

Aggiunta di Access Control List (ACL) all'associazione dell'interfaccia sugli switch serie Sx500 impilabili

Obiettivo

Quando un elenco di controllo di accesso (ACL) è associato a un'interfaccia, le relative regole ACE (Access Control Element) vengono applicate ai pacchetti che arrivano all'interfaccia. I pacchetti che non corrispondono a nessuna delle voci ACE nell'elenco di controllo di accesso vengono associati a una regola predefinita che prevede l'eliminazione dei pacchetti non corrispondenti. Anche se ogni interfaccia può essere associata a un solo ACL, è possibile associare più interfacce allo stesso ACL se le si raggruppa in una mappa dei criteri e quindi si associa la mappa dei criteri all'interfaccia. Dopo aver associato un elenco di controllo di accesso a un'interfaccia, non è possibile modificare, modificare o eliminare l'ACL finché non viene rimosso da tutte le porte a cui è associato. In questo articolo viene illustrato come associare un elenco di controllo di accesso a un'interfaccia.

Se non conosci i termini di questo documento, controlla [Cisco Business: glossario dei nuovi termini](#).

Nota: Per ulteriori dettagli sulla configurazione delle [mappe policy](#), consultare l'articolo [Configurazione delle mappe delle classi di policy QoS sugli switch impilabili serie Sx500](#).

Dispositivi interessati

- Serie Sx500 Stackable Switch

Versione del software

- 1.3.0.62

Associazione ACL a interfaccia

Passaggio 1. Accedere all'utility Configurazione Web e scegliere **Controllo di accesso > Associazione ACL**. Viene visualizzata la pagina *Binding ACL*:

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.
The default action of an ACL to forward those packets by configuring Permit Any on the interface.

ACL Binding Table

Filter: *Interface Type* equals to

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

Passaggio 2. Nel campo Filter (Filtro), scegliere il tipo di interfaccia su cui configurare l'ACL dall'elenco a discesa e fare clic su **Go** (Vai). I valori possibili sono singole porte o un gruppo di aggregazione link (LAG, Link Aggregation Group).

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			

Passaggio 3. Selezionare la casella di controllo accanto all'interfaccia desiderata.

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

Passaggio 4. Fare clic su **Modifica** per modificare la configurazione.

Interface: Unit/Slot LAG

Select MAC-Based ACL:

Select IPv4-Based ACL:

Select IPv6-Based ACL:

Passaggio 5. (Facoltativo) Fare clic sul pulsante di opzione corrispondente al tipo di interfaccia desiderato nel campo Interfaccia.

- Unità/Slot: dall'elenco a discesa Unità/Slot, scegliere l'Unità/Slot appropriato. L'unità identifica se lo switch è il membro attivo o attivo nello stack. Lo slot identifica lo switch collegato a quale slot (lo slot 1 è SF500 e lo slot 2 è SG500).
- Porta: dall'elenco a discesa Porta, scegliere la porta appropriata da configurare.
- LAG — scegliere il LAG dall'elenco a discesa LAG. Un LAG (Link Aggregate Group) viene utilizzato per collegare più porte. I LAG moltiplicano la larghezza di banda, aumentano la flessibilità delle porte e forniscono la ridondanza dei collegamenti tra due dispositivi per ottimizzare l'utilizzo delle porte.

Passaggio 6. Selezionare le caselle di controllo accanto alle opzioni desiderate per il binding:

- Select MAC Based ACL - Consente di scegliere un ACL basato su MAC da associare all'interfaccia. Per ulteriori informazioni sulla configurazione degli ACL basati sull'indirizzo MAC, consultare l'articolo [Configurazione degli ACL e delle ACE basati su MAC sugli switch impilabili serie Sx500](#).
- Select IPv4 Based ACL: per selezionare un ACL basato su IPv4 da associare all'interfaccia. Per ulteriori informazioni sulla configurazione degli ACL basati su IPv4, consultare l'articolo [Configurazione degli Access Control Lists \(ACL\) e delle Access Control Entries \(ACE\) basati su IPv4 sugli switch impilabili serie Sx500](#).
- Seleziona ACL basato su IPv6: scegliere un ACL basato su IPv6 da associare all'interfaccia. Per ulteriori informazioni sulla configurazione degli ACL basati su IPv6, consultare l'articolo [Configuration of IPv6-Based Access Control Lists \(ACL\) and Access Control Entries \(ACE\) on Sx500 Series Stackable Switch](#).

Nota: IP Source Guard non deve essere attivato sull'interfaccia se occorre definire Permit Any.

Passaggio 7. Se si sceglie di selezionare Select MAC Based ACL (Seleziona ACL basati su MAC) nel passaggio 6, selezionare l'ACL a cui si desidera associare l'interfaccia dall'elenco a discesa degli ACL basati su MAC corrispondenti.

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

Passaggio 8. Se si sceglie di selezionare Select IPv4-Based ACL nel passaggio 6, selezionare l'ACL a cui si desidera associare l'interfaccia dall'elenco a discesa dei rispettivi ACL IPv4.

Passaggio 9. Se si sceglie di selezionare Seleziona ACL basato su IPv6 nel passaggio 6, scegliere l'ACL a cui si desidera associare l'interfaccia dal rispettivo elenco a discesa ACL basato su IPv6.

Nota: È possibile avere un ACL basato su IPv4 e un binding di ACL basato su IPv6 sulla stessa interfaccia. Tuttavia, non è possibile avere sia un ACL basato su MAC che un ACL basato su IPv4 o IPv6 sulla stessa interfaccia.

Passaggio 10. Fare clic su una delle opzioni seguenti nel campo Autorizza qualsiasi:

- Disable (Deny Any): il pacchetto viene rifiutato se non corrisponde all'ACL.
- Enable: il pacchetto viene inoltrato anche se non corrisponde all'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

Passaggio 11. Fare clic su **Applica**.