

Associazione di ACL (Access Control List) a un'interfaccia sugli switch gestiti serie 200/300

Obiettivo

Un elenco di controllo di accesso (ACL, Access Control List) è un elenco di filtri del traffico di rete e di azioni correlate utilizzato per migliorare la sicurezza. Gli ACL possono essere definiti in tre modi: tramite indirizzo MAC, indirizzo IPv4 o indirizzo IPv6. Quando un ACL è associato a un'interfaccia, i pacchetti che arrivano a quell'interfaccia vengono confrontati con l'ACL e quindi autorizzati o scartati. Tuttavia, è possibile associare un solo ACL per interfaccia.

Questo documento spiega come associare gli ACL a un'interfaccia sugli switch gestiti serie 200 e 300.

Dispositivi interessati

- Switch gestiti serie SF/SG200 e SF/SG300

Versione del software

- 1.3.0.62

Associa elenco di controllo di accesso a un'interfaccia

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

ACL Binding

A port can be bound with either a [policy](#) or an ACL, but not both.

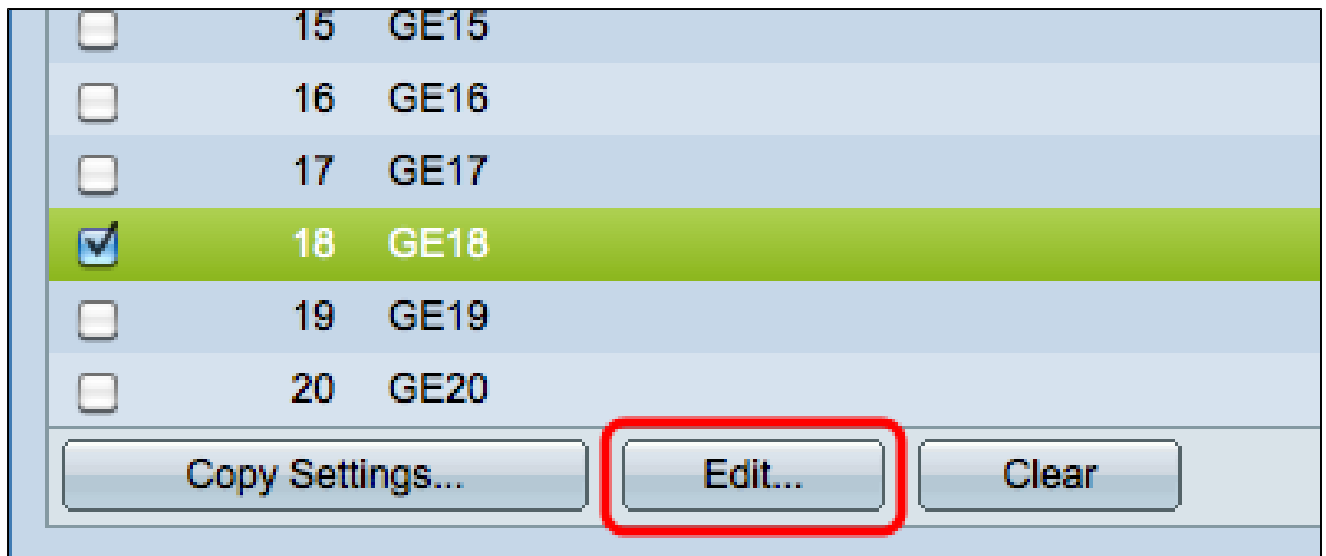
The default action is to discard (Deny Any) all the packets that do not meet the rules in the ACL. To change the default action of an ACL to forward those packets by configuring Permit Any on the desired port.

ACL Binding Table						
Filter: <i>Interface Type</i> equals to Port ▾ Go						
<input type="checkbox"/>	Entry No.	Interface	MAC ACL	IPv4 ACL	IPv6 ACL	Permit Any
<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 type="checkbox"/>	6	GE6				
<input type="checkbox"/>	7	GE7				

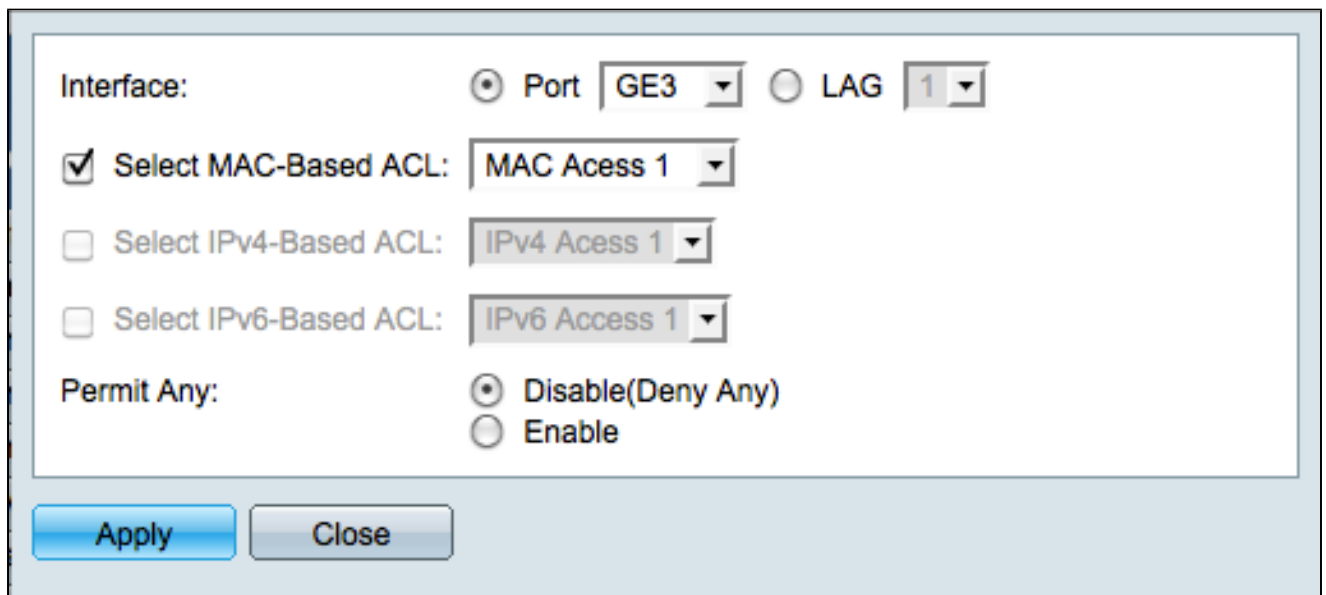
Passaggio 2. Selezionare un'interfaccia dall'elenco a discesa Interface Type (Tipo interfaccia) e fare clic su Go (Vai).

- Porta: una singola porta fisica sullo switch.
- LAG: gruppo di porte utilizzate per aumentare l'affidabilità del collegamento.

Passaggio 3. Selezionare la casella di controllo relativa alla porta o al LAG desiderato e fare clic su Modifica.



Viene visualizzata la finestra Modifica associazione ACL.



Passaggio 4. Selezionare la casella di controllo del tipo di ACL che si desidera associare all'interfaccia scelta e scegliere l'ACL dall'elenco a discesa.

- ACL basato su MAC: filtra il traffico in base ai campi di layer 2 dell'intestazione del frame.
- ACL basato su IPv4: filtra il traffico in base ai pacchetti IPv4.
- ACL basato su IPv6: filtra il traffico in base ai pacchetti IPv6.

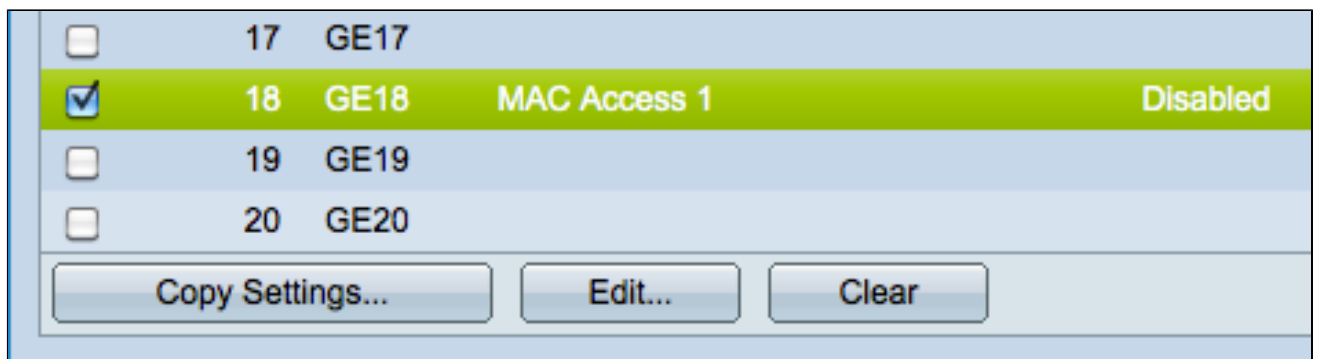
Nota: la casella di controllo di una delle opzioni dell'ACL viene evidenziata solo se è disponibile un ACL in quel formato.

Passaggio 5. Selezionare il pulsante di opzione appropriato nel campo Permit Any (Autorizza qualsiasi) per definire l'operazione da eseguire sui pacchetti che non corrispondono all'ACL scelto.

- Disable (Deny Any) (Disabilita (Deny Any) - I pacchetti vengono scartati (negati) se non corrispondono a un ACL.
- Enable: i pacchetti vengono inoltrati anche se non corrispondono a un ACL.

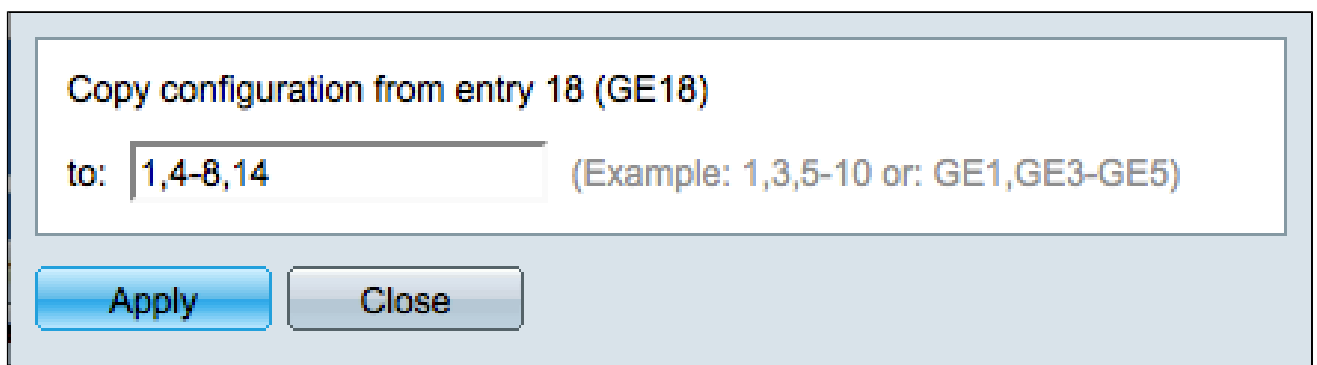
Passaggio 6. Fare clic su Apply (Applica) per associare l'ACL scelto all'interfaccia. La finestra Modifica associazione ACL si chiude.

Passaggio 7. (Facoltativo) Selezionare la casella di controllo dell'interfaccia desiderata e fare clic su Cancella per annullare il binding dell'interfaccia dall'ACL.



Passaggio 8. (Facoltativo) Selezionare la casella di controllo dell'interfaccia desiderata e fare clic su Copia impostazioni per copiare le impostazioni dell'interfaccia su altre interfacce.

Viene visualizzata la finestra Copy Settings:



Passaggio 9. Immettere i numeri o i nomi delle porte su cui copiare le impostazioni della porta scelta.

Passaggio 10. Fare clic su Apply (Applica) per applicare le impostazioni oppure su Close (Chiudi) per annullarle.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).