Hinzufügen einer Zugriffskontrollliste (ACL) zur Schnittstellenbindung auf Stackable Switches der Serie Sx500

Ziel

Wenn eine Zugriffssteuerungsliste (ACL) an eine Schnittstelle gebunden ist, werden die zugehörigen ACE-Regeln (Access Control Element) auf Pakete angewendet, die an dieser Schnittstelle eintreffen. Pakete, die keinem der ACEs in der Zugriffssteuerungsliste entsprechen, werden einer Standardregel zugeordnet, deren Aktion darin besteht, nicht übereinstimmende Pakete zu verwerfen. Obwohl jede Schnittstelle nur an eine ACL gebunden werden kann, können mehrere Schnittstellen an dieselbe ACL gebunden werden, wenn Sie sie in einer Richtlinienzuordnung gruppieren und die Richtlinienzuordnung dann an die Schnittstelle binden. Nachdem eine Zugriffssteuerungsliste an eine Schnittstelle gebunden wurde, kann die ACL nicht bearbeitet, geändert oder gelöscht werden, bis sie von allen Ports entfernt wird, an die sie gebunden ist. In diesem Artikel wird erläutert, wie eine Zugriffssteuerungsliste an eine Schnittstelle gebunden wird.

Wenn Sie die in diesem Dokument enthaltenen Begriffe nicht kennen, sehen Sie sich Cisco Business an: Glossar neuer Begriffe.

Hinweis: Weitere Informationen zur Konfiguration der Richtlinienzuweisung finden Sie im Artikel Quality of Service (QoS) Policy Class Maps Configuration on Sx500 Series Stackable Switches.

Anwendbare Geräte

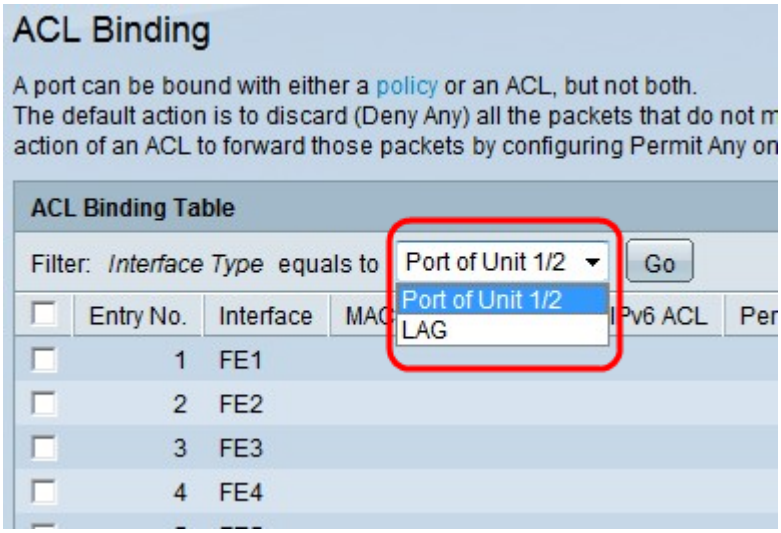
- Stackable Switches der Serie Sx500

Softwareversion

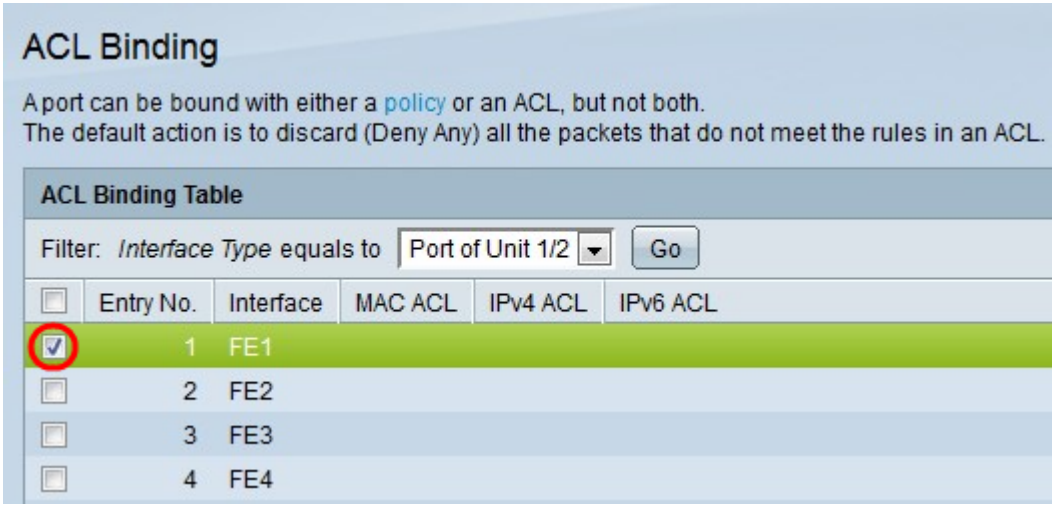
- 1,3 0,62

ACL an Schnittstellenbindung

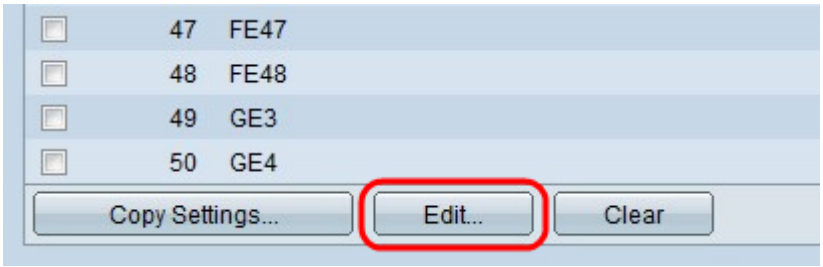
Schritt 1: Melden Sie sich beim Webkonfigurations-Dienstprogramm an, und wählen Sie **Zugriffskontrolle > ACL Binding aus**. Die Seite *ACL-Bindung* wird geöffnet:



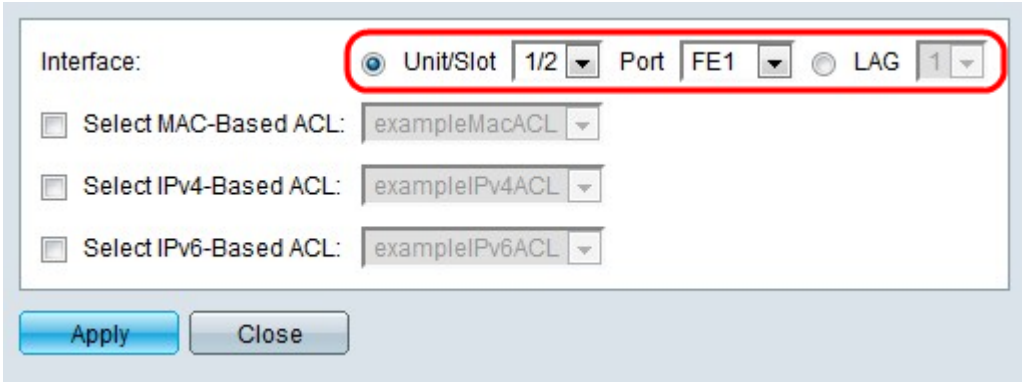
Schritt 2: Wählen Sie im Feld Filter (Filter) aus der Dropdown-Liste den Schnittstellentyp aus, auf dem die ACL konfiguriert werden soll, und klicken Sie auf **Go (Los)**. Mögliche Werte sind entweder einzelne Ports oder eine Link Aggregation Group (LAG).



Schritt 3: Aktivieren Sie das Kontrollkästchen neben der gewünschten Schnittstelle.

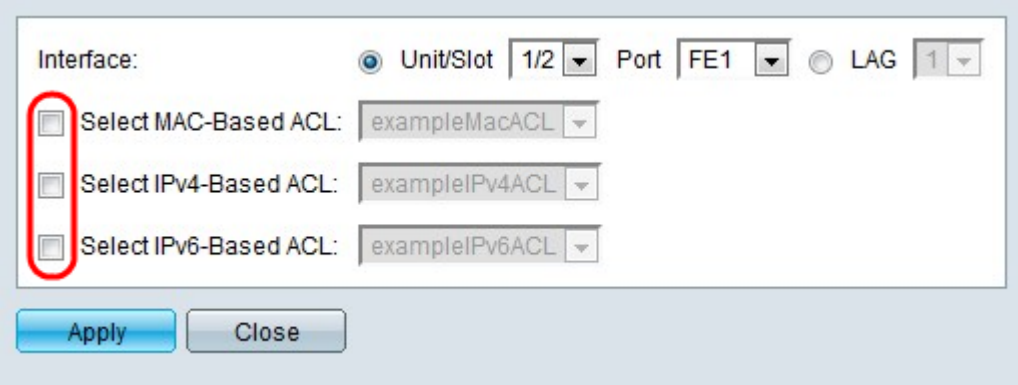


Schritt 4: Klicken Sie auf **Bearbeiten**, um die Konfiguration zu bearbeiten.



Schritt 5: (Optional) Klicken Sie im Feld Schnittstelle auf das Optionsfeld für den gewünschten Schnittstellentyp.

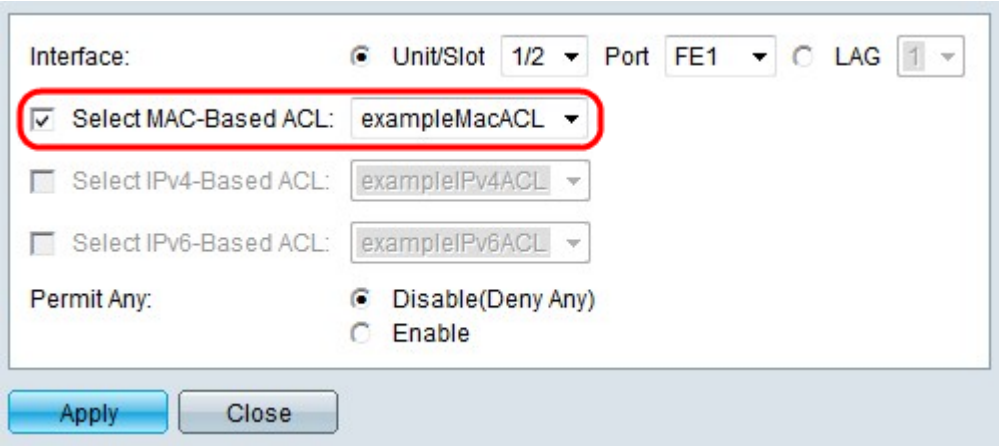
- Einheit/Steckplatz: Wählen Sie in der Dropdown-Liste "Einheit/Steckplatz" die entsprechende Einheit/den entsprechenden Steckplatz aus. Die Einheit identifiziert, ob der Switch der aktive Switch ist oder Mitglied im Stack ist. Der Steckplatz identifiziert, welcher Switch an welchen Steckplatz angeschlossen ist (Steckplatz 1 ist SF500 und Steckplatz 2 ist SG500).
- Port (Port): Wählen Sie aus der Dropdown-Liste "Port" (Port) den entsprechenden Port aus, den Sie konfigurieren möchten.
- LAG (LAG): Wählen Sie die LAG aus der Dropdown-Liste aus. Eine Link Aggregate Group (LAG) dient zum Verbinden mehrerer Ports. LAGs vervielfachen die Bandbreite, erhöhen die Portflexibilität und bieten Verbindungsredundanz zwischen zwei Geräten, um die Port-Nutzung zu optimieren.



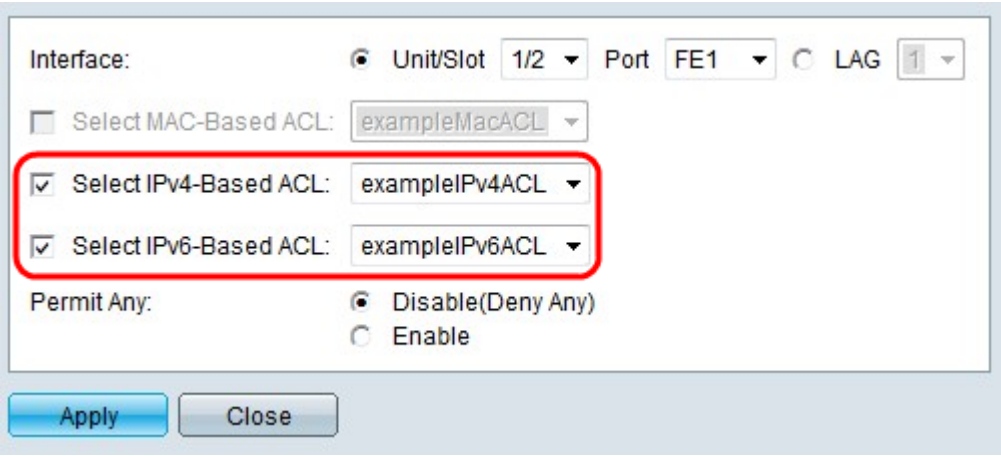
Schritt 6: Aktivieren Sie das bzw. die Kontrollkästchen neben den gewünschten Optionen für die Bindung:

- Wählen Sie MAC Based ACL (MAC-basierte ACL) aus. Wählen Sie eine MAC-basierte ACL aus, um an die Schnittstelle gebunden zu werden. Weitere Informationen zur MAC-basierten ACL-Konfiguration finden Sie im Artikel *Konfiguration von MAC-basierten ACLs und ACEs auf Stackable Switches der Serie Sx500*.
- Wählen Sie IPv4 Based ACL (IPv4-basierte ACL) aus. Wählen Sie eine IPv4-basierte ACL aus, die an die Schnittstelle gebunden werden soll. Weitere Informationen zur IPv4-basierten ACL-Konfiguration finden Sie im Artikel *Konfiguration von IPv4-basierten Zugriffskontrolllisten (ACL) und Zugriffskontrolleinträgen (ACE) auf stapelbaren Switches der Serie Sx500*.
- Wählen Sie IPv6 Based ACL (IPv6-basierte ACL) aus. Wählen Sie eine IPv6-basierte ACL aus, um an die Schnittstelle gebunden zu werden. Weitere Informationen zur IPv6-basierten ACL-Konfiguration finden Sie im Artikel *Konfiguration von IPv6-basierten Zugriffskontrolllisten (ACL) und Zugriffskontrolleinträgen (ACE) auf stapelbaren Switches der Serie Sx500*.

Hinweis: IP Source Guard sollte nicht auf der Schnittstelle aktiviert werden, wenn Permit Any (Beliebige Berechtigung) definiert werden muss.



Schritt 7: Wenn Sie in Schritt 6 *die* Option "Select MAC Based ACL" (MAC-basierte ACL auswählen*)* aktiviert haben, wählen Sie die ACL aus, an die die Schnittstelle gebunden werden soll, und wählen Sie diese aus der Dropdown-Liste MAC-Based-ACL aus.



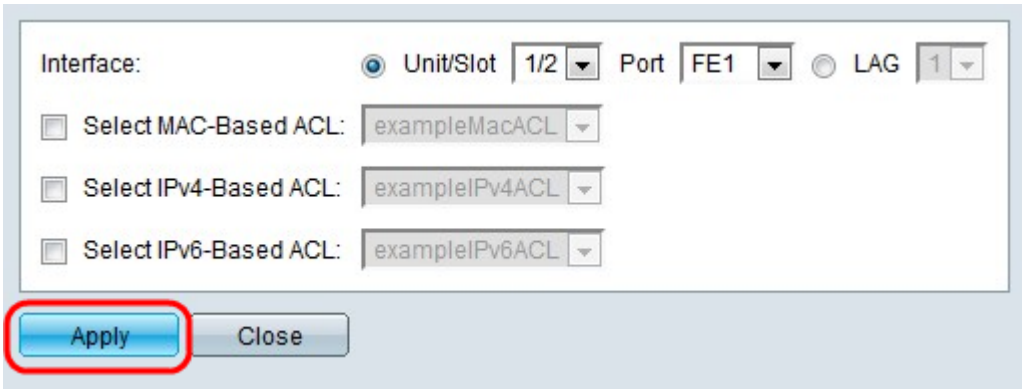
Schritt 8: Wenn Sie in Schritt 6 die Option Wählen Sie IPv4-basierte Zugriffskontrollliste aus, wählen Sie in der Dropdown-Liste IPv4-basierte Zugriffskontrolllisten die Zugriffskontrollliste aus, an die Sie die Schnittstelle binden möchten.

Schritt 9: Wenn Sie in Schritt 6 die Option Wählen Sie IPv6-basierte Zugriffskontrollliste *aus*, wählen Sie in der Dropdown-Liste IPv6-basierte Zugriffskontrolllisten die Zugriffskontrollliste aus, an die Sie die Schnittstelle binden möchten.

Hinweis: An derselben Schnittstelle können eine IPv4-basierte ACL und eine IPv6-basierte ACL-Bindung vorhanden sein. Es ist jedoch nicht möglich, eine MAC-basierte ACL und eine IPv4- oder IPv6-basierte ACL auf derselben Schnittstelle zu verwenden.

Schritt 10: Klicken Sie im Feld Zulassen auf eine der folgenden Optionen:

- Disable (Deaktivieren) (Any (Beliebig verweigern)): Das Paket wird abgelehnt, wenn es nicht mit der ACL übereinstimmt.
- Enable (Aktivieren): Das Paket wird weitergeleitet, auch wenn es nicht mit der ACL übereinstimmt.



Schritt 11: Klicken Sie auf **Übernehmen**.