

Bind Ingress oder Egress Access Control List (ACL) an einem Managed Switch

Ziel

Eine Zugriffskontrollliste (Access Control List, ACL) ist eine Liste von Filtern für den Netzwerkverkehr und zugehörigen Aktionen zur Verbesserung der Sicherheit. Sie blockiert oder ermöglicht Benutzern den Zugriff auf bestimmte Ressourcen. Eine ACL enthält die Hosts, denen der Zugriff auf das Netzwerkgerät gestattet oder verweigert wird.

ACLs können nicht nur auf Eingangs-, sondern auch auf Ausgangs-Schnittstellen angewendet werden. Der Zweck der Eingangs- (Eingangs-) und Ausgangs-ACL besteht darin, die Arten des Netzwerkverkehrs festzulegen, der vom Gerät im Netzwerk ein- oder ausgeht. Diese Funktion ermöglicht es Administratoren, den Datenverkehr im Netzwerk in das Internet oder die Unternehmens-Firewall zu filtern.

Dieser Artikel enthält Anweisungen zur Konfiguration und Bindung der Eingangs- und Ausgangs-ACLs auf Ihrem Switch.

Anwendbare Geräte

- Serie Sx350
- SG350X-Serie
- Serie Sx550X

Softwareversion

- 2,2 0,66

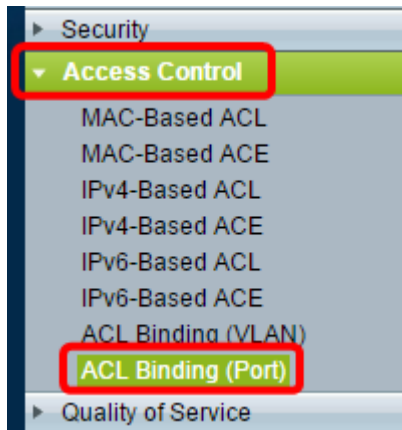
Konfigurieren der Eingangs- oder Ausgangs-ACL

Wichtig: Stellen Sie sicher, dass auf Ihrem Switch ACL und Access Control Entry (ACE) konfiguriert sind. Um IPv4-basierte ACL und ACE zu konfigurieren, klicken Sie [hier](#), um Anweisungen zu erhalten. Für IPv6-basiert, klicken Sie [hier](#). Klicken Sie [hier](#), um MAC-basierte ACL und ACE zu konfigurieren.

Konfigurieren der Eingangs-ACL auf einer Schnittstelle

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie dann **Zugriffskontrolle > ACL Binding (Port)**.

Hinweis: In diesem Szenario wird der Switch SG350-28MP verwendet.



Schritt 2: Aktivieren Sie das Kontrollkästchen neben der Schnittstelle, auf die die ACL angewendet werden soll, und klicken Sie dann auf **Bearbeiten**.

Hinweis: In diesem Beispiel wird die ACL auf die GE5-Schnittstelle angewendet.

ACL Binding Table

Filter: *Interface Type* equals to

<input type="checkbox"/>	Entry No.	Interface	Input ACL		
			MAC ACL	IPv4 ACL	IPv6 ACL
<input type="checkbox"/>	1	GE1			
<input type="checkbox"/>	2	GE2			
<input type="checkbox"/>	3	GE3			
<input type="checkbox"/>	4	GE4			
<input checked="" type="checkbox"/>	5	GE5			
<input type="checkbox"/>	6	GE6			
<input type="checkbox"/>	7	GE7			
<input type="checkbox"/>	8	GE8			
<input type="checkbox"/>	9	GE9			
<input type="checkbox"/>	10	GE10			
<input type="checkbox"/>	11	GE11			
<input type="checkbox"/>	12	GE12			
<input type="checkbox"/>	13	GE13			
<input type="checkbox"/>	14	GE14			
<input type="checkbox"/>	15	GE15			
<input type="checkbox"/>	16	GE16			
<input type="checkbox"/>	17	GE17			
<input type="checkbox"/>	18	GE18			
<input type="checkbox"/>	19	GE19			
<input type="checkbox"/>	20	GE20			
<input type="checkbox"/>	21	GE21			
<input type="checkbox"/>	22	GE22			
<input type="checkbox"/>	23	GE23			
<input type="checkbox"/>	24	GE24			
<input type="checkbox"/>	25	GE25			
<input type="checkbox"/>	26	GE26			
<input type="checkbox"/>	27	GE27			
<input type="checkbox"/>	28	GE28			

Schritt 3: Um die Eingangs-ACL für eine Schnittstelle zu konfigurieren, aktivieren Sie das Kontrollkästchen für die gewünschte Eingabe-ACL.

Hinweis: In diesem Beispiel wird die MAC-basierte Zugriffskontrollliste ausgewählt.

Interface: Port GE5 LAG 1

Input ACL

MAC-Based ACL: ACL1

IPv4-Based ACL: [dropdown]

IPv6-Based ACL: [dropdown]

Default Action: Deny Any Permit Any

Output ACL

MAC-Based ACL: ACL1

IPv4-Based ACL: [dropdown]

IPv6-Based ACL: [dropdown]

Default Action: Deny Any Permit Any

Apply Close

Hinweis: Wenn Sie eine IPv4- oder IPv6-basierte ACL binden möchten, klicken Sie auf die entsprechende Option.

Schritt 4: Wählen Sie eine ACL aus der entsprechenden Dropdown-Liste aus.

Hinweis: In diesem Beispiel wird die vorkonfigurierte MAC-basierte ACL ACL1 ausgewählt.

Interface: Port GE5 LAG 1

Input ACL

MAC-Based ACL: ACL1

IPv4-Based ACL:

IPv6-Based ACL:

Default Action: Deny Any Permit Any

Output ACL

MAC-Based ACL: ACL1

IPv4-Based ACL:

IPv6-Based ACL:

Default Action: Deny Any Permit Any

Apply Close

Schritt 5: Klicken Sie auf das Optionsfeld Standardaktion.

Interface: Port GE5 LAG 1

Input ACL

MAC-Based ACL: ACL1

IPv4-Based ACL:

IPv6-Based ACL:

Default Action: Deny Any Permit Any

Output ACL

MAC-Based ACL: ACL1

IPv4-Based ACL:

IPv6-Based ACL:

Default Action: Deny Any Permit Any

Apply Close

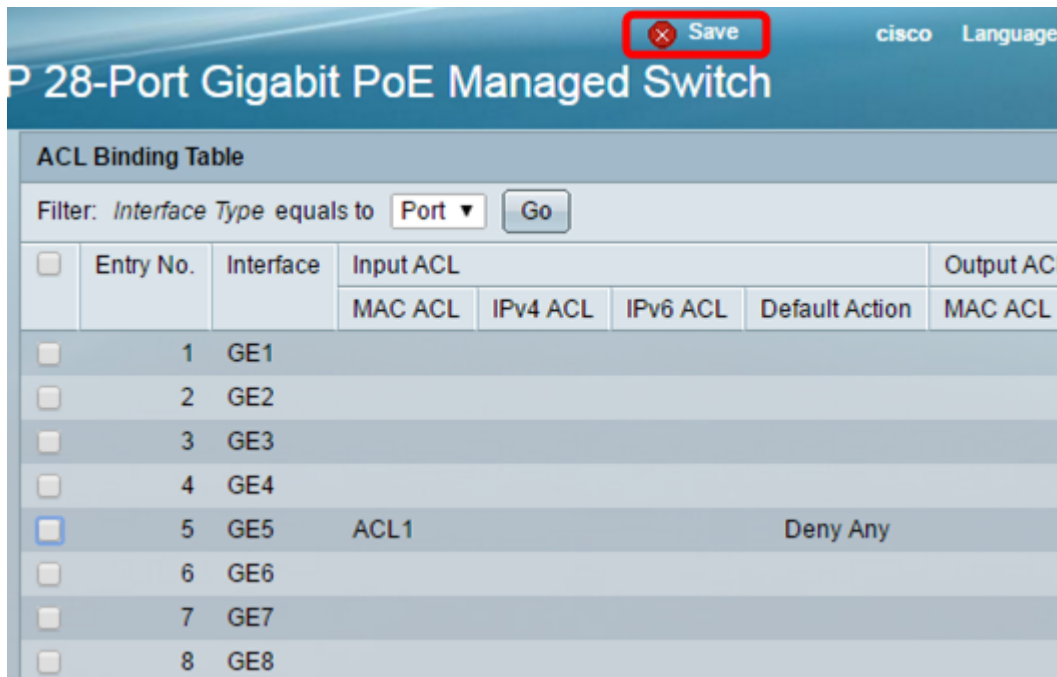
Folgende Optionen stehen zur Verfügung:

- Deny Any (Beliebig verweigern): Der Switch verwirft Pakete, die nicht die erforderlichen Kriterien der ACL erfüllen.
- Permit Any (Belassen): Der Switch leitet Pakete weiter, die die erforderlichen Kriterien der ACL erfüllen.

Schritt 6: Klicken Sie auf **Übernehmen**, um die Änderungen in der aktuellen

Konfigurationsdatei zu speichern, und klicken Sie dann auf **Schließen**.

Schritt 7: Die ACL-Bindungstabelle sollte die konfigurierte ACL auf der ausgewählten Schnittstelle anzeigen. Klicken Sie auf **Speichern**, um die Startkonfigurationsdatei zu aktualisieren.



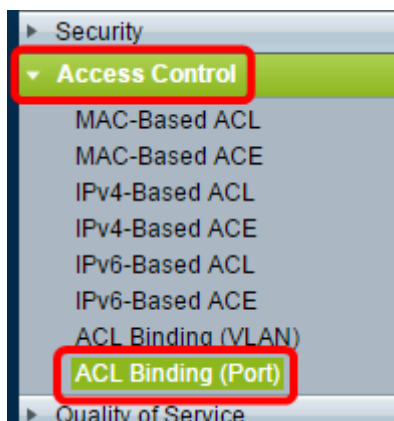
<input type="checkbox"/>	Entry No.	Interface	Input ACL				Output ACL
			MAC ACL	IPv4 ACL	IPv6 ACL	Default Action	MAC ACL
<input type="checkbox"/>	1	GE1					
<input type="checkbox"/>	2	GE2					
<input type="checkbox"/>	3	GE3					
<input type="checkbox"/>	4	GE4					
<input checked="" type="checkbox"/>	5	GE5	ACL1			Deny Any	
<input type="checkbox"/>	6	GE6					
<input type="checkbox"/>	7	GE7					
<input type="checkbox"/>	8	GE8					

Konfigurieren der Eingangs-ACL auf einer Schnittstelle

Wichtig: Bevor Sie mit den Schritten fortfahren, stellen Sie sicher, dass Sie bereits eine MAC-basierte Zugriffskontrollliste (ACL) und einen Zugriffskontrolleintrag (ACE) auf Ihrem Switch erstellt haben. Klicken Sie hier, um detaillierte Anweisungen zu erhalten.

Schritt 1: Wählen Sie im webbasierten Dienstprogramm **Access Control > ACL Binding (Port)** aus.

Hinweis: In diesem Szenario wird der Switch SG350-28MP verwendet.



Schritt 2: Aktivieren Sie das Kontrollkästchen neben der Schnittstelle, auf die die ACL angewendet werden soll, und klicken Sie dann auf **Bearbeiten**.

Hinweis: In diesem Beispiel wird GE6 gewählt.

ACL Binding Table

Filter: *Interface Type* equals to

<input type="checkbox"/>	Entry No.	Interface	Input ACL		
			MAC ACL	IPv4 ACL	IPv6 ACL
<input type="checkbox"/>	1	GE1			
<input type="checkbox"/>	2	GE2			
<input type="checkbox"/>	3	GE3			
<input type="checkbox"/>	4	GE4			
<input type="checkbox"/>	5	GE5			
<input checked="" type="checkbox"/>	6	GE6			
<input type="checkbox"/>	7	GE7			
<input type="checkbox"/>	8	GE8			
<input type="checkbox"/>	9	GE9			
<input type="checkbox"/>	10	GE10			
<input type="checkbox"/>	11	GE11			
<input type="checkbox"/>	12	GE12			
<input type="checkbox"/>	13	GE13			
<input type="checkbox"/>	14	GE14			
<input type="checkbox"/>	15	GE15			
<input type="checkbox"/>	16	GE16			
<input type="checkbox"/>	17	GE17			
<input type="checkbox"/>	18	GE18			
<input type="checkbox"/>	19	GE19			
<input type="checkbox"/>	20	GE20			
<input type="checkbox"/>	21	GE21			
<input type="checkbox"/>	22	GE22			
<input type="checkbox"/>	23	GE23			
<input type="checkbox"/>	24	GE24			
<input type="checkbox"/>	25	GE25			
<input type="checkbox"/>	26	GE26			
<input type="checkbox"/>	27	GE27			
<input type="checkbox"/>	28	GE28			

Copy Settings...

Edit...

Clear

Schritt 3: Um die Eingangs-ACL für eine Schnittstelle zu konfigurieren, aktivieren Sie das Kontrollkästchen für die gewünschte Ausgabe-ACL.

Hinweis: In diesem Beispiel wird die MAC-basierte Zugriffskontrollliste ausgewählt.

Interface: Port GE5 LAG 1

Input ACL

MAC-Based ACL: ACL1

IPv4-Based ACL: [Dropdown]

IPv6-Based ACL: [Dropdown]

Default Action: Deny Any Permit Any

Output ACL

MAC-Based ACL: ACL2

IPv4-Based ACL: [Dropdown]

IPv6-Based ACL: [Dropdown]

Default Action: Deny Any Permit Any

Apply Close

Hinweis: Wenn Sie eine IPv4- oder IPv6-basierte ACL binden möchten, klicken Sie auf die entsprechende Option.

Schritt 4: Wählen Sie eine ACL aus der Dropdown-Liste MAC-Based ACL (MAC-basierte ACL) aus.

Hinweis: In diesem Beispiel wird die vorkonfigurierte MAC-basierte ACL ACL2 ausgewählt.

Interface: Port GE6 LAG 1

Input ACL

MAC-Based ACL: ACL1

IPv4-Based ACL: [Dropdown]

Default Action: Deny Any Permit Any

Output ACL

MAC-Based ACL: ACL2

IPv4-Based ACL: [Dropdown]

Default Action: Deny Any Permit Any

Apply Close

Schritt 5: Klicken Sie auf das Optionsfeld Standardaktion.

Folgende Optionen stehen zur Verfügung:

- Deny Any (Beliebig verweigern): Der Switch verwirft Pakete, die nicht die erforderlichen Kriterien der ACL erfüllen.
- Permit Any (Belassen): Der Switch leitet Pakete weiter, die die erforderlichen Kriterien der ACL erfüllen.

Schritt 6: Klicken Sie auf **Übernehmen**, um die Änderungen in der aktuellen Konfigurationsdatei zu speichern, und klicken Sie dann auf **Schließen**.

Schritt 7: Die ACL-Bindungstabelle sollte die konfigurierte ACL auf der ausgewählten Schnittstelle anzeigen. Klicken Sie auf **Speichern**, um die Startkonfigurationsdatei zu aktualisieren.

No.	Interface	Input ACL				Output ACL			
		MAC ACL	IPv4 ACL	IPv6 ACL	Default Action	MAC ACL	IPv4 ACL	IPv6 ACL	Default Action
1	GE1								
2	GE2								
3	GE3								
4	GE4								
5	GE5	ACL1			Deny Any				
6	GE6					ACL2			Permit Any
7	GE7								
8	GE8								

Hinweis: Wenn Sie die Eingangs- und Ausgangszugriffskontrolllisten gleichzeitig

konfigurieren möchten, konfigurieren Sie dazu sowohl die Eingangs-ACL- als auch die Ausgangszugriffskontrollbereiche.

Sie sollten jetzt die Eingangs- und Ausgangs-ACLs an den Schnittstellen Ihres Switches konfiguriert haben.