

Configurazione di elenchi di controllo di accesso MAC, IPv4 e IPv6 in un punto di accesso wireless

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. Blocca gli utenti non autorizzati e consente agli utenti autorizzati di accedere a risorse specifiche. Un ACL contiene gli host a cui è consentito o negato l'accesso al dispositivo di rete. Gli ACL possono essere definiti in due modi: in base all'indirizzo IPv4 o all'indirizzo IPv6.

In questo articolo viene illustrato come creare correttamente un ACL e configurare ACL basati su IPv4, IPv6 e Media Access Control (MAC) sul punto di accesso wireless (WAP) per migliorare la sicurezza della rete.

Dispositivi interessati

- Serie WAP100
- Serie WAP300
- Serie WAP500

Versione del software

- 1.0.6.2 - WAP121, WAP321
- 1.2.0.2 - WAP371, WAP551, WAP561
- 1.0.1.4 - WAP131, WAP351
- 1.0.0.16 - WAP150, WAP361

Creazione di ACL

Nota: Le immagini utilizzate per questa configurazione provengono da WAP150.

Passaggio 1. Accedere all'utility basata sul Web access point e scegliere **ACL > Regola ACL**.



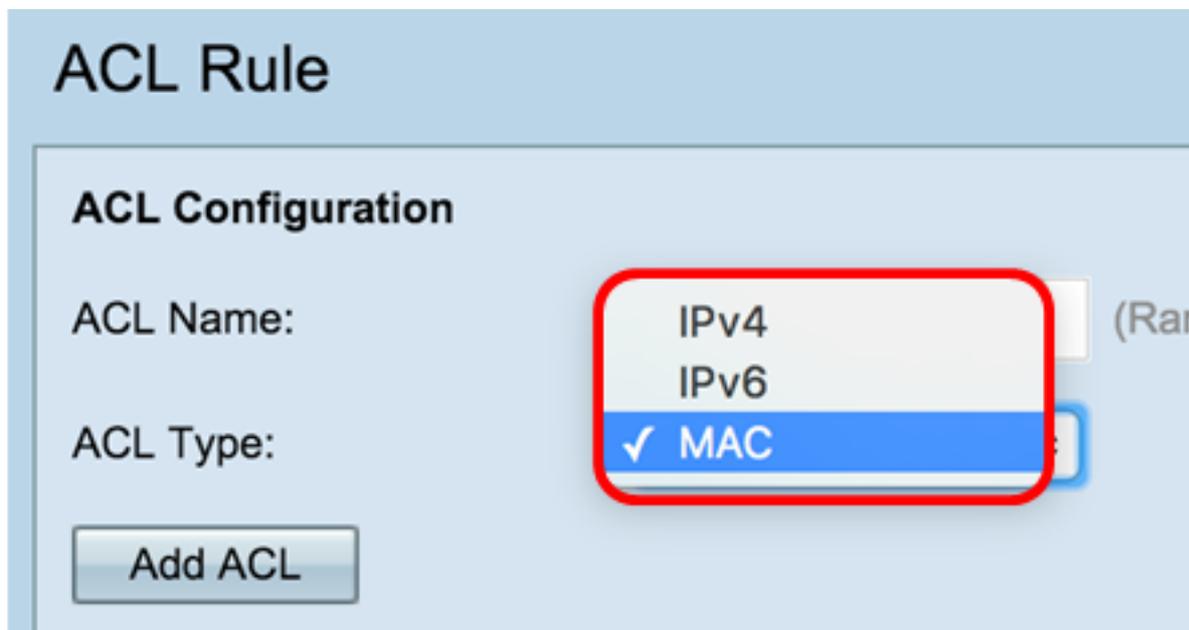
Nota: Per WAP121, WAP321, WAP371, WAP551 e WAP561: Accedere all'utility basata sul Web del punto di accesso e scegliere QoS client > ACL.



Passaggio 2. Dopo aver aperto la pagina Configurazione ACL, immettere il nome dell'ACL nel campo *Nome ACL*.



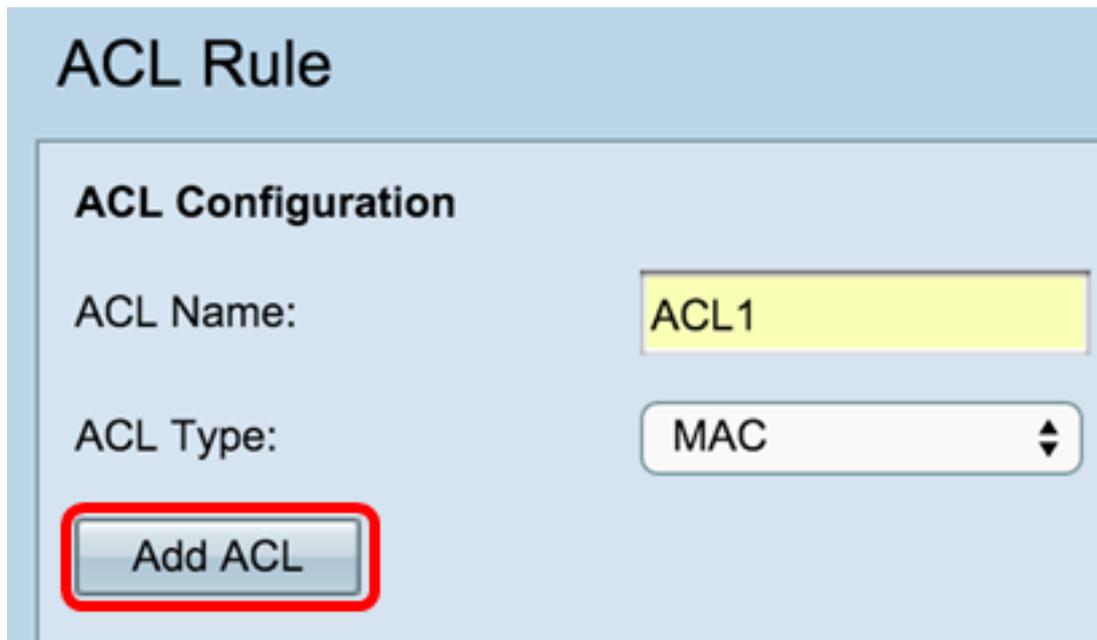
Passaggio 3. Selezionare un **tipo di ACL** dall'elenco a discesa Tipo di ACL.



- IPv4: un indirizzo a 32 bit (4 byte).

- IPv6: successore di IPv4, costituito da un indirizzo a 128 bit (8 byte).
- MAC — l'indirizzo MAC è l'indirizzo univoco assegnato a un'interfaccia di rete.

Passaggio 4. Fare clic sul pulsante **Add ACL**.



ACL Rule

ACL Configuration

ACL Name:

ACL Type:

Add ACL

Se si sceglie MAC, saltare alla sezione [Configurazione di ACL basati su MAC](#).

Se si sceglie IPv4, saltare alla [configurazione dell'ACL basato su IPv4](#).

Se si sceglie IPv6, saltare alla [configurazione dell'ACL basato su IPv6](#).

La creazione dell'ACL è stata completata.

Configurazione di ACL basati su MAC

Passaggio 1. Selezionare l'ACL dall'elenco a discesa Nome ACL - Tipo ACL a cui si desidera aggiungere le regole.

Nota: Nell'immagine seguente, è stato scelto ACL1 MAC come esempio.



ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Passaggio 2. Se è necessario configurare una nuova regola per l'ACL scelto, scegliere **Nuova regola** dall'elenco a discesa *Regola*. In caso contrario, scegliere una delle regole correnti dall'elenco a discesa *Regola*.

Nota: è possibile creare un massimo di 10 regole per un singolo ACL.

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Passaggio 3. Selezionare l'azione per la regola ACL dall'elenco a discesa *Azione*.

Nota: in questo esempio viene creata un'istruzione Deny.

Action:

Match Every Packet:

- Rifiuta — blocca tutto il traffico che soddisfa i criteri della regola per l'ingresso o l'uscita da WAP. Poiché alla fine di ogni ACL è presente una regola di negazione implicita di tutto, il traffico che non è esplicitamente autorizzato viene interrotto.
- Autorizza — consente a tutto il traffico che soddisfa i criteri della regola di accedere o uscire dal WAP. Il traffico che non soddisfa i criteri viene eliminato.

Nota: I passaggi da 4 a 11 sono facoltativi. I filtri selezionati sono attivati. Deselezionare la casella di controllo relativa al filtro che non si desidera applicare alla regola specifica.

Passaggio 4. Selezionare la casella di controllo **Corrispondenza ogni pacchetto** per verificare la corrispondenza con la regola per ogni frame o pacchetto, indipendentemente dal relativo contenuto. Deselezionare la casella per configurare uno qualsiasi dei criteri di corrispondenza aggiuntivi.

Suggerimento: se **Corrispondenza per ogni pacchetto** è già selezionato, andare al [passo 12](#).

Action:

Match Every Packet:

Passaggio 5. Nell'area EtherType, scegliere un pulsante di opzione per confrontare i criteri corrispondenti con il valore nell'intestazione di un frame Ethernet. È possibile scegliere una di queste opzioni o scegliere Qualsiasi:

- Select From List: consente di scegliere un protocollo dall'elenco a discesa. L'elenco include le opzioni seguenti: appletalk, arp, IPv4, IPv6, ipx, netbios, pppoe.
- Corrispondenza con valore - per l'identificativo di protocollo personalizzato, immettere l'identificativo che va da 0600 a FFFF.

Protocol:

Any

Select From List:

Match to Value:

icmp

0 (Range)

Passaggio 6. Nell'area Classe di servizio, scegliere un pulsante di opzione per immettere la priorità utente 802.1p da confrontare con un frame Ethernet. È possibile scegliere Qualsiasi o una priorità definita dall'utente. Immettere la priorità compresa tra 0 e 7 nel campo *Definita dall'utente*.

Class Of Service:

Any

User Defined

6

Passaggio 7. Nell'area MAC di origine, scegliere un pulsante di opzione per confrontare l'indirizzo MAC di origine con un frame Ethernet. È possibile scegliere **Qualsiasi** o **Definito dall'utente** e immettere l'indirizzo MAC di origine nel campo fornito.

Source MAC:

Any

User Defined

Source MAC Address: 04:FE:36:A5:670B

Source MAC Mask:

Passaggio 8. Immettere la maschera dell'indirizzo MAC di origine nel campo *Maschera MAC di origine* per specificare i bit dell'indirizzo MAC di origine da confrontare con un frame Ethernet.

Nota: Se la maschera MAC utilizza un bit 0, l'indirizzo viene accettato e se utilizza un bit 1, l'indirizzo viene ignorato.

Source MAC:

Any

User Defined

Source MAC Address: 04:FE:36:A5:670B

Source MAC Mask: 00:00:00:00:00:00

Passaggio 9. Nell'area MAC di destinazione, scegliere un pulsante di opzione per confrontare l'indirizzo MAC di destinazione con un frame Ethernet. È possibile scegliere Any o Definito dall'utente e immettere l'indirizzo MAC di destinazione nel campo fornito.

Destination MAC:

Any

User Defined

Destination MAC Address: F2:CA:46:11:EA:09

Destination MAC Mask:

Passaggio 10. Immettere la maschera dell'indirizzo MAC di destinazione nel campo *Maschera MAC di destinazione* per specificare i bit dell'indirizzo MAC di destinazione da confrontare con un frame Ethernet.

Nota: Se la maschera MAC utilizza un bit 0, l'indirizzo viene accettato e se utilizza un bit 1, l'indirizzo viene ignorato.

Destination MAC: Any
 User Defined
Destination MAC Address: F2:CA:46:11:EA:09
Destination MAC Mask: 00:00:00:00:00:00

Passaggio 11. Nell'area **VLAN ID**, selezionare un pulsante di opzione per confrontare l'ID VLAN con un frame Ethernet. Immettere l'ID VLAN da 0 a 4095 nel campo fornito.

VLAN ID: Any
 User Defined 52 (Range: 0 - 4095)

Passaggio 12. Fare clic su **Salva**.

VLAN ID: Any
 User Defined
Delete ACL:

Save

Passaggio 13. (Facoltativo) Per eliminare l'ACL configurato, selezionare la casella di controllo **Elimina ACL** e fare clic su **Salva**.

A questo punto, è necessario configurare correttamente l'ACL MAC sul WAP.

Configurazione di ACL basati su IPv4

Passaggio 1. Nell'area Configurazione regola ACL, configurare i seguenti parametri della regola:

Nome ACL - Tipo ACL
selezionare l'ACL da configurare con la nuova regola.

Nota: Nell'immagine seguente, è stato scelto come esempio IPv4_ACL-IPv4.

ACL Rule Configuration

ACL Name - ACL Type: ✓ IPv4_ACL - IPv4
ACL1 - MAC

Rule: New Rule

Passaggio 2. Se è necessario configurare una nuova regola per l'ACL scelto, scegliere **Nuova regola** dall'elenco a discesa *Regola*. In caso contrario, scegliere una delle regole correnti dall'elenco a discesa *Regola*.

Nota: è possibile creare un massimo di 10 regole per un singolo ACL.

ACL Rule Configuration

ACL Name - ACL Type: IPv4_ACL - IPv4

Rule: New Rule

Passaggio 3. Selezionare l'azione per la regola ACL dall'elenco a discesa *Azione*.

Nota: in questo esempio viene creata un'istruzione Permit.

- Rifiuta — blocca tutto il traffico che soddisfa i criteri della regola per l'ingresso o l'uscita da WAP. Poiché alla fine di ogni ACL è presente una regola di negazione implicita di tutto, il traffico che non è esplicitamente autorizzato viene interrotto.
- Autorizza — consente a tutto il traffico che soddisfa i criteri della regola di accedere o uscire dal WAP. Il traffico che non soddisfa i criteri viene eliminato.

Action: Deny
✓ Permit

Nota: I passaggi da 4 a 9 sono facoltativi. I filtri selezionati sono attivati. Deselezionare la casella di controllo relativa al filtro se non si desidera applicarlo alla regola specifica.

Passaggio 4. Selezionare la casella di controllo **Corrispondenza ogni pacchetto** per verificare la corrispondenza con la regola per ogni frame o pacchetto, indipendentemente dal relativo contenuto. Deselezionare la casella per configurare uno dei criteri di corrispondenza aggiuntivi.

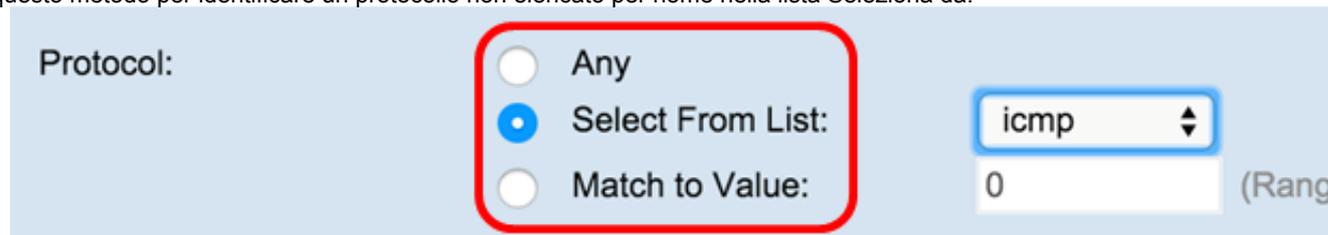
Match Every Packet: ✓

Suggerimento: l'opzione Corrispondenza per ogni pacchetto è abilitata per impostazione predefinita. Se si desidera

mantenere questa impostazione, andare al [passaggio 11](#).

Passaggio 5. Nell'area Protocollo, scegliere un pulsante di opzione per confrontare i criteri corrispondenti con il valore nell'intestazione di un frame Ethernet. È possibile scegliere Qualsiasi o effettuare una selezione dall'elenco a discesa

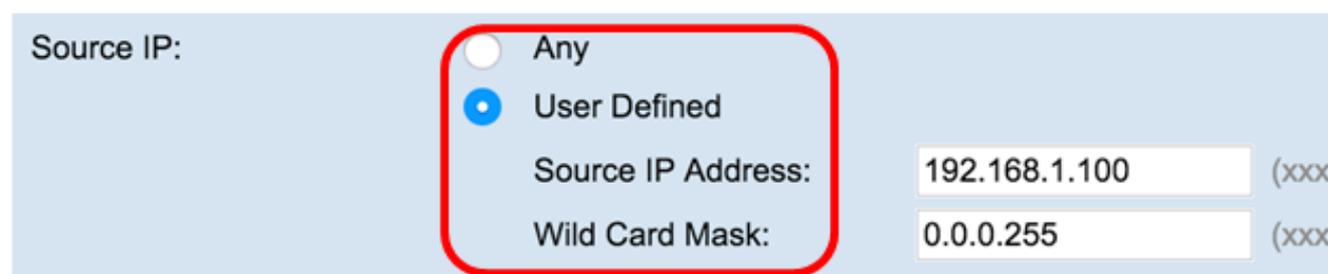
- Select From List: consente di scegliere uno dei seguenti protocolli:
 - IP — Il protocollo di comunicazione principale nella suite di protocolli Internet per l'inoltro dei dati sulle reti.
 - ICMP — Protocollo della Internet Protocol Suite utilizzato da dispositivi come i router per inviare messaggi di errore.
 - IGMP — Protocollo di comunicazione utilizzato dall'host per stabilire l'appartenenza a gruppi multicast su reti IPv4.
 - TCP — Consente a due host di stabilire una connessione e scambiare flussi di dati.
 - UDP — Protocollo della suite di protocolli Internet che utilizza un modello di trasmissione senza connessione.
- Corrispondenza con valore: immettere un ID di protocollo standard assegnato da IANA compreso tra 0 e 255. Scegliere questo metodo per identificare un protocollo non elencato per nome nella lista Seleziona da.



Passaggio 6. Nell'area IP origine, scegliere un pulsante di opzione per includere l'indirizzo IP dell'origine nella condizione di corrispondenza. È possibile scegliere Qualsiasi o Definito dall'utente, quindi immettere l'indirizzo IP e la maschera con caratteri jolly dell'origine nei campi corrispondenti.

- Source IP Address: immettere un indirizzo IP per applicare questo criterio.
- Maschera con caratteri jolly — immettere la maschera con caratteri jolly per l'indirizzo IP di destinazione. La maschera con caratteri jolly determina i bit utilizzati e i bit ignorati. Una maschera con caratteri jolly di 255.255.255.255 indica che nessun bit è importante. Un carattere jolly 0.0.0.0 indica che tutti i bit sono importanti. Questo campo è obbligatorio quando si seleziona Indirizzo IP di origine.

Nota: Una maschera con caratteri jolly è fondamentalmente l'inverso di una subnet mask. Ad esempio, per far corrispondere i criteri a un singolo indirizzo host, utilizzare una maschera con caratteri jolly di 0.0.0.0. Per far corrispondere i criteri a una subnet a 24 bit, ad esempio 192.168.10.0/24, utilizzare una maschera con caratteri jolly di 0.0.0.255.



Passaggio 7. Nell'area Porta di origine, scegliere un pulsante di opzione per includere una porta di origine nella condizione di corrispondenza. È possibile scegliere Qualsiasi per far corrispondere qualsiasi porta di origine oppure scegliere quanto segue:

- Seleziona dall'elenco - Scegliere una porta di origine dall'elenco a discesa Seleziona dall'elenco. Le opzioni sono le seguenti:
 - File Transfer Protocol (FTP) — FTP è un protocollo di rete standard utilizzato per trasferire file da un host all'altro su una rete basata su TCP (Transmission Control Protocol), ad esempio Internet.
 - dati FTP — Canale dati avviato dal server collegato a un client, in genere tramite la porta 20.
 - HTTP (Hypertext Transfer Protocol) — HTTP è un protocollo applicativo alla base della comunicazione dei dati per il World Wide Web.
 - Simple Mail Transfer Protocol (SMTP) — SMTP è uno standard Internet per la trasmissione della posta elettronica.
 - Simple Network Management Protocol (SNMP) — SNMP è un protocollo Internet standard per la gestione di dispositivi su reti

IP.

— Telnet — Protocollo a livello di sessione utilizzato su Internet o nelle reti locali per fornire comunicazioni bidirezionali interattive orientate al testo.

— Trivial File Transfer Protocol (TFTP) — Il TFTP è un'utility software Internet per il trasferimento di file più semplice da utilizzare rispetto al protocollo FTP, ma meno capace.

— World Wide Web (WWW) — WWW è un sistema di server Internet che supportano documenti in formato HTTP.

- Corrispondenza con porta - immettere il numero di porta non presente nell'elenco. I numeri di porta sono compresi tra 0 e 65535 nel campo *Confronta con porta* per le porte di origine non elencate. L'intervallo include tre tipi diversi di porte. Gli intervalli sono descritti come segue

— da 0 a 1023 — Porte conosciute

— da 1024 a 49151 — Porte registrate

— da 49152 a 65535 — porte dinamiche e/o private

- Maschera — immettere la maschera della porta. La maschera determina i bit utilizzati e i bit ignorati. È consentita solo la cifra esadecimale (0 — 0xFFFF). 0 indica che il bit è importante e 1 indica che questo bit deve essere ignorato.

Source Port:

Any

Select From List:

Match to Port:

Mask:

www (Range: 0 - 65535)

(Range: 0 ~ 0xffff, 0s)

Passaggio 8. Nell'area IP di destinazione, scegliere un pulsante di opzione per includere l'indirizzo IP della destinazione nella condizione di corrispondenza. È possibile scegliere Qualsiasi o Definito dall'utente, quindi immettere l'indirizzo IP e il formato jolly della destinazione nei campi corrispondenti.

- Indirizzo IP di destinazione: immettere un indirizzo IP per applicare questo criterio.
- Maschera con caratteri jolly — immettere la maschera con caratteri jolly per l'indirizzo IP di destinazione. La maschera con caratteri jolly determina i bit utilizzati e i bit ignorati. Una maschera con caratteri jolly di 255.255.255.255 indica che nessun bit è importante. Un carattere jolly 0.0.0.0 indica che tutti i bit sono importanti. Questo campo è obbligatorio quando si seleziona Indirizzo IP di destinazione.

Nota: Una maschera con caratteri jolly è fondamentalmente l'inverso di una subnet mask. Ad esempio, per far corrispondere i criteri a un singolo indirizzo host, utilizzare una maschera con caratteri jolly di 0.0.0.0. Per far corrispondere i criteri a una subnet a 24 bit, ad esempio 192.168.10.0/24, utilizzare una maschera con caratteri jolly di 0.0.0.255.

Destination IP:

Any

User Defined

Match to Port:

Destination IP Address: 192.168.1.110 (xxx.xxx.xxx.xxx)

Wild Card Mask: 0.0.0.255 (xxx.xxx.xxx.xxx -)

Passaggio 9. Nell'area Porta di destinazione, scegliere un pulsante di opzione per includere una porta di destinazione nella condizione di corrispondenza. È possibile scegliere Qualsiasi in base a qualsiasi porta di destinazione oppure scegliere quanto segue:

- Seleziona da elenco — scegliere una porta di destinazione dall'elenco a discesa. Le opzioni sono le seguenti

— FTP — Protocollo di rete standard utilizzato per trasferire file da un host a un altro su una rete basata su TCP, ad esempio Internet.

— dati FTP — Canale dati avviato dal server collegato a un client, in genere tramite la porta 20.

— HTTP — Protocollo applicativo alla base della comunicazione dei dati per il World Wide Web.

— SMTP — Standard Internet per la trasmissione della posta elettronica.

— SNMP — Un protocollo Internet standard per la gestione dei dispositivi sulle reti IP.

— Telnet — Protocollo a livello di sessione utilizzato su Internet o nelle reti locali per fornire comunicazioni bidirezionali interattive

orientate al testo.

— TFTP — Utilità software Internet per il trasferimento di file più semplice da utilizzare rispetto a FTP ma meno funzionale.

— WWW — Un sistema di server Internet che supportano documenti in formato HTTP.

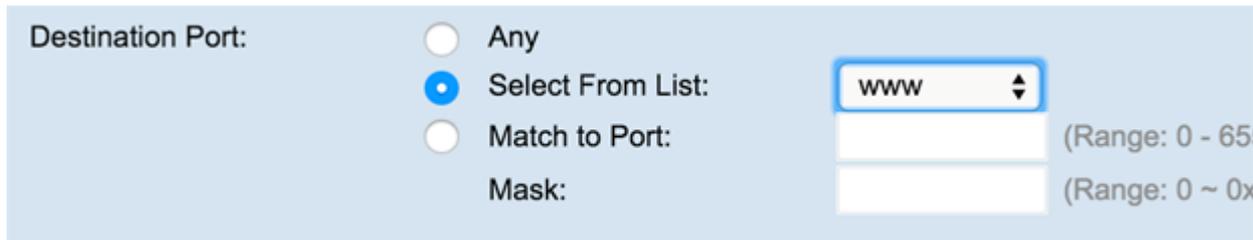
- Corrispondenza con porta - immettere il numero di porta non presente nell'elenco. I numeri di porta sono compresi tra 0 e 65535 nel campo *Confronta con porta* per le porte di origine non elencate. L'intervallo include tre tipi diversi di porte. Gli intervalli sono descritti come segue:

— da 0 a 1023 — Porte conosciute

— da 1024 a 49151 — Porte registrate

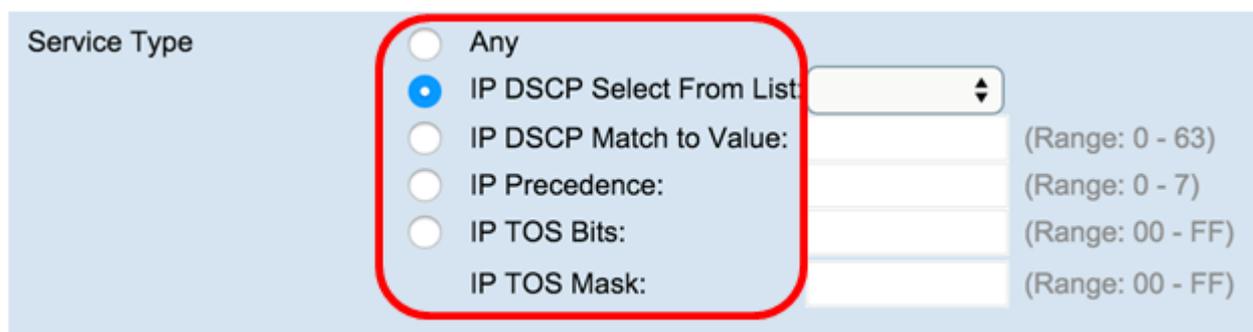
— da 49152 a 65535 — porte dinamiche e/o private

- Maschera — immettere la maschera della porta. La maschera determina i bit utilizzati e i bit ignorati. È consentita solo la cifra esadecimale (0-0xFFFF). 0 indica che il bit è importante e 1 indica che questo bit deve essere ignorato.



Passaggio 10. Nell'area Tipo di servizio, scegliere un pulsante di opzione per cercare i pacchetti corrispondenti a un tipo di servizio specifico. È possibile scegliere Qualsiasi oppure scegliere tra le opzioni seguenti:

- IP DSCP Select From List: trova i pacchetti in base ai relativi valori DSCP (Differentiated Services Code Point), AS (Assured Forwarding), CS (Class of Service) o EF (Expedited Forwarding).
- Corrispondenza DSCP IP al valore — Corrisponde ai pacchetti in base a un valore DSCP personalizzato. Se selezionato, immettere un valore compreso tra 0 e 63 in questo campo.
- IP Precedence: trova i pacchetti in base al relativo valore di IP Precedence. Se è stato selezionato, immettere un valore di precedenza IP compreso tra 0 e 7.
- Bit TOS IP: specifica un valore per utilizzare i bit TOS dei pacchetti nell'intestazione IP come criteri di corrispondenza.
- Il campo TOS IP in un pacchetto è definito come tutti gli otto bit dell'ottetto Service Type nell'intestazione IP. Il valore IP TOS Bits è un numero esadecimale a due cifre compreso tra 00 e ff. I tre bit di ordine superiore rappresentano il valore di precedenza IP. I sei bit più significativi rappresentano il valore IP DSCP.
- Maschera TOS IP: immettere un valore di maschera TOS IP per identificare le posizioni dei bit nel valore dei bit TOS IP utilizzati per il confronto con il campo TOS IP di un pacchetto.
- Il valore IP TOS Mask è un numero esadecimale a due cifre compreso tra 00 e FF che rappresenta una maschera invertita, ovvero un carattere jolly. I bit con valore zero nella maschera TOS IP indicano le posizioni dei bit nel valore dei bit del TOS IP utilizzati per il confronto con il campo TOS IP di un pacchetto. Ad esempio, per controllare un valore IP TOS con bit 7 e 5 impostati e bit 1 non impostato, dove il bit 7 è il più significativo, usare un valore IP TOS Bits di 0 e una maschera IP TOS di 00.



Passaggio 11. Fare clic su Salva.

VLAN ID: Any
 User Defined

Delete ACL:

Save

A questo punto, è necessario configurare correttamente un ACL basato su IPv4.

Configurare ACL basati su IPv6

Passaggio 1. Nell'area Configurazione regola ACL, configurare i seguenti parametri della regola:

Nome ACL - Tipo ACL - Selezionare l'ACL da configurare con la nuova regola.

Nota: Nell'immagine seguente è stato scelto IPv6_ACL — Pv6 come esempio.

ACL Rule Configuration

ACL Name - ACL Type: **IPv6_ACL - IPv6**

Rule: **New Rule**

Passaggio 2. Se è necessario configurare una nuova regola per l'ACL scelto, scegliere Nuova regola dall'elenco a discesa Regola. In caso contrario, scegliere una delle regole correnti dall'elenco a discesa Regola.

Nota: È possibile creare un massimo di 10 regole per un singolo ACL.

ACL Rule Configuration

ACL Name - ACL Type: IPv6_ACL - IPv6

Rule: **New Rule**

Passaggio 3. Selezionare l'azione per la regola ACL dall'elenco a discesa *Azione*

- Rifiuta — blocca tutto il traffico che soddisfa i criteri della regola per l'ingresso o l'uscita da WAP. Poiché alla fine di ogni ACL è presente una regola di negazione implicita di tutto, il traffico che non è esplicitamente autorizzato viene interrotto.
- Autorizza — consente a tutto il traffico che soddisfa i criteri della regola di accedere o uscire dal WAP. Il traffico che non soddisfa i criteri viene eliminato.

Action: **Deny**

Match Every Packet:

Nota: I passaggi da 4 a 11 sono facoltativi. I filtri selezionati sono attivati. Deselezionare la casella di controllo relativa al filtro se non si desidera applicarlo alla regola specifica.

Passaggio 4. Selezionare la casella di controllo *Corrispondenza ogni pacchetto* per verificare la corrispondenza con la regola per ogni frame o pacchetto, indipendentemente dal relativo contenuto. Deselezionare la casella per configurare uno dei criteri di corrispondenza aggiuntivi.

Match Every Packet:



Suggerimento: Corrispondenza ogni pacchetto è abilitato per impostazione predefinita. Se si desidera mantenere questa impostazione, andare al [punto 12](#).

Passaggio 5. Nell'area Protocollo, scegliere un pulsante di opzione per confrontare i criteri corrispondenti con il valore nell'intestazione di un frame Ethernet. È possibile scegliere una di queste opzioni o scegliere Qualsiasi:

- Select From List: consente di scegliere uno dei seguenti protocolli:
 - IP — Il protocollo di comunicazione principale nella suite di protocolli Internet per l'inoltro dei dati sulle reti.
 - ICMP — Protocollo della Internet Protocol Suite utilizzato da dispositivi come i router per inviare messaggi di errore.
 - IGMP — Protocollo di comunicazione utilizzato dall'host per stabilire l'appartenenza a gruppi multicast su reti IPv4.
 - TCP — Consente a due host di stabilire una connessione e scambiare flussi di dati.
 - UDP — Protocollo della suite di protocolli Internet che utilizza un modello di trasmissione senza connessione.
- Corrispondenza con valore: immettere un ID di protocollo standard assegnato da IANA compreso tra 0 e 255. Scegliere questo metodo per identificare un protocollo non elencato per nome nella lista Seleziona da.

Passaggio 6. Nell'area IPv6 di origine scegliere un pulsante di opzione per includere l'indirizzo IP dell'origine nella condizione di corrispondenza. È possibile scegliere Qualsiasi o Definito dall'utente, quindi immettere l'indirizzo IPv6 e la lunghezza del prefisso IPv6 di origine.

- Indirizzo IPv6 di origine: immettere un indirizzo IPv6 per applicare questo criterio.
- Lunghezza prefisso IPv6 di origine: immettere la lunghezza del prefisso dell'indirizzo IPv6 di origine.

Passaggio 7. Nell'area *Porta di origine*, scegliere un pulsante di opzione per includere una porta di origine nella condizione di corrispondenza. È possibile scegliere Qualsiasi in base a qualsiasi porta di origine oppure scegliere quanto segue:

- Seleziona dall'elenco — scegliere una porta di origine dall'elenco a discesa *Seleziona da elenco*. Le opzioni sono le seguenti:

— FTP — Protocollo di rete standard utilizzato per trasferire file da un host a un altro su una rete basata su TCP, ad esempio Internet.
— dati FTP — Canale dati avviato dal server collegato a un client, in genere tramite la porta 20.
— HTTP — Protocollo applicativo alla base della comunicazione dei dati per il World Wide Web.
— SMTP — Standard Internet per la trasmissione della posta elettronica.
— SNMP — Un protocollo Internet standard per la gestione dei dispositivi sulle reti IP.
— Telnet — Protocollo a livello di sessione utilizzato su Internet o nelle reti locali per fornire comunicazioni bidirezionali interattive orientate al testo.
— TFTP — Utilità software Internet per il trasferimento di file più semplice da utilizzare rispetto a FTP ma meno funzionale.
— WWW — Un sistema di server Internet che supportano documenti in formato HTTP.

- Corrispondenza con porta - immettere il numero di porta non presente nell'elenco. I numeri di porta sono compresi tra 0 e 65535 nel campo *Confronta con porta* per le porte di origine non elencate. L'intervallo include tre tipi diversi di porte. Gli intervalli sono descritti come segue:

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

- Maschera — immettere la maschera della porta. La maschera determina i bit utilizzati e i bit ignorati. È consentita solo la cifra esadecimale (0 à 0xFFFF). 0 indica che il bit è importante e 1 indica che questo bit deve essere ignorato.

Passaggio 8. Nell'area IPv6 di destinazione scegliere un pulsante di opzione per includere l'indirizzo IP della destinazione nella condizione di corrispondenza. È possibile scegliere Qualsiasi o Definito dall'utente per immettere l'indirizzo IPv6 e la lunghezza del prefisso IPv6 di destinazione.

- Indirizzo IPv6 di destinazione: immettere un indirizzo IPv6 per applicare questo criterio.
- Lunghezza prefisso IPv6 di destinazione: immettere la lunghezza del prefisso dell'indirizzo IPv6 di destinazione.

Passaggio 9. Nell'area Porta di destinazione, scegliere un pulsante di opzione per includere una porta di destinazione nella condizione di corrispondenza. È possibile scegliere Qualsiasi in base a qualsiasi porta di destinazione oppure scegliere quanto segue:

- Seleziona dall'elenco — scegliere una porta di destinazione dall'elenco a discesa *Seleziona da elenco*. Le opzioni sono FTP, FTP data, HTTP, SNMP, SMTP, TFTP, Telnet, WWW.
- Corrispondenza con porta - immettere il numero di porta non presente nell'elenco. I numeri di porta sono compresi tra 0 e 65535 nel campo *Confronta con porta* per le porte di origine non elencate. L'intervallo include tre tipi diversi di porte. Gli intervalli sono descritti come segue:

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

- Maschera — immettere la maschera della porta. La maschera determina i bit utilizzati e i bit ignorati. È consentita solo la cifra esadecimale (0-0xFFFF). 0 indica che il bit è importante e 1 indica che questo bit deve essere ignorato.

Passaggio 10. Nell'area Etichetta flusso IPv6 scegliere un pulsante di opzione per includere l'etichetta di flusso IPv6 nella condizione di corrispondenza. È possibile scegliere Qualsiasi o Definito dall'utente e immettere un numero a 20 bit univoco per un pacchetto IPv6. L'intervallo è compreso tra 0 e 0xffff.

Passaggio 11. Nell'area DSCP IPv6 scegliere un pulsante di opzione per far corrispondere i pacchetti al relativo valore DSCP IP. È possibile scegliere Qualsiasi oppure scegliere quanto segue:

- Seleziona dall'elenco - Scegliere uno dei seguenti valori: DSCP Assured Forwarding (AF), Class of Service (CS) o Expedited

Forwarding (EF).

- Corrispondenza con valore - immettere un valore DSCP personalizzato compreso tra 0 e 63.

IPv6 DSCP:

Any

Select From List:

Match to Value:

(Range: 0 - 63)

Delete ACL:

Save

[Passaggio 12.](#) Fare clic su Salva.

IPv6 DSCP:

Any

Select From List:

Match to Value:

Delete ACL:

Save

Passaggio 13. (Facoltativo) Per eliminare un ACL, verificare che il nome dell'ACL sia selezionato nell'elenco Nome ACL-Tipo ACL, quindi selezionare Elimina ACL.

È ora necessario configurare correttamente un ACL basato su IPv6.