

Add Access Control List (ACL) naar interfacebinding op SX500 Series Stackable-switches

Doel

Wanneer een toegangscontrolelijst (ACL) aan een interface is gebonden, worden zijn regels voor toegangscontrole over element (ACE) toegepast op pakketten die op die interface arriveren. Packets die niet overeenkomen met een van de ACE's in de toegangscontrolelijst worden aangepast aan een standaardregel waarvan de actie is om ongeëvenaarde pakketten te laten vallen. Hoewel elke interface alleen aan één ACL kan worden gebonden, kunnen meerdere interfaces aan dezelfde ACL worden gebonden als u ze in een beleidsplan groeperen en vervolgens de beleidskaart aan de interface binden. Nadat een toegangscontrolelijst aan een interface is gebonden, kan ACL niet worden bewerkt, gewijzigd of verwijderd totdat deze wordt verwijderd uit alle poorten waaraan deze is gebonden. Dit artikel legt uit hoe u een toegangscontrolelijst aan een interface bindt.

Als u niet bekend bent met termen in dit document, raadpleegt u [Cisco Business: Lijst van termen van nieuwe termen](#).

Opmerking: Raadpleeg de [configuratie](#) van de [Beleidsklasse \(QoS\) van artikel Quality of Service \(QoS\) op SX500 Series Stackable-switches](#) voor meer informatie over de configuratie van beleidskaarten.

Toepasselijke apparaten

- SX500 Series Stackable-switches

Softwareversie

- 1.3.0.62

ACL-naar-interfacebinding

Stap 1. Meld u aan bij het programma Web Configuration en kies **Access Control > ACL-binding**. De ACL-bindpagina wordt geopend:

ACL Binding

A port can be bound with either a [policy](#) or an ACL, but not both.
The default action is to discard (Deny Any) all the packets that do not meet the action of an ACL to forward those packets by configuring Permit Any on

ACL Binding Table

Filter: *Interface Type* equals to

| <input type="checkbox"/> | Entry No. | Interface | MAC | IPv6 ACL | Per |
|--------------------------|-----------|-----------|-------------------------|----------|-----|
| <input type="checkbox"/> | 1 | FE1 | Port of Unit 1/2 LAG | | |
| <input type="checkbox"/> | 2 | FE2 | | | |
| <input type="checkbox"/> | 3 | FE3 | | | |
| <input type="checkbox"/> | 4 | FE4 | | | |

Stap 2. Kies in het veld Filter het type interface waarop u de ACL wilt configureren in de vervolgkeuzelijst en klik op **Ga**. De mogelijke waarden zijn afzonderlijke poorten of een Link Aggregation Group (LAG).

ACL Binding

A port can be bound with either a [policy](#) or an ACL, but not both.
The default action is to discard (Deny Any) all the packets that do not meet the rules in an ACL.

ACL Binding Table

Filter: *Interface Type* equals to

| <input type="checkbox"/> | Entry No. | Interface | MAC ACL | IPv4 ACL | IPv6 ACL |
|-------------------------------------|-----------|-----------|---------|----------|----------|
| <input checked="" type="checkbox"/> | 1 | FE1 | | | |
| <input type="checkbox"/> | 2 | FE2 | | | |
| <input type="checkbox"/> | 3 | FE3 | | | |
| <input type="checkbox"/> | 4 | FE4 | | | |

Stap 3. Controleer het vakje naast de gewenste interface.

| | | | | | |
|--------------------------|----|------|--|--|--|
| <input type="checkbox"/> | 47 | FE47 | | | |
| <input type="checkbox"/> | 48 | FE48 | | | |
| <input type="checkbox"/> | 49 | GE3 | | | |
| <input type="checkbox"/> | 50 | GE4 | | | |

Stap 4. Klik op **Bewerken** om de configuratie te bewerken.

Interface: Unit/Slot LAG

Select MAC-Based ACL:

Select IPv4-Based ACL:

Select IPv6-Based ACL:

Stap 5. (Optioneel) Klik op de radioknop die overeenkomt met het gewenste interfacetype in het interfaceveld.

- Eenheid/sleuf — Kies in de vervolgkeuzelijst Eenheid/sleuf de juiste eenheid/sleuf. De eenheid identificeert of de schakelaar het actieve of lid in de stapel is. De sleuf identificeert welke switch is aangesloten op welke sleuf (sleuf 1 is SF500 en sleuf 2 is SG500).
- Poort — Kies in de vervolgkeuzelijst Poorten de juiste poort om te configureren.
- LAG — Kies de LAG in de vervolgkeuzelijst LAG. Een Link Aggregate Group (LAG) wordt gebruikt om meerdere poorten onderling te verbinden. LAGs vermenigvuldigt bandbreedte, verhoogt poortflexibiliteit, en verstrekt verbindingsredundantie tussen twee apparaten om poortgebruik te optimaliseren.

Stap 6. Controleer het/de aankruisvakje(s) naast de gewenste optie(s) voor binding:

- Selecteer MAC-gebaseerde ACL — Kies een MAC-gebaseerde ACL om aan de interface te worden gebonden. Raadpleeg het artikel [Configuration of MAC-gebaseerde ACL's en ACE's op Sx500 Series Stackable-switches](#) voor nadere informatie over de op MAC-gebaseerde ACL-configuratie.
- Selecteer IPv4 gebaseerde ACL — Kies een op IPv4 gebaseerde ACL om aan de interface te worden gebonden. Raadpleeg het artikel [Configuratie van IPv4-gebaseerde toegangscontrolelijsten \(ACL's\) en toegangscontrolelijsten \(ACE\) op SX500 Series Stackable-switches](#) voor meer informatie over de op IPv4 gebaseerde ACL-configuratie.
- Selecteer IPv6 gebaseerde ACL — Kies een op IPv6 gebaseerde ACL om aan de interface te worden gebonden. Raadpleeg het artikel [Configuratie van IPv6-gebaseerde toegangscontrolelijsten \(ACL's\) en toegangscontrolelijsten \(ACE\) op SX500 Series Stackable-switches](#) voor meer informatie over de op IPv6 gebaseerde ACL-configuratie.

Opmerking: IP-bronbewaking mag niet op de interface worden geactiveerd als er een definitie van de bronbewaking nodig is.

Stap 7. Als u hebt gekozen om MAC-gebaseerde ACL in Stap 6 te controleren, kiest u de ACL-interface waarop u de respectieve MAC-gebaseerde ACL-vervolgkeuzelijst wilt binden.

Interface: Unit/Slot 1/2 Port FE1 LAG 1

Select MAC-Based ACL: exampleMacACL

Select IPv4-Based ACL: exampleIPv4ACL

Select IPv6-Based ACL: exampleIPv6ACL

Permit Any: Disable(Deny Any) Enable

Apply Close

Stap 8. Als u hebt gekozen om op IPv4-gebaseerde ACL te controleren in Stap 6, kies ACL u aan de interface wilt binden van de respectieve vervolgkeuzelijst IPv4-gebaseerde ACL.

Stap 9. Als u ervoor hebt gekozen om IPv6-gebaseerde ACL te controleren in stap 6, kies ACL u de interface naar van de respectieve vervolgkeuzelijst IPv6-gebaseerde ACL wilt binden.

Opmerking: U kunt zowel een IPv4-gebaseerde ACL en een IPv6-gebaseerde ACL op dezelfde interface hebben. U kunt echter niet zowel een MAC-Based ACL als een IPv4 of IPv6-gebaseerde ACL op dezelfde interface hebben.

Stap 10. Klik op een van de volgende opties in het veld Vergunning:

- Uitschakelen (AnyDeny) — Packet wordt ontkend als dit niet overeenkomt met de ACL.
- Inschakelen — Packet wordt doorgestuurd zelfs als het niet overeenkomt met ACL.

Interface: Unit/Slot 1/2 Port FE1 LAG 1

Select MAC-Based ACL: exampleMacACL

Select IPv4-Based ACL: exampleIPv4ACL

Select IPv6-Based ACL: exampleIPv6ACL

Apply Close

Stap 1. Klik op **Toepassen**.