

Creazione e configurazione di una regola per un ACL (Access Control List) basato su IPv4 sui punti di accesso WAP121 e WAP321

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. Un ACL contiene gli host a cui è consentito o negato l'accesso al dispositivo di rete. La funzionalità QoS contiene il supporto DiffServ (Differentiated Services), che consente di classificare il traffico in flussi e ricevere un determinato trattamento QoS in base ai comportamenti per hop definiti.

In questo documento viene spiegato come creare e configurare ACL IPv4 con punti di accesso WAP121 e WAP321 (WAP).

Dispositivi interessati

- WAP121
- WAP321

Versione del software

- v1.0.3.4

Configurazione di ACL basati su IPv4

Gli ACL IP classificano il traffico per il layer 3 dello stack IP. Ogni ACL è costituito da un massimo di 10 regole applicate al traffico inviato da un client wireless o che deve essere ricevuto da un client wireless. Ogni regola specifica se il contenuto di un determinato campo deve essere utilizzato per consentire o negare l'accesso alla rete. Le regole possono essere basate su diversi criteri e possono essere applicate a uno o più campi all'interno di un pacchetto, ad esempio l'indirizzo IP di origine o di destinazione, la porta di origine o di destinazione o il protocollo contenuto nel pacchetto.

Creazione di ACL IPv4

Passaggio 1. Accedere all'utility di configurazione del punto di accesso e scegliere **QoS client > ACL**. Viene visualizzata la pagina *ACL*:

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: IPv4 ▾

Passaggio 2. Inserire il nome dell'ACL nel campo *Nome ACL*.

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: IPv4 ▾

Passaggio 3. Selezionare il tipo di **IPv4** per l'ACL dall'elenco a discesa *ACL Type* (Tipo di ACL).

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: ▾

- IPv4
- IPv6
- MAC

Passaggio 4. Per creare un nuovo ACL IPv4, fare clic su **Add ACL**.

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: IPv4 ▾

Configurazione di una regola per l'ACL IPv4

Passaggio 1. Selezionare l'ACL dall'elenco a discesa *Nome ACL-Tipo ACL* per cui configurare le regole.

ACL Rule Configuration

ACL Name - ACL Type: ExampleAllowSMTP - IPv4 ▼

Rule: New Rule ▼

Action: Deny ▼

Match Every Packet:

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*.

ACL Rule Configuration

ACL Name - ACL Type: ExampleAllowSMTP - IPv4 ▼

Rule: New Rule ▼

Action: Deny ▼

Match Every Packet:

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

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

ACL

ACL Configuration

ACL Name: (Range: 1-31 Characters)

ACL Type: IPv4 ▼

ACL Rule Configuration

ACL Name - ACL Type: User1 - IPv4 ▼

Rule: New Rule ▼

Action: Deny ▼
Deny
Permit

Match Every Packet:

Protocol: Select From List: ip ▼ Match to Value: (Range: 0-255)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Le opzioni disponibili sono descritte come segue:

- Nega: blocca tutto il traffico che soddisfa i criteri della regola per l'ingresso o l'uscita dal dispositivo WAP.
- Autorizza: consente a tutto il traffico che soddisfa i criteri della regola di entrare o uscire dal dispositivo WAP.

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. Se si desidera configurare un criterio di corrispondenza specifico, deselegionare la casella di controllo *Corrispondenza ogni pacchetto*.

The screenshot shows the 'ACL Rule Configuration' window. At the top, 'ACL Name - ACL Type' is set to 'sample - IPv4' and 'Rule' is 'New Rule'. The 'Action' is 'Deny'. The 'Match Every Packet' checkbox is checked and highlighted with a red circle. Below it, the 'Protocol' is set to 'ip'. Other fields like 'Source IP Address', 'Destination IP Address', 'Source Port', and 'Destination Port' are present but not selected. At the bottom, there is a 'Save' button and a 'Delete ACL' checkbox.

Timesaver: Se si seleziona la casella di controllo *Corrispondenza ogni pacchetto*, andare al [punto 13](#).

Passaggio 5. (Facoltativo) Selezionare la casella di controllo *Protocollo* per la condizione di corrispondenza del protocollo L3 o L4 in base al valore del campo Protocollo IP nei pacchetti IPv4. Se la casella di controllo *Protocollo* è selezionata, fare clic su uno di questi pulsanti di opzione.

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range:)

Source IP Address: (xxx.xxx.xxx) Wild Card Mask:

Source Port: Select From List: Match to Port: (Range:)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port: Select From List: Match to Port: (Range:)

Service Type

IP DSCP: Select From List: Match to Value: (Range:)

Le opzioni sono descritte come segue:

- Select From List: consente di scegliere un protocollo dall'elenco a discesa *Select From List*. L'elenco a discesa contiene i protocolli ip, icmp, igmp, tcp, udp.
- Corrispondenza con valore - per il protocollo non presente nell'elenco. Immettere un ID di protocollo standard assegnato da IANA compreso tra 0 e 255.

Passaggio 6. (Facoltativo) Selezionare la casella di controllo *Source IP Address* (Indirizzo IP di origine) per includere un indirizzo IP dell'origine nella condizione di corrispondenza. Immettere l'indirizzo IP e la *maschera con caratteri jolly* dell'origine nei rispettivi campi. La wildcard mask consente di specificare a quale host dell'indirizzo IP di origine viene applicato questo elenco degli accessi.

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range: 0 - 255)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx)

Source Port: Select From List: Match to Port: (Range: 0 - 65535)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx)

Destination Port: Select From List: Match to Port: (Range: 0 - 65535)

Service Type

IP DSCP: Select From List: Match to Value: (Range: 0 - 63)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range: 0 - 255)

Delete ACL:

Passaggio 7. (Facoltativo) Selezionare la casella di controllo **Porta di origine** per includere una porta di origine nella condizione di corrispondenza. Se la casella di controllo *Porta di origine* è selezionata, fare clic su uno di questi pulsanti di opzione.

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range: 0 - 255)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx)

Source Port: Select From List: Match to Port: (Range: 0 - 65535)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask: (xxx.xxx.xxx.xxx)

Destination Port: Select From List: Match to Port: (Range: 0 - 65535)

Service Type

IP DSCP: Select From List: Match to Value: (Range: 0 - 63)

IP Precedence: (Range: 0 - 7)

·Seleziona dall'elenco — Scegliere una porta di origine dall'elenco a discesa *Seleziona da elenco*. L'elenco a discesa contiene le porte ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

ACL Rule Configuration

ACL Name - ACL Type:

Rule:

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range: 0 - 255)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port: Select From List: Match to Port: (Range: 0 - 65535)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port: Select From List: Match to Port: (Range: 0 - 65535)

·Corrispondenza con porta - per la porta di origine non presente nell'elenco. Immettere il numero di porta compreso tra 0 e 65535.

Passaggio 8. (Facoltativo) Selezionare la casella di controllo *Indirizzo IP di destinazione* per includere l'indirizzo IP della destinazione nella condizione di corrispondenza. Immettere l'indirizzo IP e la *maschera con caratteri jolly* della destinazione nei rispettivi campi. La wildcard mask consente di specificare a quale host dell'indirizzo IP di destinazione applicare questo elenco degli accessi.

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range: 0 - 255)

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port: Select From List: Match to Port: (Range: 0 - 65535)

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port: Select From List: Match to Port: (Range: 0 - 65535)

Service Type

IP DSCP: Select From List: Match to Value: (Range: 0 - 63)

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range: 00 - FF)

Delete ACL:

Passaggio 9. (Facoltativo) Selezionare la casella di controllo **Porta di destinazione** per includere una porta di destinazione nella condizione di corrispondenza. Se la casella di controllo *Porta di destinazione* è selezionata, fare clic su uno di questi pulsanti di opzione.

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range:

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port: Select From List: Match to Port: (Range:

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port: Select From List: Match to Port: (Range:

Service Type

IP DSCP: Select From List: Match to Value: (Range:

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range:

Delete ACL:

·Select From List (Seleziona dall'elenco) - Consente di scegliere una porta di destinazione dall'elenco a discesa *Select From List (Seleziona dall'elenco)*. L'elenco a discesa contiene le porte ftp, ftpdata, http, smtp, snmp, telnet, tftp, www.

Action:

Match Every Packet:

Protocol: Select From List: Match to Value: (Range:

Source IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Source Port: Select From List: Match to Port: (Range:

Destination IP Address: (xxx.xxx.xxx.xxx) Wild Card Mask:

Destination Port: Select From List: Match to Port: (Range:

Service Type

IP DSCP: Select From List: Match to Value: (Range:

IP Precedence: (Range: 0 - 7)

IP TOS Bits: (Range: 00 - FF) IP TOS Mask: (Range:

Delete ACL:

·Corrispondenza con porta - per la porta di destinazione non presente nell'elenco. Immettere il numero di porta compreso tra 0 e 65535 nel campo Corrispondenza con porta.

Nota: Solo uno dei servizi può essere selezionato dall'area *Tipo di servizio* e può essere aggiunto per la condizione di corrispondenza.

Passaggio 10. (Facoltativo) Selezionare la casella di controllo *IP DSCP* per trovare una corrispondenza con i pacchetti basati sui valori IP DSCP. Se la casella di controllo *IP DSCP* è selezionata, fare clic su uno di questi pulsanti di opzione. Il protocollo DSCP viene usato

per specificare le priorità del traffico sull'intestazione IP del frame. In questo modo tutti i pacchetti per il flusso di traffico associato vengono classificati con il valore IP DSCP selezionato dall'elenco. Per ulteriori informazioni su DSCP, fare riferimento [qui](#).

The screenshot shows the 'ACL Rule Configuration' window. The 'Service Type' section is highlighted, showing the 'IP DSCP' field set to 'af11'. A red box highlights a dropdown menu containing a list of DSCP values: af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs0, cs1, cs2, cs3, cs4, cs5, and cs6. The 'af11' value is selected.

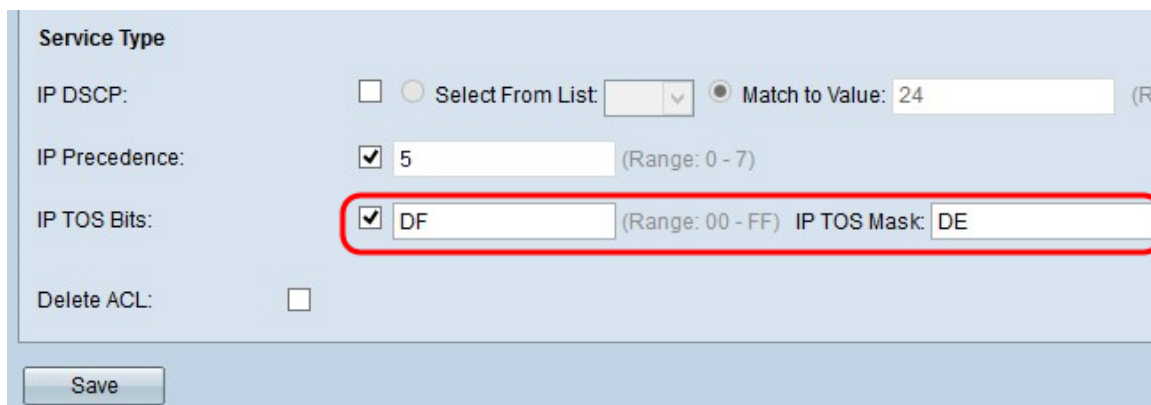
- Select From List (Seleziona da elenco) - Consente di scegliere un valore DSCP IP dall'elenco a discesa *Select From List (Seleziona da elenco)*. L'elenco a discesa contiene i valori DSCP Assured Forwarding (AS), Class of Service (CS) o Expedited Forwarding (EF).
- Corrispondenza con valore - Consente di personalizzare i valori DSCP. Immettere il valore DSCP compreso tra 0 e 63 nel campo Corrispondenza con valore.

Passaggio 11. (Facoltativo) Selezionare *la* casella di controllo *Precedenza IP* per includere un valore di Precedenza IP nella condizione di corrispondenza. Se la casella di controllo Precedenza IP è selezionata, inserire un valore di precedenza IP compreso tra 0 e 7. Per ulteriori informazioni su Precedenza IP, fare riferimento a [questo punto](#).

The screenshot shows the 'Service Type' section of the ACL configuration. The 'IP DSCP' field is set to 'Match to Value: 24'. The 'IP Precedence' field is checked and set to '5' (Range: 0 - 7), which is highlighted with a red box. The 'IP TOS Bits' field is checked and set to 'DF' (Range: 00 - FF). The 'Delete ACL' checkbox is unchecked.

Passaggio 12. (Facoltativo) Selezionare la casella di controllo *IP TOS Bits* (Bit del tipo di

servizio) per utilizzare i bit del pacchetto nell'intestazione IP come criteri di corrispondenza. Se la casella di controllo Bit IP TOS è selezionata, immettere i bit IP TOS compresi tra 00-FF e la maschera IP TOS compresa tra 00-FF nei campi corrispondenti.



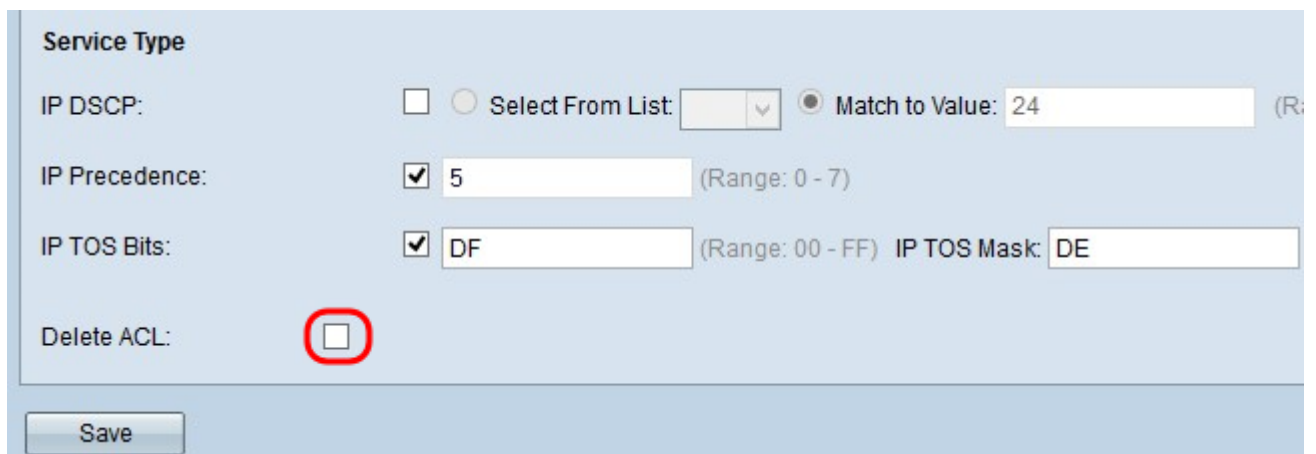
The screenshot shows a configuration form titled "Service Type". It contains the following fields and options:

- IP DSCP:** Select From List: Match to Value: (R)
- IP Precedence:** (Range: 0 - 7)
- IP TOS Bits:** (Range: 00 - FF) IP TOS Mask:
- Delete ACL:**

A red rectangle highlights the "IP TOS Bits" field, which is checked and contains the value "DF".

Save

[Passaggio 13](#). (Facoltativo) Se si desidera eliminare l'ACL configurato, selezionare la casella di controllo *Elimina ACL*.



The screenshot shows the same configuration form as above, but with the "Delete ACL" checkbox highlighted by a red circle.

The "Delete ACL" checkbox is currently unchecked.

Save

Passaggio 14. Fare clic su **Save** per salvare le impostazioni.