Configuration des règles de liste de contrôle d'accès sur le WAP371

Objectif

Une liste de contrôle d’accès au réseau (ACL) est une couche de sécurité facultative qui agit comme un pare-feu pour contrôler le trafic entrant et sortant d’un sous-réseau. Les listes d'accès sont des ensembles de conditions d'autorisation et de refus, ou règles, qui fournissent la sécurité pour plusieurs raisons. Par exemple, ces règles peuvent bloquer les utilisateurs non autorisés, autoriser les utilisateurs autorisés à accéder à des ressources spécifiques et bloquer toute tentative injustifiée d'atteindre des ressources réseau.

L'objectif de ce document est de vous montrer comment configurer les règles de liste de contrôle d'accès sur le WAP 371.

Périphériques pertinents

·WAP371

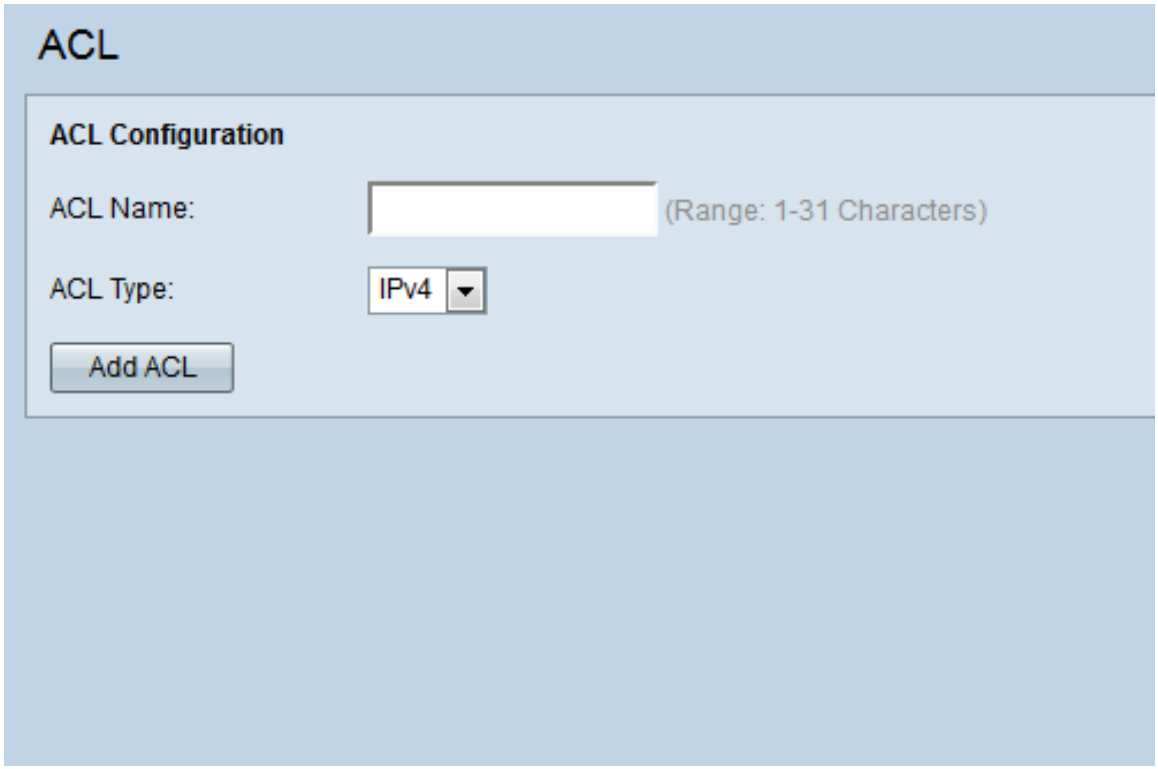
Version du logiciel

•v 1.2.0.2

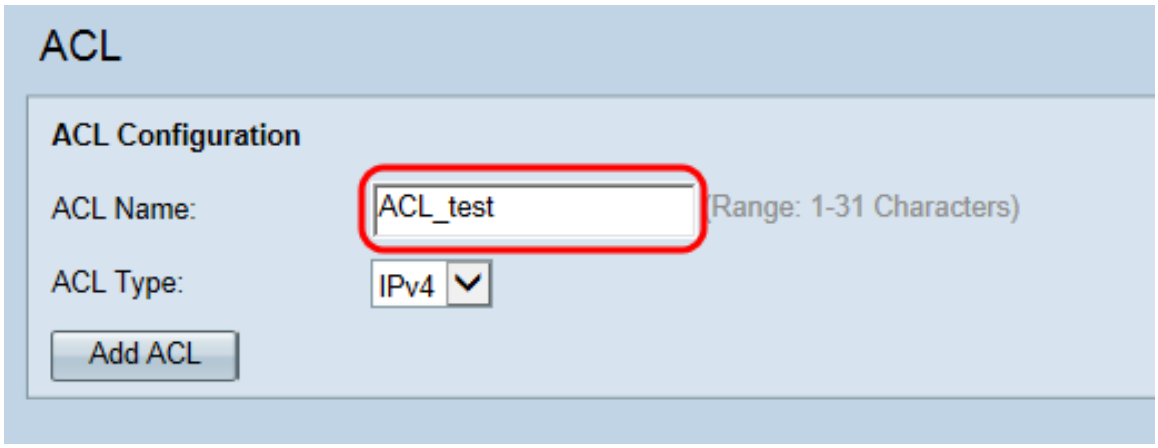
Configuration des règles ACL

Configuration ACL

Étape 1. Connectez-vous à l'utilitaire de configuration Web et choisissez **Client QoS > ACL**. La page *ACL* s'ouvre :

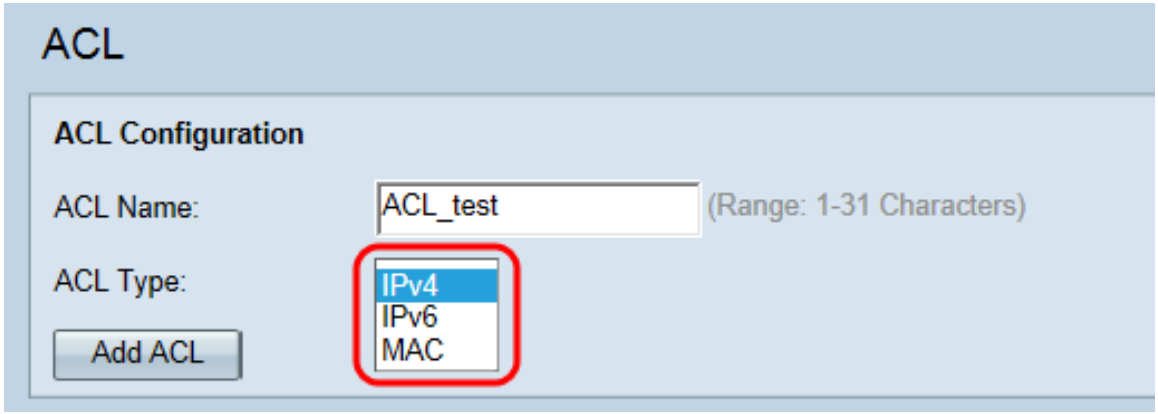


Étape 2. Entrez le nom de la liste de contrôle d'accès souhaité dans le champ *Nom de la liste de contrôle d'accès*. La plage est comprise entre 1 et 31 caractères.



Note: Le nom de la liste de contrôle d’accès est un identificateur de la liste de contrôle d’accès donnée ; elle n'a aucune incidence sur le fonctionnement du périphérique.

Étape 3. Sélectionnez le type de liste de contrôle d'accès dans la liste déroulante *Type de liste de contrôle d'accès*.



Les options sont les suivantes :

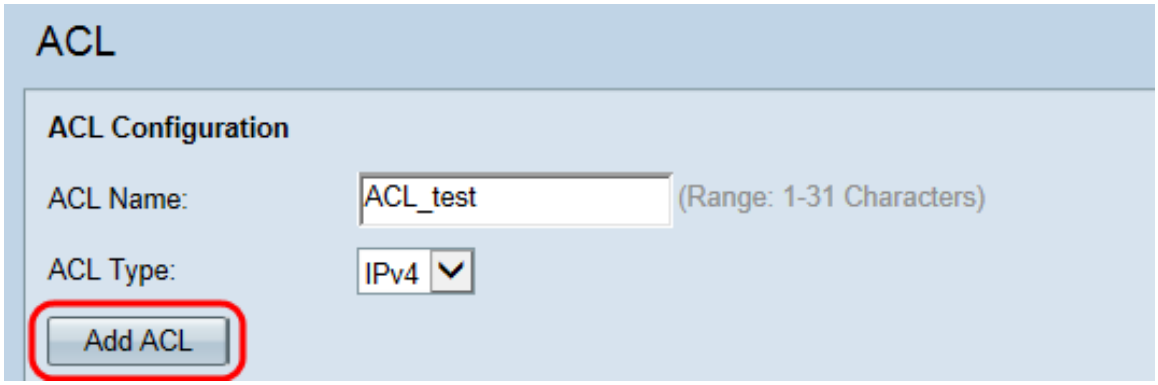
·IPv4 : adresse 32 bits (quatre octets).

·IPv6 : successeur d'IPv4, se compose d'une adresse de 128 bits (8 octets).

·MAC : adresse MAC unique attribuée à une interface réseau.

Note: Les listes de contrôle d'accès IPv4 et IPv6 contrôlent l'accès aux ressources réseau en fonction des critères des couches 3 et 4. Les listes de contrôle d'accès MAC contrôlent l'accès en fonction des critères de couche 2.

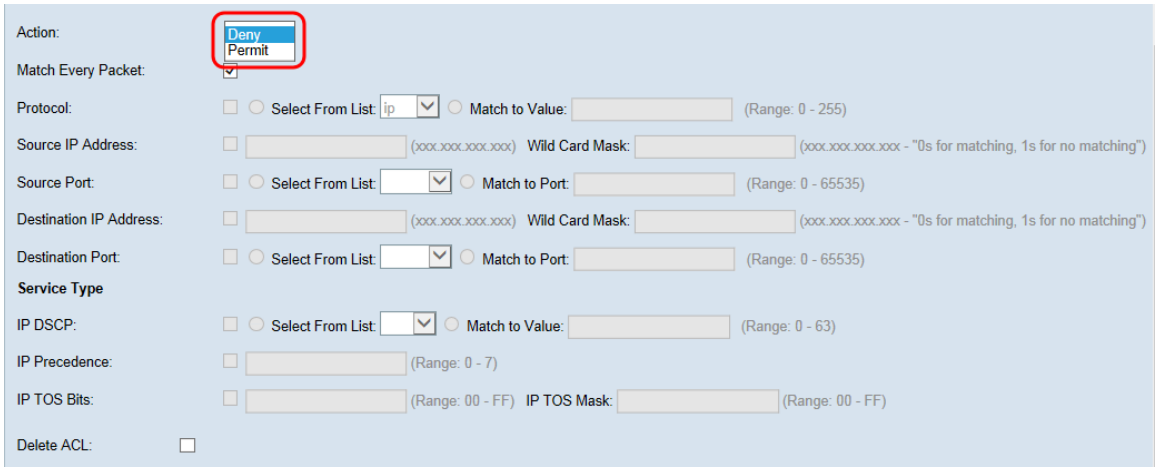
Étape 4. Cliquez sur **Add ACL** pour ajouter la nouvelle ACL.



Configuration des règles de liste de contrôle d'accès pour IPv4 et IPv6

Note: Les captures d'écran suivantes concernent les règles de liste de contrôle d'accès IPv4 mais sont interchangeables avec les règles de liste de contrôle d'accès IPv6.

Étape 1. Sélectionnez une action pour la règle dans la liste déroulante *Action*.

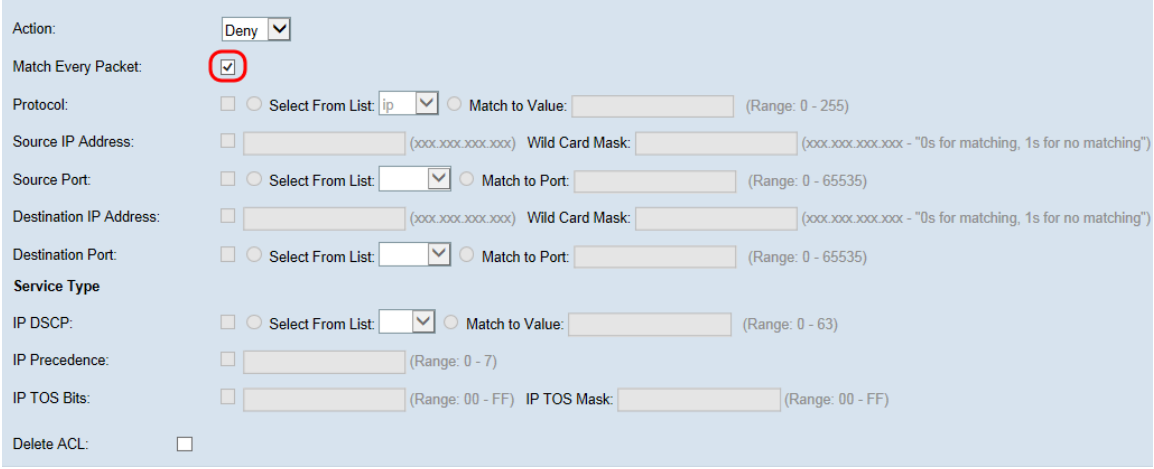


Les options sont décrites comme suit :

·Autoriser : la règle autorise tout le trafic qui satisfait aux critères de la règle à entrer ou à quitter le périphérique WAP. Le trafic qui ne répond pas aux critères est abandonné.

·Refuser : la règle empêche tout trafic répondant aux critères de la règle d'entrer ou de sortir du périphérique WAP. Le trafic qui ne répond pas aux critères est transféré à la règle suivante. S'il s'agit de la règle finale, le trafic qui n'est pas explicitement autorisé est abandonné.

Étape 2. Cochez ou décochez la case **Correspondance de chaque paquet**. Si cette option est sélectionnée, la règle, qui comporte une action d'autorisation ou de refus, correspond à la trame ou au paquet, quel que soit son contenu.



Note: Si vous sélectionnez ce champ, vous ne pouvez pas configurer de critères de correspondance supplémentaires. L'option **Correspondre à chaque paquet** est sélectionnée par défaut pour une nouvelle règle. Vous devez désactiver l'option pour configurer d'autres champs de correspondance.

Étape 3. Cochez la case **Protocol** pour utiliser une condition de correspondance de protocole de couche 3 ou de couche 4 en fonction de la valeur du champ IP Protocol dans les paquets IPv4 ou du champ Next Header dans les paquets IPv6. Si la case Protocole est cochée, sélectionnez l'une des cases d'option suivantes.

Les options sont décrites comme suit :

·Sélectionner dans la liste : sélectionnez un protocole dans la liste déroulante *Sélectionner dans la liste*. Les options sont les suivantes :

- IP : le protocole IP (Internet Protocol) est le principal protocole de communication de la suite de protocoles Internet pour le relais de données sur les réseaux.

- ICMP : le protocole ICMP (Internet Control Message Protocol) est un protocole de la suite de protocoles Internet utilisé par des périphériques tels que des routeurs pour envoyer des messages d'erreur.

- IGMP : le protocole IGMP (Internet Group Management Protocol) est un protocole de communication utilisé par l'hôte pour établir des appartenances de groupe de multidiffusion sur des réseaux IPv4.

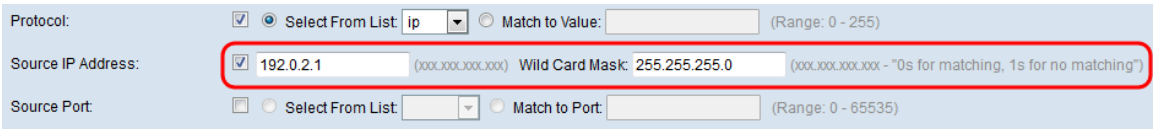
- TCP : le protocole TCP (Transmission Control Protocol) permet à deux hôtes d'établir une connexion et d'échanger des flux de données.

- UDP : le protocole de datagramme utilisateur est un protocole de la suite de protocoles Internet qui utilise un modèle de transmission sans connexion.

·Match to Value : saisissez un ID de protocole attribué à l'IANA standard, compris entre 0 et

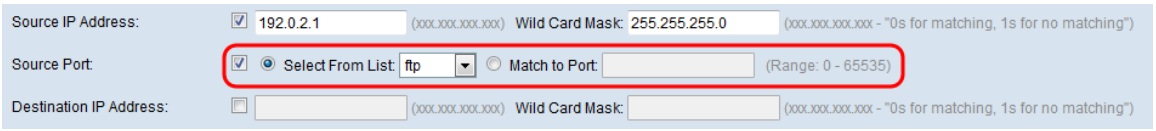
255 pour tous les protocoles non répertoriés. Référez-vous à *Numéros de protocole Internet attribués* pour plus d'informations sur les ID de protocole attribués à IANA.

Étape 4. Cochez la case **Adresse IP source** pour inclure une adresse IP de la source dans la condition de correspondance. Saisissez l'adresse IP et le masque générique de la source dans leurs champs respectifs. Le masque générique détermine quels bits de l'adresse source sont utilisés et lesquels sont ignorés. Il peut être considéré comme un masque de sous-réseau inversé. Cela permet d'indiquer la taille d'un réseau ou d'un sous-réseau pour certains protocoles de routage ou d'autoriser ou de refuser une plage d'adresses IP.



Note: Le champ Masque de carte générique est obligatoire si la case **Adresse IP source** est cochée.

Étape 5. Cochez la case **Port source** pour inclure un port source dans la condition de correspondance. Si la case **Port source** est cochée, sélectionnez l'un des boutons d'option suivants.



Les options sont décrites comme suit :

·Sélectionner dans la liste — Choisissez un port source dans la liste déroulante *Sélectionner dans la liste*. Les options sont les suivantes :

- FTP : le protocole FTP (File Transfer Protocol) est un protocole réseau standard utilisé pour transférer des fichiers d'un hôte à un autre sur un réseau TCP tel qu'Internet.

- Données FTP : canal de données initié par le serveur connecté à un client, généralement via le port 20.

- HTTP : le protocole HTTP (Hypertext Transfer Protocol) est un protocole d'application qui constitue la base de la communication de données pour le World Wide Web.

- SMTP - Le protocole SMTP (Simple Mail Transfer Protocol) est une norme Internet de transmission de courrier électronique (courriel).

- SNMP : le protocole SNMP (Simple Network Management Protocol) est un protocole standard Internet permettant de gérer les périphériques sur les réseaux IP.

- Telnet : protocole de couche session utilisé sur Internet ou sur les réseaux locaux pour fournir une communication bidirectionnelle interactive textuelle.

- TFTP - Le protocole TFTP (Trivial File Transfer Protocol) est un utilitaire logiciel Internet permettant de transférer des fichiers plus simples à utiliser que le protocole FTP mais moins capables.

- WWW - Le World Wide Web est un système de serveurs Internet qui prend en charge les documents formatés HTTP.

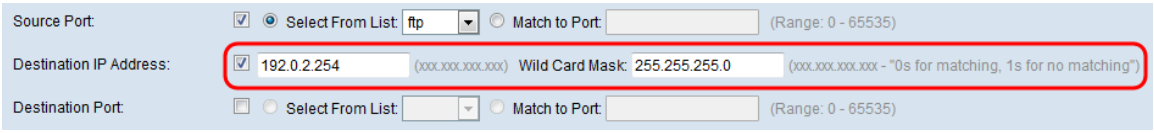
Correspondance au port : saisissez le numéro de port compris entre 0 et 65 535 dans le champ *Correspondance au port* pour les ports source non répertoriés. La plage comprend trois types de ports différents. Les plages sont décrites comme suit :

- 0 à 1023 — Ports réservés.

- 1024 à 49151 — Ports enregistrés.

- 49152 à 65535 — Ports dynamiques et/ou privés.

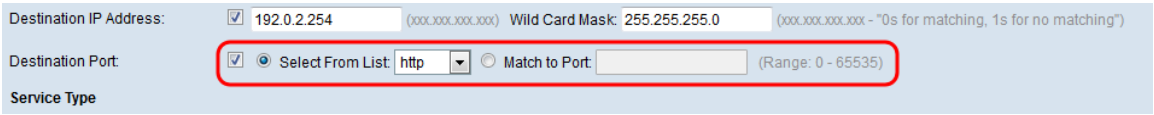
Étape 6. Cochez la case **Adresse IP de destination** pour inclure l'adresse IP de destination dans la condition de correspondance. Saisissez l'adresse IP et le masque générique de la destination dans leurs champs respectifs. Le masque générique détermine quels bits de l'adresse source sont utilisés et lesquels sont ignorés. Il peut être considéré comme un masque de sous-réseau inversé. Cela permet d'indiquer la taille d'un réseau ou d'un sous-réseau pour certains protocoles de routage ou d'autoriser ou de refuser une plage d'adresses IP.



Note: Le champ *Masque de carte générique* est obligatoire si la case **Adresse IP de destination** est cochée.

Note: Si vous souhaitez ne faire correspondre qu'une seule adresse IP, utilisez le masque générique 0.0.0.0.

Étape 7. Cochez la case **Port de destination** pour inclure un port de destination dans la condition de correspondance. Si la case **Port de destination** est cochée, sélectionnez l'une des cases d'option suivantes.



Les options sont décrites comme suit :

·Sélectionner dans la liste — Choisissez un port de destination dans la liste déroulante *Sélectionner dans la liste*. Les options de la liste déroulante sont les suivantes :

- FTP : le protocole FTP (File Transfer Protocol) est un protocole réseau standard utilisé pour transférer des fichiers d'un hôte à un autre sur un réseau TCP tel qu'Internet.

- Données FTP : canal de données initié par le serveur connecté à un client, généralement via le port 20.

- HTTP : le protocole HTTP (Hypertext Transfer Protocol) est un protocole d'application qui constitue la base de la communication de données pour le World Wide Web.

- SMTP - Le protocole SMTP (Simple Mail Transfer Protocol) est une norme Internet de transmission de courrier électronique (courriel).

- SNMP : le protocole SNMP (Simple Network Management Protocol) est un protocole standard Internet permettant de gérer les périphériques sur les réseaux IP.

- Telnet : protocole de couche session utilisé sur Internet ou sur les réseaux locaux pour fournir une communication bidirectionnelle interactive textuelle.

- TFTP - Le protocole TFTP (Trivial File Transfer Protocol) est un utilitaire logiciel Internet permettant de transférer des fichiers plus simples à utiliser que le protocole FTP mais moins capables.

- WWW - Le World Wide Web est un système de serveurs Internet qui prend en charge les documents formatés HTTP.

Correspondance au port : saisissez le numéro de port compris entre 0 et 65 535 dans le champ *Correspondance au port* pour les ports de destination non répertoriés. La plage comprend trois types de ports différents. Les plages sont décrites comme suit :

- 0 à 1023 — Ports réservés.

- 1024 à 49151 — Ports enregistrés.

- 49152 à 65535 — Ports dynamiques et/ou privés.

Note: Un seul des services peut être sélectionné dans la zone Type de service et peut être ajouté pour la condition de correspondance.

Configuration du type de service de règle ACL pour IPv4

Étape 1. Cochez la case **IP DSCP** pour qu'elle corresponde aux paquets basés sur les valeurs IP DSCP. DSCP est utilisé pour spécifier les priorités de trafic sur l'en-tête IP de la trame. Ceci classe tous les paquets pour le flux de trafic associé avec la valeur IP DSCP que vous sélectionnez dans la liste. Si la case IP DSCP est cochée, sélectionnez l'une des cases d'option suivantes.

Les options sont décrites comme suit :

·Select From List : sélectionnez une valeur DSCP IP dans la liste déroulante *Select From List*. Les options sont les suivantes :

- DSCP Asened Forwarding (AS) - Permet à l'opérateur de fournir une assurance de livraison tant que le trafic ne dépasse pas un certain débit d'abonnement.

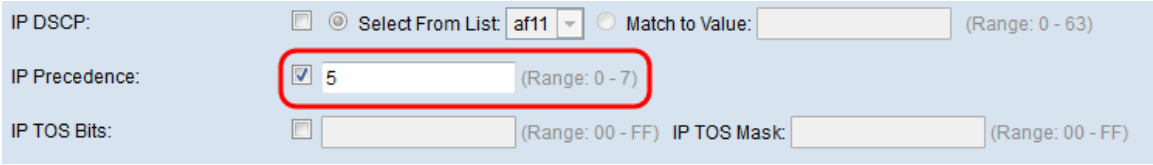
- Classe de service (CS) - Permet la rétrocompatibilité avec les périphériques réseau qui utilisent toujours le champ Priorité.

- Transmission accélérée (EF) : utilisée pour créer un service de bout en bout avec des domaines DS (DiffServ) à faible perte, faible latence, faible gigue, bande passante garantie.

·faire correspondre à la valeur : saisissez la valeur DSCP comprise entre 0 et 63 dans le champ *Correspondance à la valeur* pour personnaliser les valeurs DSCP.

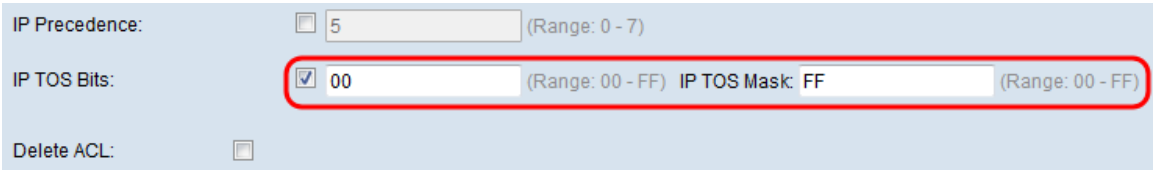
Note: Référez-vous à *Valeurs DSCP et de priorité* pour plus de détails sur DSCP.

Étape 2. Cochez la case **Priorité IP** pour inclure une valeur Priorité IP dans la condition de correspondance. Il s'agit d'un mécanisme permettant d'attribuer une priorité à chaque paquet IP où 0 est la priorité la plus basse et 7 la priorité la plus élevée. Si la case **Priorité IP** est cochée, entrez une valeur de priorité IP comprise entre 0 et 7.



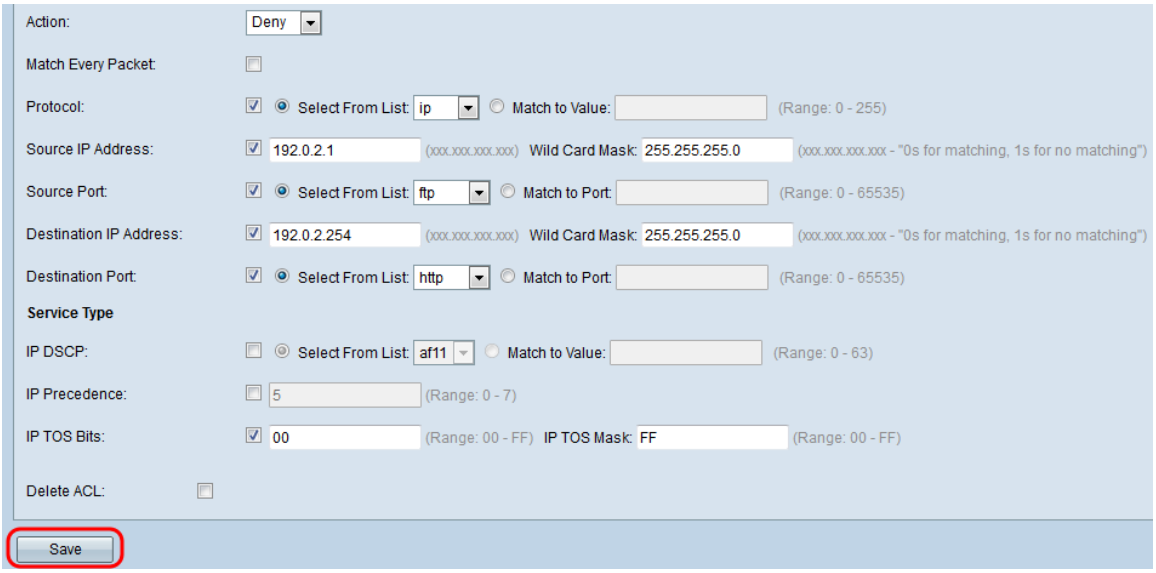
Note: Référez-vous à *Valeurs DSCP et de priorité* pour plus de détails sur la priorité IP.

Étape 3. Cochez la case **Bits TOS IP** pour utiliser les bits TOS (Type of Service) du paquet dans l'en-tête IP comme critères de correspondance. Un champ TOS est utilisé pour spécifier la priorité d'un datagramme et l'acheminer en conséquence. Si la case à cocher IP TOS Bits est cochée, saisissez les bits IP TOS compris entre 00-FF et le masque IP TOS compris entre 00-FF dans leurs champs respectifs.



Étape 4. (Facultatif) Si vous voulez supprimer la liste de contrôle d'accès configurée, cochez la case **Supprimer la liste de contrôle d'accès**.

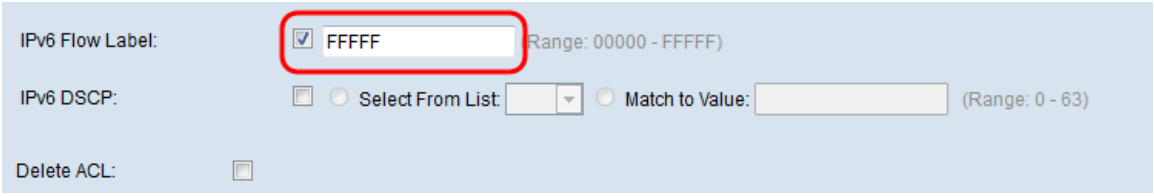
Étape 5. Cliquez sur Save pour enregistrer les paramètres.



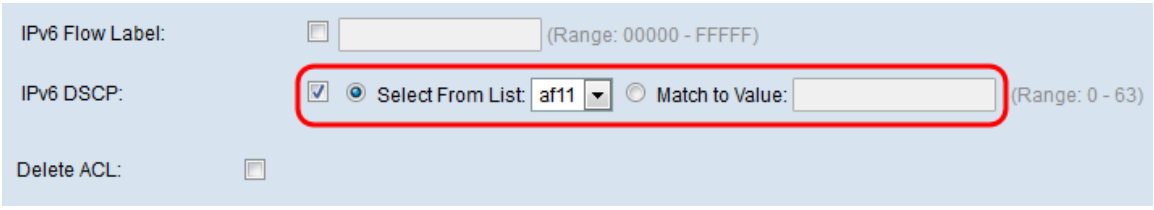
Configuration des règles de liste de contrôle d'accès pour IPv6

Étape 1. Cochez la case **Étiquette de flux IPv6** pour définir un nombre de 20 bits unique à un

paquet IPv6. Il est utilisé par les stations d'extrémité pour indiquer la gestion de la qualité de service dans les routeurs (plage 0 à 1048575).



Étape 2. Cochez la case **DSCP IPv6** pour qu'elle corresponde aux paquets basés sur les valeurs DSCP IP. DSCP est utilisé pour spécifier les priorités de trafic sur l'en-tête IP de la trame. Ceci classe tous les paquets pour le flux de trafic associé avec la valeur IP DSCP que vous sélectionnez dans la liste. Si la case **IPv6 DSCP** est cochée, sélectionnez l'une des cases d'option suivantes.



Les options sont décrites comme suit :

·Select From List : sélectionnez une valeur DSCP IP dans la liste déroulante *Select From List*. Les options sont les suivantes :

- DSCP Asened Forwarding (AS) - permet à l'opérateur de fournir une assurance de livraison tant que le trafic ne dépasse pas un certain débit d'abonnement.

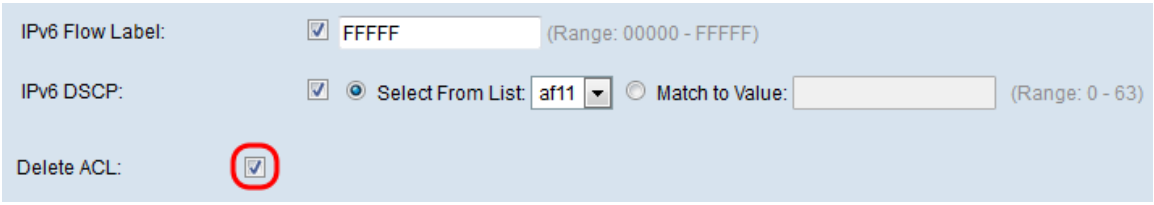
- Classe de service (CS) : permet la rétrocompatibilité avec les périphériques réseau qui utilisent toujours le champ Priorité.

- Transmission accélérée (EF) - Permet de créer un service de bout en bout avec des domaines DS (DiffServ) à faible perte, faible latence, faible gigue, bande passante garantie.

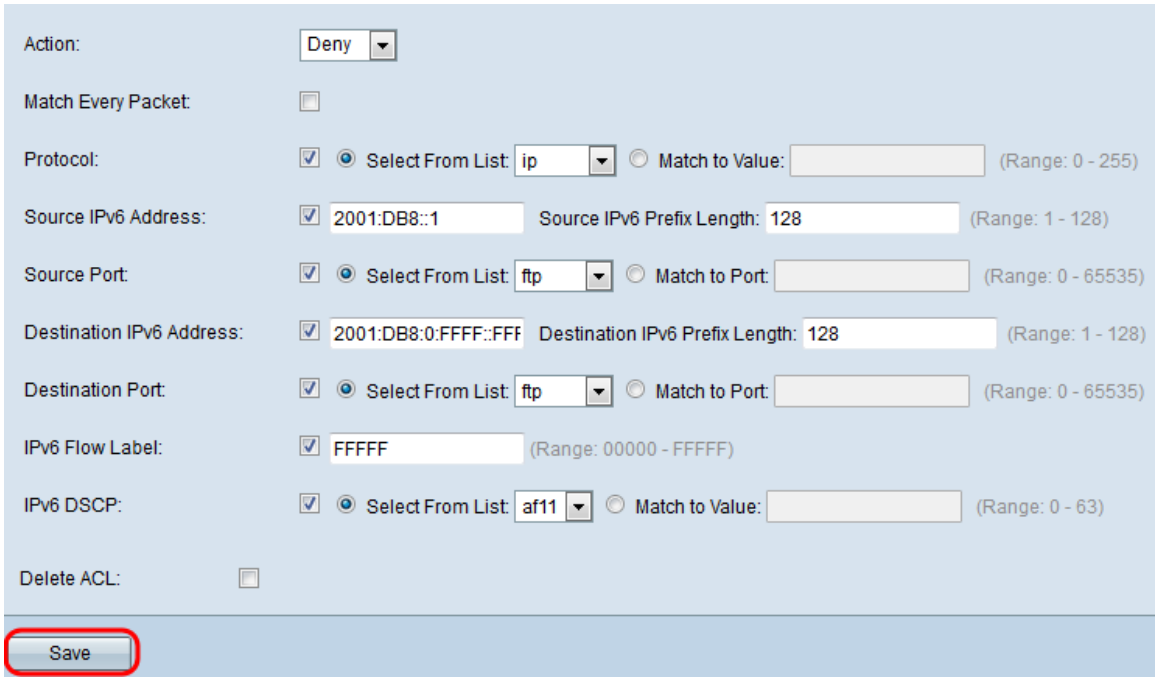
·faire correspondre à la valeur : saisissez la valeur DSCP comprise entre 0 et 63 dans le champ *Correspondance à la valeur* pour personnaliser les valeurs DSCP.

Note: Référez-vous à *Valeurs DSCP et de priorité* pour plus de détails sur DSCP.

Étape 3. (Facultatif) Si vous voulez supprimer la liste de contrôle d'accès configurée, cochez la case **Supprimer la liste de contrôle d'accès**.

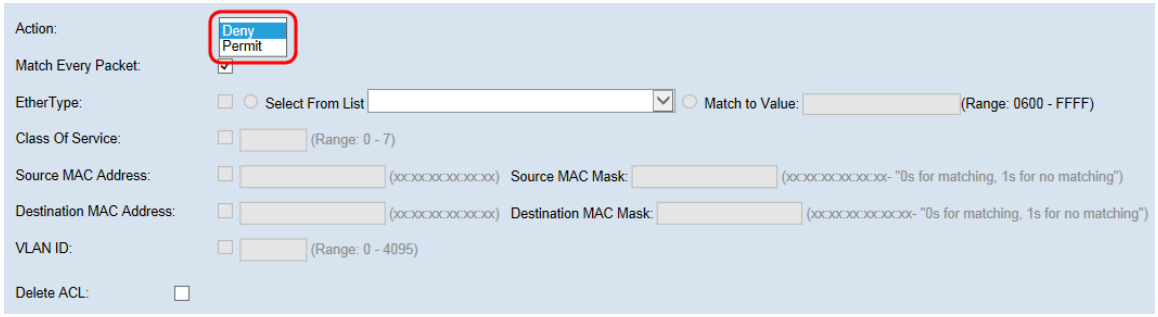


Étape 4. Cliquez sur **Save** pour enregistrer les paramètres.



Configuration des règles ACL pour MAC

Étape 1. Sélectionnez une action pour la règle dans la liste déroulante *Action*.

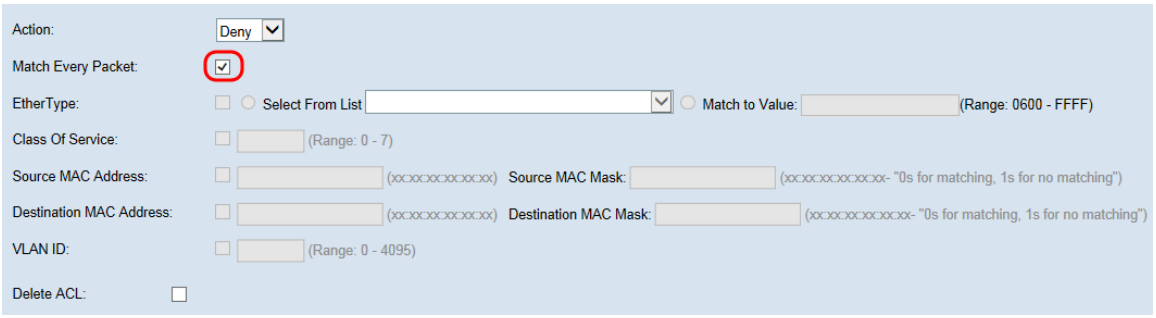


Les options sont décrites comme suit :

·Autoriser : la règle autorise tout le trafic qui satisfait aux critères de la règle à entrer ou à quitter le périphérique WAP. Le trafic qui ne répond pas aux critères est abandonné.

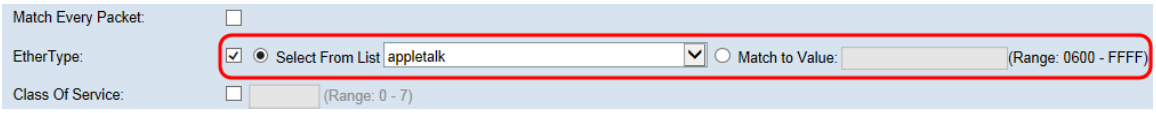
·Refuser : la règle empêche tout trafic répondant aux critères de la règle d'entrer ou de sortir du périphérique WAP. Le trafic qui ne répond pas aux critères est transféré à la règle suivante. S'il s'agit de la règle finale, le trafic qui n'est pas explicitement autorisé est abandonné.

Étape 2. Cochez ou décochez la case **Correspondance de chaque paquet**. Si cette option est sélectionnée, la règle, qui comporte une action d'autorisation ou de refus, correspond à la trame ou au paquet, quel que soit son contenu.



Note: Si vous sélectionnez ce champ, vous ne pouvez pas configurer de critères de correspondance supplémentaires. L'option **Correspondre à chaque paquet** est sélectionnée par défaut pour une nouvelle règle. Vous devez désactiver l'option pour configurer d'autres champs de correspondance.

Étape 3. Cochez la case **Type d'ther** pour comparer les critères de correspondance avec la valeur de l'en-tête d'une trame Ethernet. Si la case à cocher **Type Ether** est activée, sélectionnez l'une des cases d'option suivantes.



Les options sont décrites comme suit :

Sélectionner dans la liste : sélectionnez un protocole dans la liste déroulante *Sélectionner dans la liste*. Les options sont les suivantes :

- AppleTalk - AppleTalk est une suite propriétaire de protocoles réseau développés par Apple Inc. pour leurs ordinateurs Macintosh. AppleTalk inclut un certain nombre de fonctionnalités qui permettent aux réseaux locaux d'être connectés sans configuration préalable ou la nécessité d'un routeur ou serveur centralisé de toute sorte.

- ARP : le protocole ARP (Address Resolution Protocol) est un protocole de télécommunication utilisé pour la résolution des adresses de couche réseau en adresses de couche liaison, une fonction essentielle dans les réseaux à accès multiple.

- IPv4 - Le protocole IP version 4 (IPv4) est la quatrième version du développement du protocole Internet (IP). Il s'agit de l'un des principaux protocoles des méthodes d'interconnexion de réseaux normalisées sur Internet.

- IPv6 : le protocole IP version 6 (IPv6) est la version la plus récente du protocole IP (Internet Protocol), le protocole de communication qui fournit un système d'identification et de localisation pour les ordinateurs sur les réseaux et achemine le trafic sur Internet.

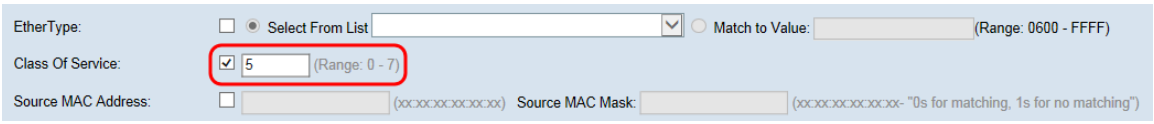
- IPX - IPX (Internetwork Packet Exchange) est le protocole de couche réseau de la suite de protocoles IPX/SPX. IPX est dérivé du PCI de Xerox Network Systems. Il peut également servir de protocole de couche transport.

- NetBIOS - NetBIOS est un acronyme pour Network Basic Input/Output System. Il fournit des services liés à la couche session du modèle OSI, permettant aux applications sur des ordinateurs distincts de communiquer sur un réseau local. En tant qu'API, NetBIOS n'est pas un protocole réseau.

- PPPOE - Le protocole PPPoE (Point-to-Point Protocol over Ethernet) est un protocole réseau permettant d'encapsuler des trames PPP dans des trames Ethernet.

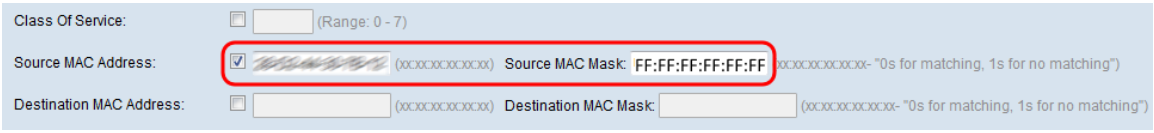
·Match to Value : saisissez un identificateur de protocole personnalisé auquel les paquets correspondent. La valeur est un nombre hexadécimal à quatre chiffres compris entre 0600 et FFFF.

Étape 4. Cochez la case **Classe de service** pour saisir une priorité utilisateur 802.1p à comparer à une trame Ethernet. Comme la priorité IP, 0 est la priorité la plus basse et 7 la priorité la plus élevée. La plage valide est comprise entre 0 et 7.

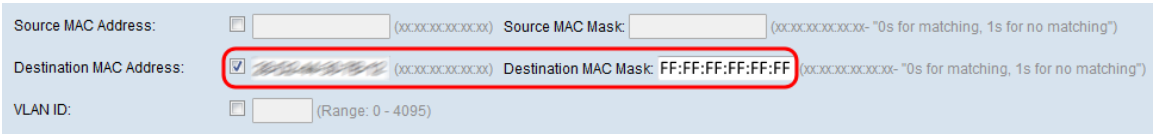


Étape 5. Cochez la case **Adresse MAC source** pour entrer une adresse MAC source à comparer à une trame Ethernet. Si la case Adresse MAC source est cochée, entrez l'adresse MAC source dans le champ *Adresse MAC source*. Saisissez ensuite le masque d'adresse MAC source dans le champ *Masque MAC source*. Cela spécifie quels bits de l'adresse MAC source seront comparés à une trame Ethernet.

Note: Si vous souhaitez ne faire correspondre qu'une seule adresse MAC, utilisez le masque générique 00:00:00:00:00:00.

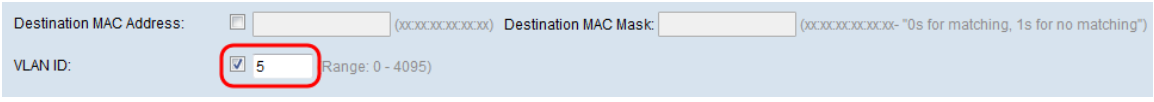


Étape 6. Cochez la case **Adresse MAC de destination** pour entrer une adresse MAC de destination à comparer à une trame Ethernet. Si la case Adresse MAC de destination est cochée, entrez l'adresse MAC de destination dans le champ *Adresse MAC de destination*. Entrez ensuite le masque d'adresse MAC dans le champ *Masque MAC de destination*. Cela spécifie quels bits de l'adresse MAC de destination seront comparés à une trame Ethernet.

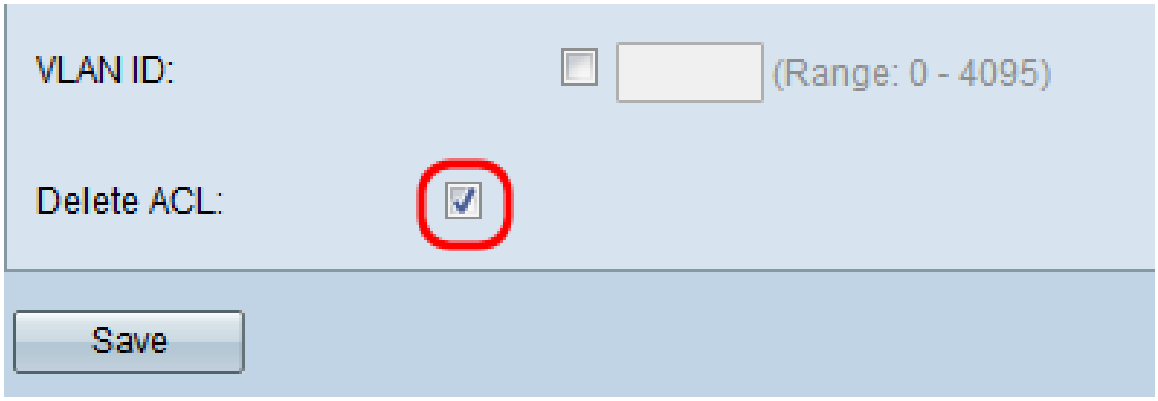


Note: Si vous souhaitez ne faire correspondre qu'une seule adresse MAC, utilisez le masque générique 00:00:00:00:00:00.

Étape 7. Cochez la case **ID VLAN** pour entrer un ID VLAN à comparer à une trame Ethernet. Si la case **ID VLAN** est cochée, entrez l'ID VLAN dans le champ *ID VLAN*. La plage d'ID de VLAN est comprise entre 0 et 4 095.



Étape 8. (Facultatif) Si vous voulez supprimer la liste de contrôle d'accès configurée, cochez la case **Supprimer la liste de contrôle d'accès**.



Étape 9. Cliquez sur **Save pour enregistrer les paramètres.**