken van de interface die u wilt kopiëren en vervolgens klikt u op de

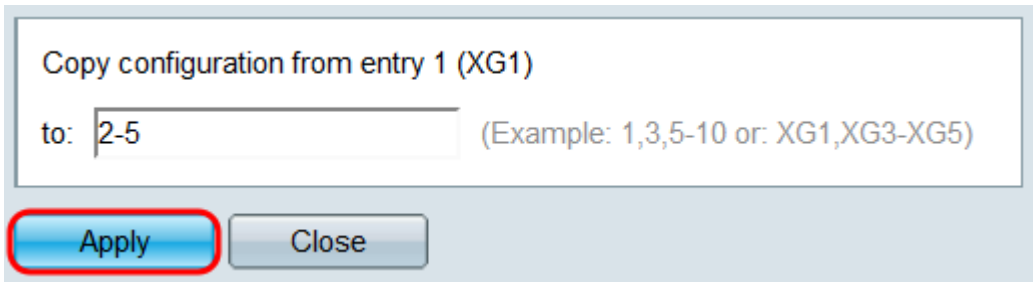
knop **Kopie**.. Het venster *Instellingen kopiëren* wordt geopend.



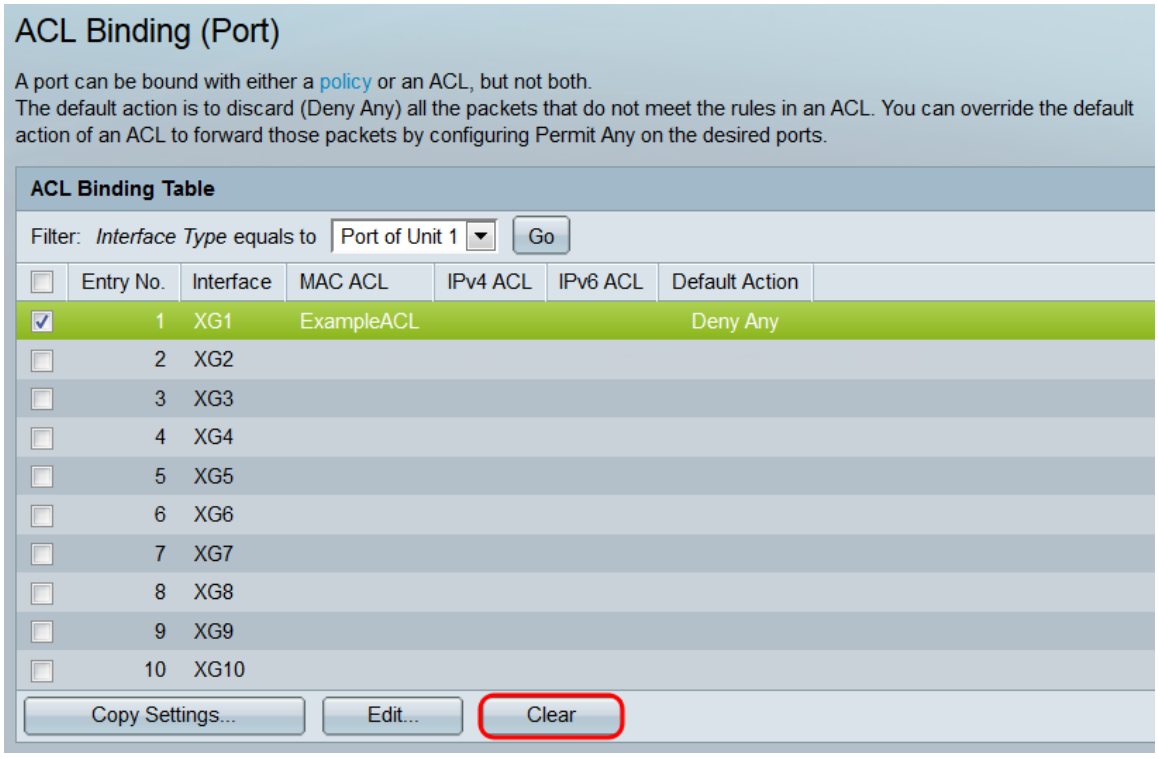
Stap 9. Voer in het tekstveld de interface of interfaces in waarop u instellingen wilt kopiëren. De interfaces kunnen worden gescheiden door komma's, of er kan een bereik worden opgegeven.



Stap 10. Klik op **Toepassen**. De instellingen worden gekopieerd.

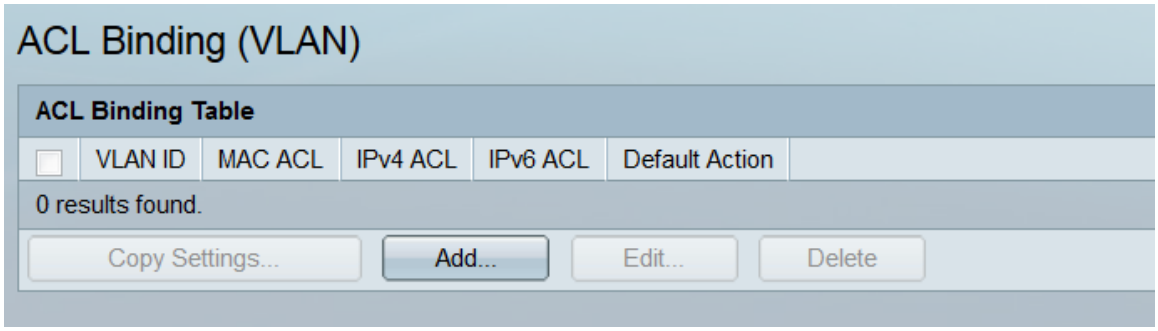


Stap 1. Als u de instellingen van een interface wilt wissen, selecteert u het bijbehorende vakje en klikt u op **Wissen**. Merk op dat meerdere interfaces tegelijkertijd kunnen worden geselecteerd en gewist.

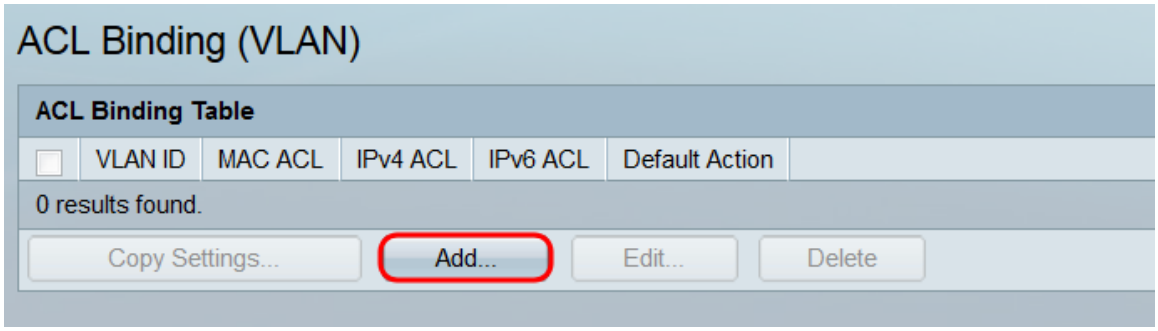


Toewijzing van een MAC-gebaseerde ACL's

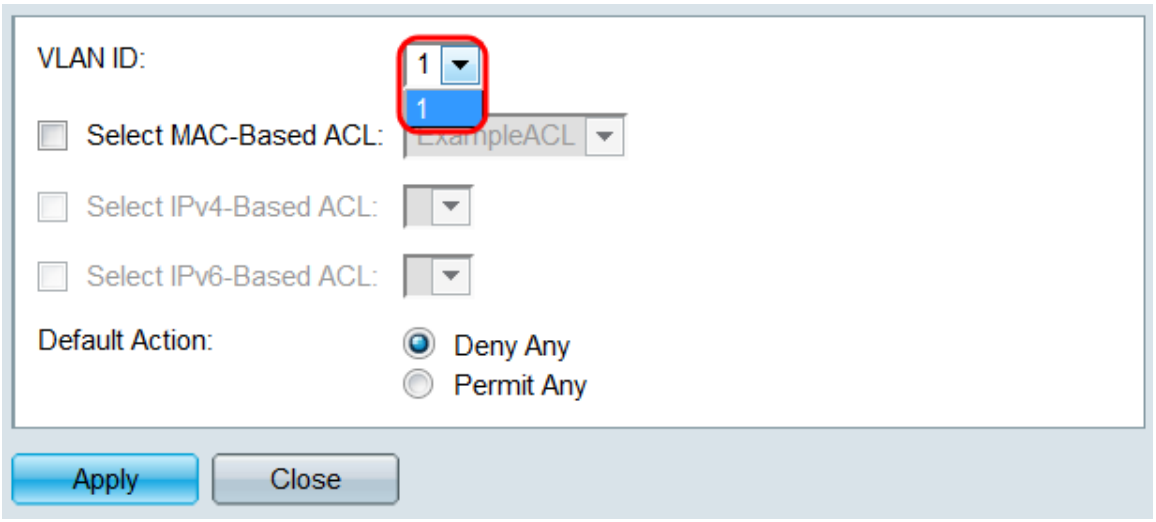
Stap 1. ACL kan aan of poorten of VLAN's worden toegewezen. Om een MAC-Based ACL aan een VLAN in kaart te brengen, navigeer naar **toegangscontrole > ACL-binding (VLAN)**. De *ACL*-pagina *(VLAN)* wordt geopend.



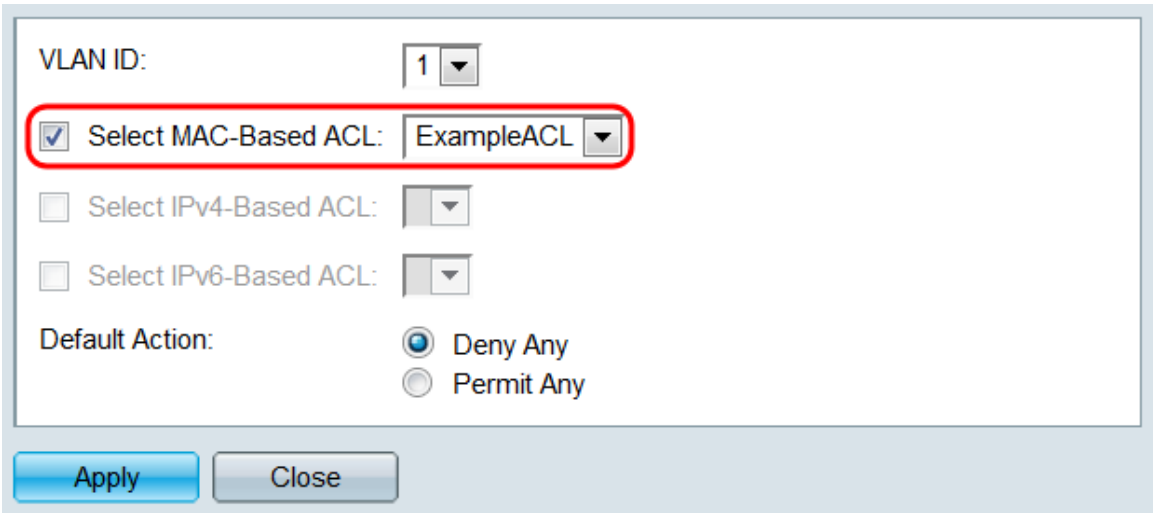
Stap 2. De *ACL-bindende tabel* toont alle ACL's die momenteel in kaart zijn gebracht in VLAN's. Als er geen ACL's zijn toegewezen, is de tabel leeg. Om ACL aan een VLAN in kaart te brengen, klik op de knop **Toevoegen...**. Het *venster ACL-binding toevoegen* wordt geopend.



Stap 3. Selecteer een VLAN om ACL in kaart te brengen om de vervolgkeuzelijst in het veld *VLAN-id te* gebruiken. Dit veld kan ook worden gebruikt om snel tussen verschillende VLAN's te switches zonder naar de *ACL*-pagina *(VLAN)* terug te keren.

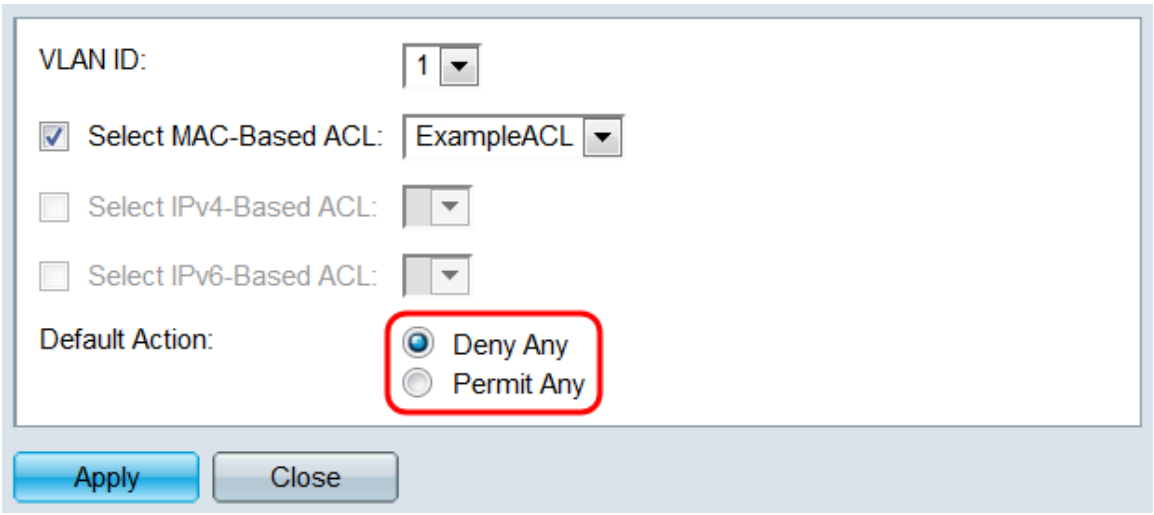


Stap 4. Controleer het selectieteken **MAC-Based ACL** en gebruik de vervolgkeuzelijst om ACL te selecteren om aan het gespecificeerde VLAN in kaart te brengen.

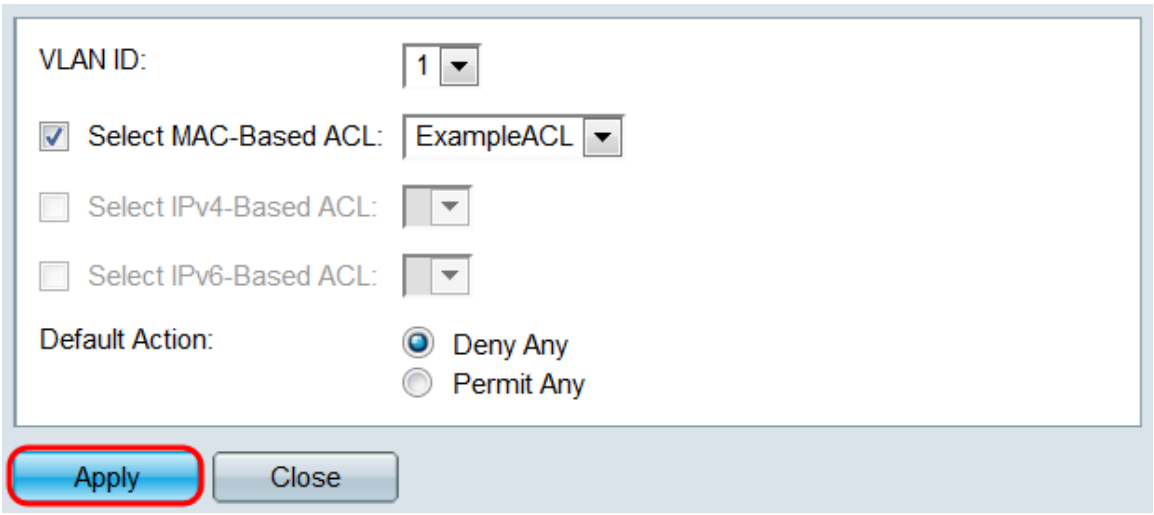


Opmerking: U kunt geen MAC-Based ACL binden die een VLAN-id als deel van zijn criteria aan een VLAN gebruikt. Bovendien kan ACL met een tijdbereik niet aan een VLAN worden gebonden.

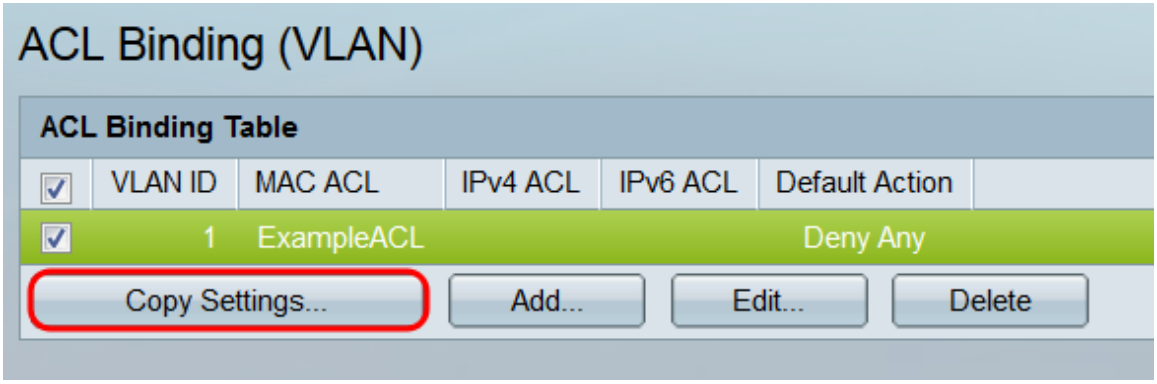
Stap 5. Selecteer in het veld *Default Action* een radioknop om te bepalen hoe pakketten die niet overeenkomen met de criteria van ACL worden verwerkt. De standaardinstelling is **Deny Any**, waardoor alle pakketten die niet aan de criteria van ACL beantwoorden, worden weggelaten; **Geef** toe dat **Any** andere pakketten worden verzonden.



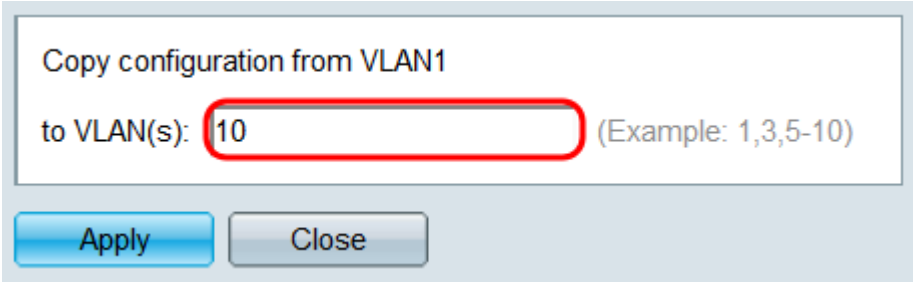
Stap 6. Klik op **Toepassen**. ACL wordt in kaart gebracht aan het gespecificeerde VLAN. U kunt het veld *VLAN-ID* gebruiken om een ander VLAN te selecteren dat u wilt configureren of op **Close** klikken om terug te keren naar de *ACL*-pagina (VLAN*)*.



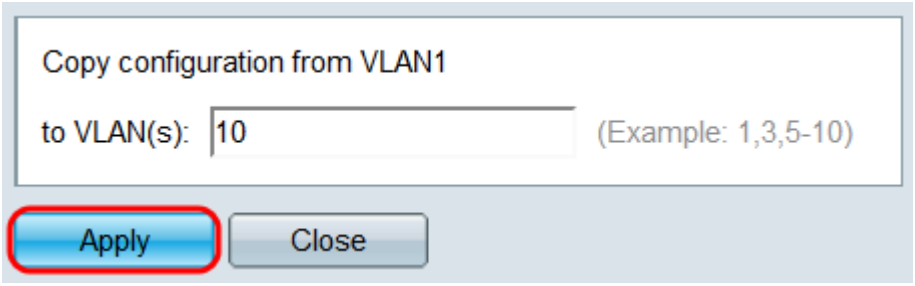
Stap 7. Als u de instellingen van een VLAN aan andere VLAN's snel wilt kopiëren, selecteert u het selectieteken van de VLAN-configuratie die u wilt kopiëren, en vervolgens klikt u op de knop **Kopieinstellingen...** Het venster *Instellingen kopiëren* wordt geopend.



Stap 8. Voer in het tekstveld de VLAN-id of VLAN-id's in waarop u instellingen wilt kopiëren. De ID's kunnen van elkaar worden gescheiden door komma's, of er kan een bereik worden opgegeven.



Stap 9. Klik op **Toepassen**. De instellingen worden gekopieerd.



Stap 10. Als u de instellingen van een VLAN wilt wissen, selecteert u het selectieteken van een VLAN en klikt u op **Verwijderen**. Merk op dat meerdere VLAN's tegelijkertijd kunnen worden geselecteerd en gewist.