

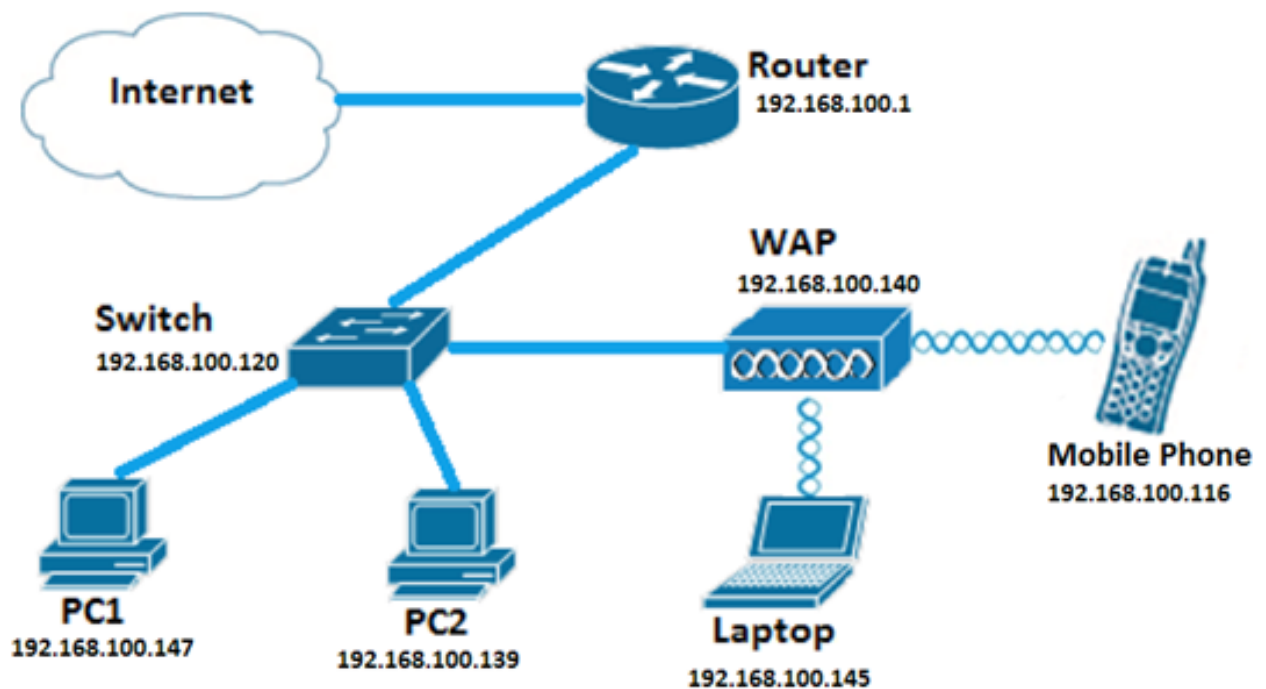
Configurare gli ACL IPv4 sui modelli WAP125 e WAP581

Introduzione

Gli elenchi di controllo di accesso (ACL, Access Control List) IP versione 4 (IPv4) e IPv6 (Internet Protocol versione 6) sono un insieme di regole applicate ai pacchetti ricevuti dal punto di accesso wireless (WAP, Wireless Access Point). Ogni regola viene utilizzata per determinare se consentire o negare l'accesso alla rete. Gli ACL possono essere configurati per ispezionare i campi di un frame, ad esempio l'indirizzo IP di origine o di destinazione, l'ID (Virtual Local Area Network) o la classe di servizio (CoS). Quando un frame entra nella porta del dispositivo WAP, controlla il frame e confronta le regole ACL con il contenuto del frame. Se una delle regole corrisponde al contenuto, viene eseguita un'azione di autorizzazione o rifiuto sul frame.

La configurazione degli ACL IPv4 viene in genere utilizzata per autorizzare l'accesso alle risorse di rete per selezionare i dispositivi della rete.

Nota: Alla fine di ogni regola creata è presente un rifiuto implicito.



Nota: In questo scenario, tutto il traffico proveniente da PC2 sarà autorizzato ad accedere alla rete. Tutto il traffico proveniente da altri host verrà rifiutato.

Obiettivo

In questo documento viene spiegato come configurare un ACL IPv4 su un access point WAP125 e WAP581.

Dispositivi interessati

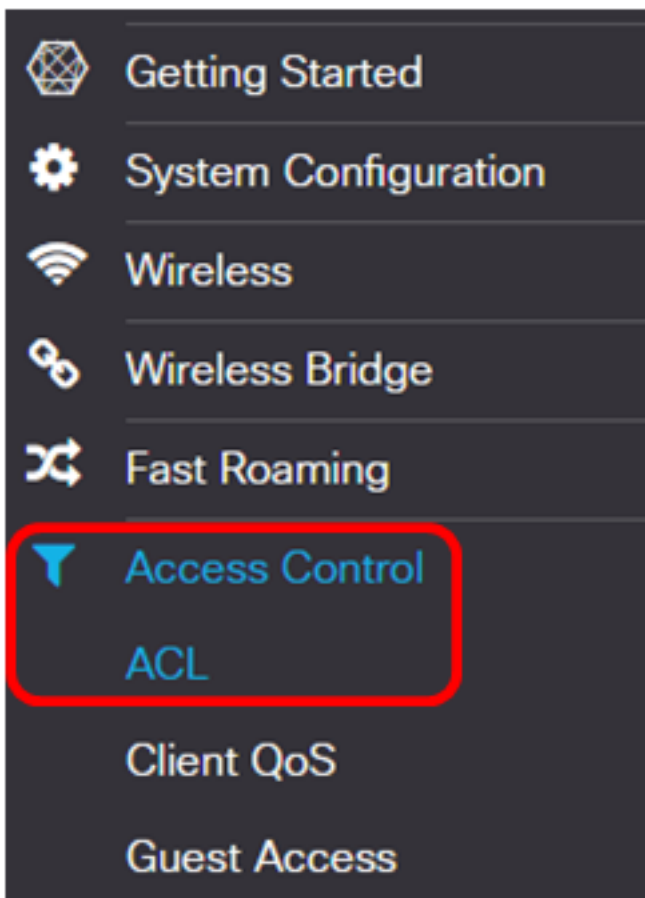
- WAP125
- WAP581

Versione del software

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

Configurazione di un ACL IPv4

Passaggio 1. Accedere all'utility basata sul Web di WAP e scegliere **Controllo accesso > ACL**.

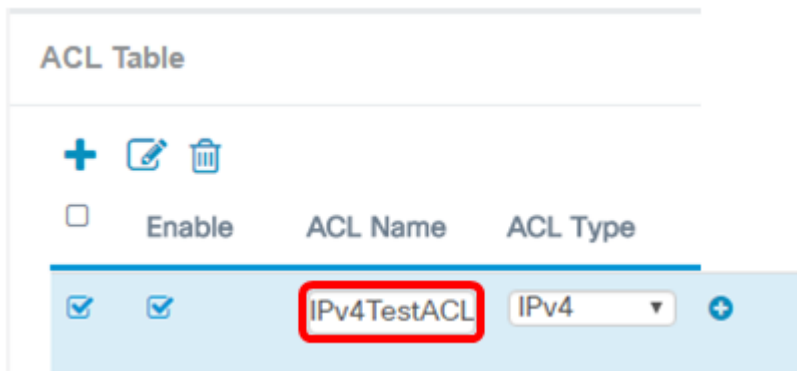


Passaggio 2. Fare clic sul **+** pulsante per creare un nuovo ACL.

ACL Table

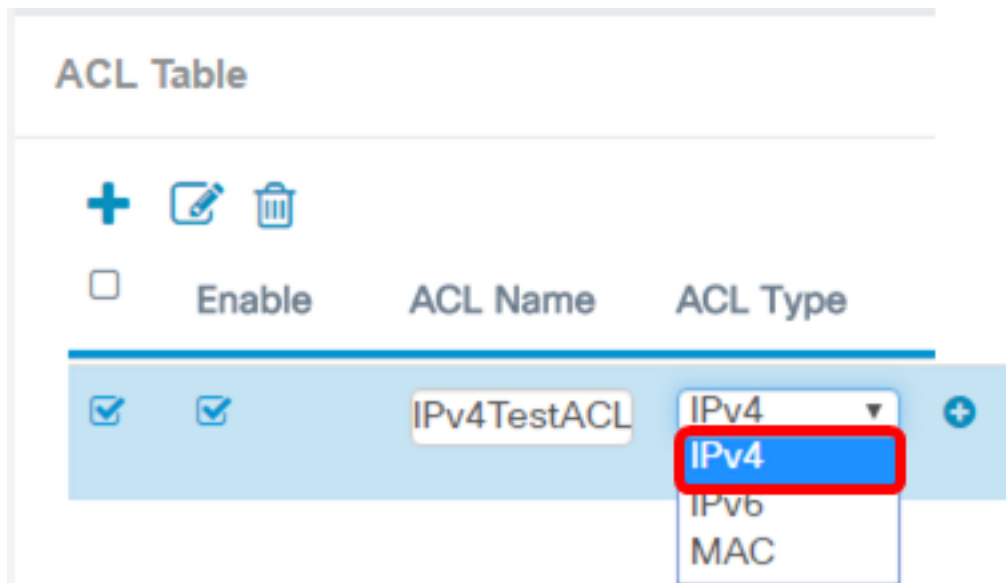



Passaggio 3. Inserire un nome per l'ACL nel campo *Nome ACL*.



Nota: Nell'esempio, viene immesso IPv4TestACL.

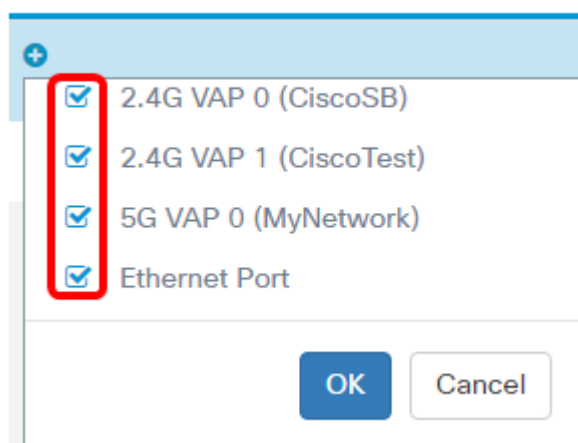
Passaggio 4. Selezionare IPv4 dall'elenco a discesa Tipo di ACL.



Passaggio 5. Fare clic sul  pulsante e scegliere un'interfaccia dall'elenco a discesa Interfaccia associata. Le opzioni sono:

- 2.4G VAP 0 (nome SSID): questa opzione applica l'ACL MAC al VAP (Virtual Access Point) a 2,4 GHz. La sezione Nome SSID può variare a seconda del nome SSID configurato nel punto di accesso WAP.
- 5G VAP0 (nome SSID) - Questa opzione applica l'ACL MAC al VAP da 5 GHz.
- Ethernet Port: questa opzione applica l'ACL MAC all'interfaccia Ethernet del WAP.

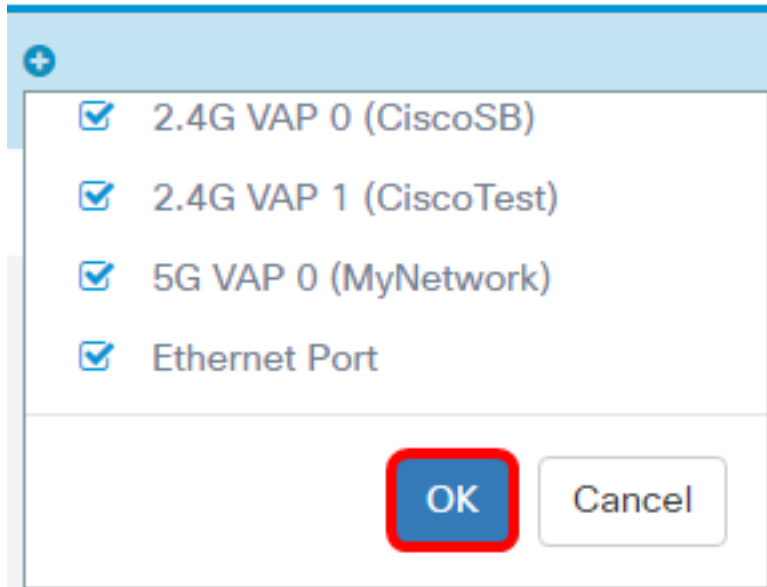
Associated Interface



Nota: Ad un ACL possono essere associate più interfacce. Tuttavia, non può essere associato a un ACL se è già stato associato a un altro ACL. Nell'esempio, tutte le interfacce sono associate a IPv4TestACL. Deselezionare la casella per dissociare l'interfaccia dall'ACL.

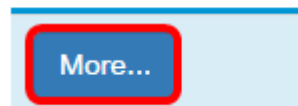
Passaggio 6. Fare clic su **OK**.

Associated Interface



Passaggio 7. Fare clic sul pulsante **More...** per configurare i parametri dell'ACL.

Details Of Rule(s)

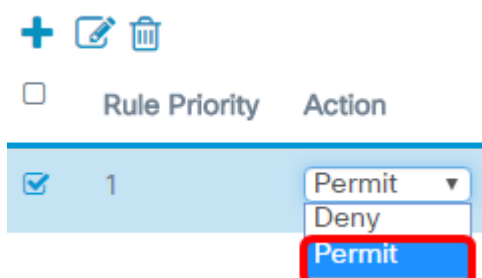


Passaggio 8. Fare clic sul **+** pulsante per aggiungere una nuova regola.



Passaggio 9. Scegliere un'azione dall'elenco a discesa Azione. Le opzioni sono:

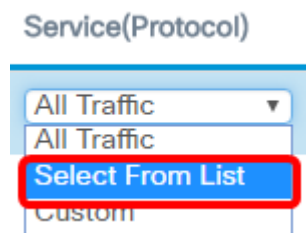
- Permit: questa opzione consente la connessione alla rete dei pacchetti che soddisfano i criteri ACL.
- Nega — questa opzione impedisce ai pacchetti che soddisfano i criteri ACL di connettersi alla rete.



Nota: Nell'esempio riportato di seguito, viene selezionato Permit.

Passaggio 10. Scegliere un servizio o un protocollo da filtrare dall'elenco a discesa Servizio (protocollo). Le opzioni sono:

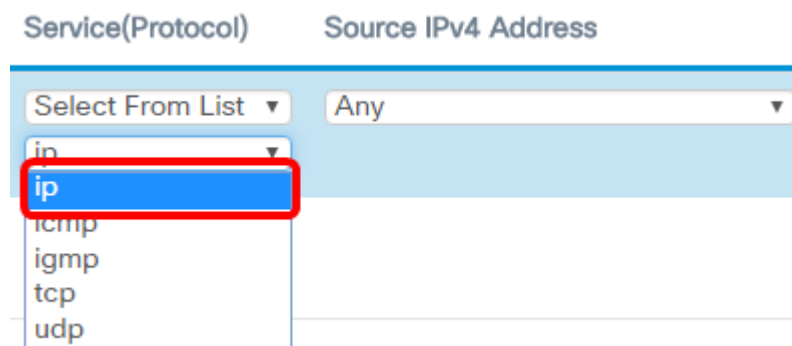
- All Traffic: questa opzione considera tutti i pacchetti come una corrispondenza con il filtro ACL.
- Select From List: questa opzione permette di scegliere IP, ICMP, IGMP, TCP o UDP come filtri per l'ACL. Se si sceglie questa opzione, andare al passo 11.
- Personalizzato — questa opzione consente di immettere un identificativo di protocollo personalizzato come filtro per i pacchetti. Il valore è un numero esadecimale a quattro cifre. L'intervallo è compreso tra 0 e 255.



Nota: In questo esempio, viene scelto Seleziona da elenco.

Passaggio 11. Definire il protocollo che deve essere autorizzato a connettersi alla rete. Le opzioni sono:

- ip - questa opzione consente al punto di accesso di filtrare gli host che accedono alla rete utilizzando il loro indirizzo IP come filtro.
- icmp — Questa opzione consente al punto di accesso di filtrare i pacchetti ICMP (Internet Control Message Protocol) che entrano nella rete attraverso il punto di accesso.
- igmp — questa opzione consente al punto di accesso di filtrare i pacchetti IGMP (Internet Group Management Protocol) che entrano nella rete attraverso il punto di accesso.
- tcp — questa opzione consente ai pacchetti TCP (Transmission Control Protocol) del filtro del punto di accesso di entrare nella rete attraverso il punto di accesso.
- udp: questa opzione consente al punto di accesso di filtrare i pacchetti UDP (User Datagram Protocol) che entrano nella rete attraverso il punto di accesso.



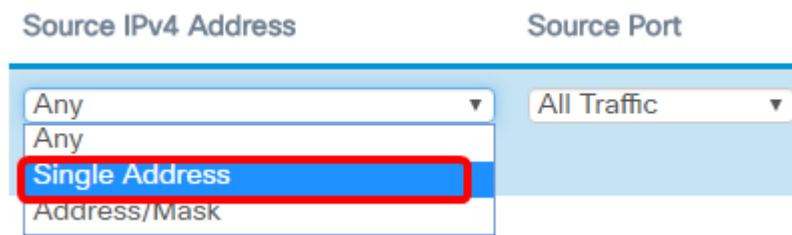
Nota: nell'esempio, viene scelto ip.

Passaggio 12. Definire l'indirizzo IPv4 di origine dall'elenco a discesa Indirizzo IPv4 di origine. Le opzioni sono:

- Qualsiasi - Questa opzione consente al WAP di applicare il filtro ai pacchetti provenienti

da qualsiasi indirizzo IP.

- Indirizzo singolo — questa opzione consente al WAP di applicare il filtro ai pacchetti provenienti da un indirizzo IP specificato.
- Indirizzo/Maschera — questa opzione consente al punto di accesso Windows di applicare il filtro ai pacchetti a un indirizzo IP e alla maschera dell'IP.



Nota: Nell'esempio viene scelto Indirizzo singolo.

Passaggio 13. Immettere l'indirizzo IP dell'host che deve essere autorizzato per l'accesso alla rete.



Nota: Nell'esempio, viene immesso 192.168.100.139. Questo è l'indirizzo IP di PC2.

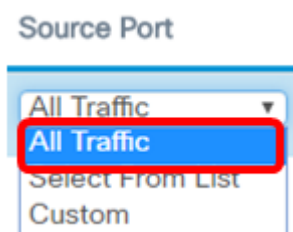
Passaggio 14. Scegliere una porta di origine per la condizione. Le opzioni sono:

- All Traffic - Questa opzione consente di usare tutti i pacchetti della porta di origine che soddisfano i criteri.
- Seleziona da elenco - questa opzione consente di scegliere ftp, ftpdata, http, smtp, snmp, telnet, tftp e www.
- Personalizzata - questa opzione consente di immettere un numero di porta IANA corrispondente alla porta di origine identificata nell'intestazione del datagramma. L'intervallo di porte è compreso tra 0 e 65535 e include quanto segue:

da - 0 a 1023 — Porte conosciute

- 1024 — 49151 — Porti registrati

- 49152 — 65535 — Porte dinamiche e/o private



Nota: Nell'esempio, viene scelto Tutto il traffico.

Passaggio 15. Selezionare un indirizzo di destinazione dall'elenco a discesa Indirizzo IPv4 destinazione. Le opzioni sono:

- Any: questa opzione considera qualsiasi indirizzo IP come una corrispondenza con

l'istruzione ACL.

- Indirizzo singolo - questa opzione permette di immettere un indirizzo IP specifico per la condizione ACL.
- Indirizzo/maschera - questa opzione consente di immettere un intervallo di indirizzi IP o una maschera.

The image shows a configuration interface with two dropdown menus. The first menu, labeled 'Source Port', has 'All Traffic' selected. The second menu, labeled 'Destination IPv4 Address', is open and shows 'Any' selected and highlighted with a red box. Below 'Any', the options 'Single Address' and 'Address/Mask' are visible.

Nota: Nell'esempio, viene scelto Qualsiasi.

Passaggio 16. Scegliere una porta di destinazione dall'elenco a discesa Porta di destinazione. Le opzioni sono:

- Any: questa opzione considera tutte le porte di destinazione dei pacchetti come corrispondenze con l'istruzione nell'ACL.
- Select From List - Questa opzione consente di scegliere una parola chiave associata alla porta di destinazione da associare. Le opzioni sono: ftp, ftpdata, http, smtp, snmp, telnet, tftp e www. Queste parole chiave vengono convertite nei numeri di porta corrispondenti.
- Personalizzata - questa opzione consente di immettere un numero di porta IANA corrispondente alla porta di origine identificata nell'intestazione del datagramma. L'intervallo di porte è compreso tra 0 e 65535 e include quanto segue:

- da - 0 a 1023 — Porte conosciute
- 1024 — 49151 — Porti registrati
- 49152 — 65535 — Porte dinamiche e/o private

Passaggio 17. Scegliere un tipo di servizio corrispondente al tipo di pacchetto dall'elenco a discesa Tipo di servizio. Le opzioni sono:

- Any - Questa opzione considera qualsiasi servizio come una corrispondenza per i pacchetti.
- Select From List: questa opzione consente di associare i pacchetti in base ai valori DSCP (Differentiated Services Code Point), CoS (Class of Service) o EF (Expedited Forwarding).
- DSCP — l'opzione individua i pacchetti in base al valore DSCP personalizzato. Quando si sceglie questa opzione, immettere un valore compreso tra 0 e 63 nel campo Valore DSCP.
- Precedenza: questa opzione consente di trovare i pacchetti in base al relativo valore di precedenza IP. Quando si sceglie questa opzione, immettere un valore di precedenza IP compreso tra 0 e 7.
- ToS/Mask: questa opzione consente di immettere una maschera IP ToS per identificare le posizioni dei bit nel valore dei bit del tos IP utilizzati per il confronto con il campo ToS IP di un pacchetto.

Destination Port Type Of Service

Any Any

Any

Select From List

DSCP

Precedence

ToS/Mask

Passaggio 18. (Facoltativo) Ripetere i passaggi da 8 a 17 finché l'ACL non è completo.

Nota: Poiché alla fine di ciascuna regola creata viene visualizzato un messaggio di negazione implicita, non è necessario aggiungere una regola di negazione all'ACL per impedire l'accesso da altri dispositivi della rete.

Passaggio 19. (Facoltativo) Modificare l'ordine delle condizioni nell'ACL facendo clic sui pulsanti Su e Giù finché non sono nell'ordine corretto.

+ ✎ 🗑️

Rule Priority

1 ▼

2 ▲

Passaggio 20. Fare clic su **OK**.

Source Port Destination IPv4 Address

All Traffic Any



Passaggio 21. Fare clic su **Salva**.

WAP125-wap5e0940 cisco ? i ↻

ACL Save

ACL Table

+ ✎ 🗑️

<input type="checkbox"/>	Enable	ACL Name	ACL Type	Associated Interface	Details Of Rule(s)
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TestIPv4ACL	IPv4	<ul style="list-style-type: none"> 2.4G VAP 0 (CiscoSB) 2.4G VAP 1 (CiscoTest) 5G VAP 0 (MyNetwork) Ethernet Port 	More...

A questo punto, è necessario aver completato la configurazione di un ACL IPv4 che consenta a un solo host di accedere alla rete quando collegato al WAP.