Configuration des listes de contrôle d'accès IPv4 et IPv6 sur les points d'accès WAP551 et WAP561

Objectif

Les listes de contrôle d'accès (ACL) sont des ensembles de conditions d'autorisation et de refus, appelées règles, qui fournissent la sécurité nécessaire pour bloquer les utilisateurs non autorisés et autoriser les utilisateurs autorisés à accéder à des ressources spécifiques. Les listes de contrôle d'accès peuvent bloquer toute tentative injustifiée d'atteindre les ressources réseau. La fonctionnalité QoS contient la prise en charge des services différenciés (DiffServ) qui permet de classer le trafic en flux et de lui attribuer un traitement QoS en fonction des comportements définis par saut.

Cet article explique comment créer et configurer une liste de contrôle d'accès IPv4 et IPv6 sur les points d'accès WAP551 et WAP561.

Périphériques pertinents

·WAP551
· WAP561

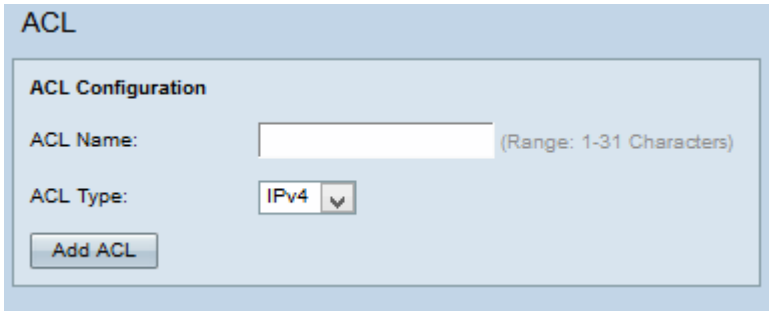
Version du logiciel

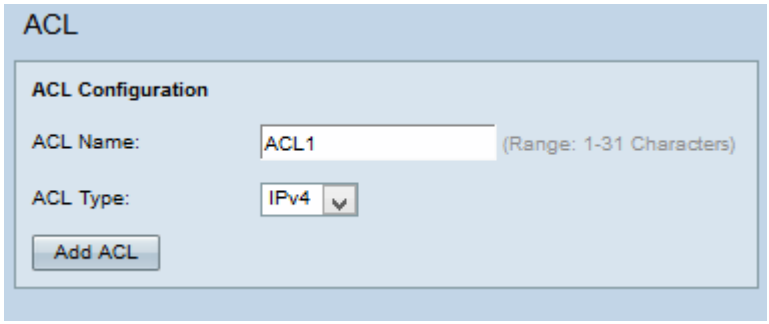
•v 1.0.4.2

Configuration ACL

Les listes de contrôle d'accès IP classent le trafic de couche 3 dans la pile IP. Chaque liste de contrôle d'accès est un ensemble de 10 règles maximum appliquées au trafic envoyé par un client sans fil ou à recevoir par un client sans fil. Chaque règle spécifie si le contenu d'un champ donné doit être utilisé pour autoriser ou refuser l'accès au réseau. Les règles peuvent être basées sur différents critères et peuvent s'appliquer à un ou plusieurs champs d'un paquet, tels que l'adresse IP source ou de destination, le port source ou de destination ou le protocole transporté dans le paquet.

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





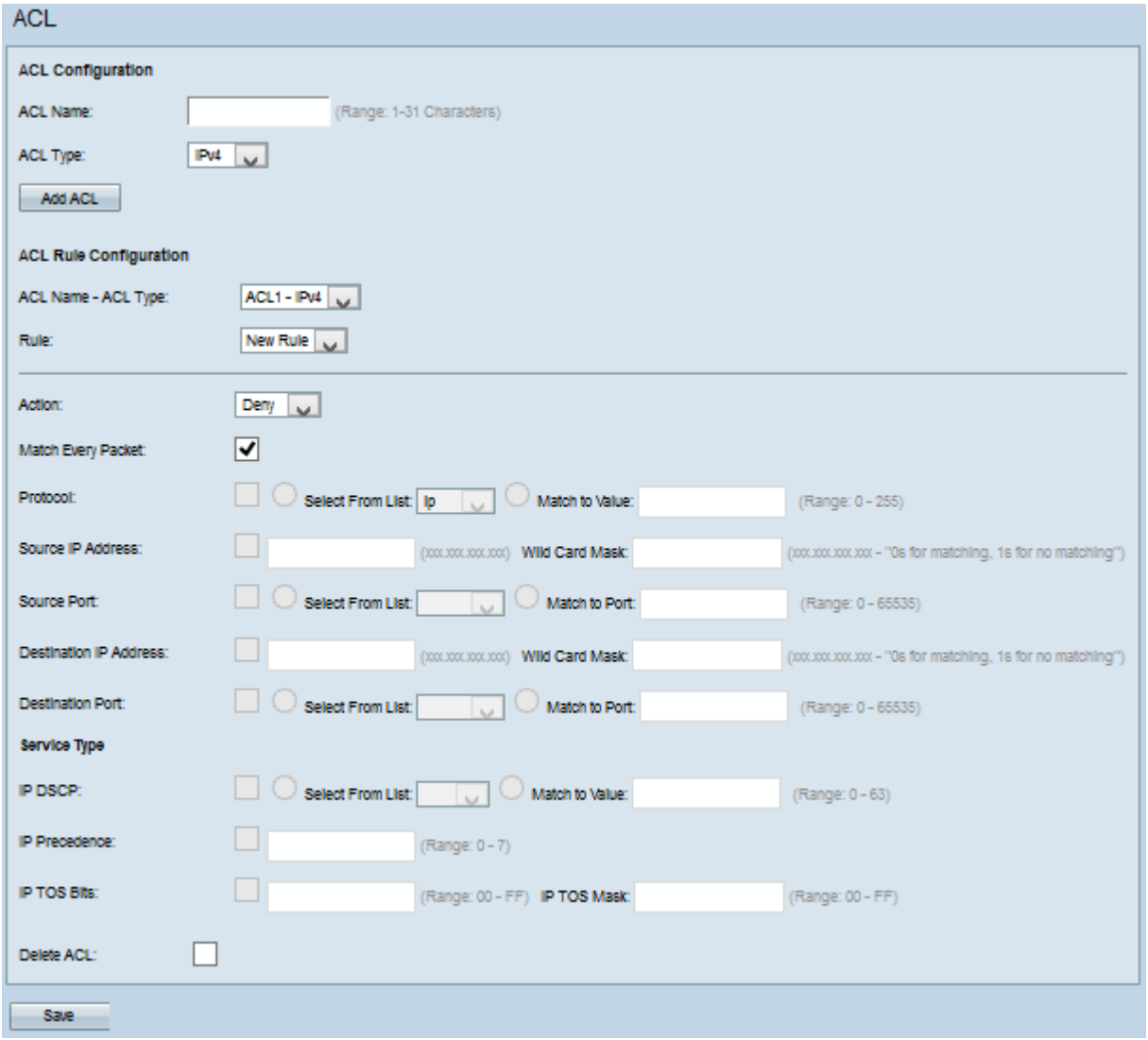
Étape 2. Saisissez le nom de la liste de contrôle d'accès dans le champ ACL Name.

Étape 3. Sélectionnez le type de liste de contrôle d'accès souhaité dans la liste déroulante Type de liste de contrôle d'accès. Si IPv6 est sélectionné, reportez-vous à la section *Configuration de la liste de contrôle d'accès IPv6*. Si la liste de contrôle d'accès basée sur MAC est choisie dans la liste déroulante Type de liste de contrôle d'accès, reportez-vous à l'article *Configuration de la liste de contrôle d'accès basée sur MAC (ACL) sur les points d'accès WAP551 et WAP561*.

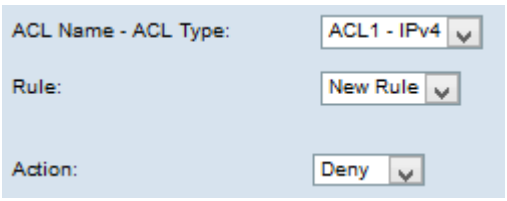
Étape 4. Cliquez sur **Add ACL** pour créer une liste de contrôle d'accès.

Configuration de la liste de contrôle d'accès IPv4

Note: Si IPv4 est sélectionné dans la liste déroulante Type de liste de contrôle d'accès, suivez les étapes ci-dessous pour configurer les règles de liste de contrôle d'accès IPv4.



Étape 1. Sélectionnez la liste de contrôle d'accès créée dans la liste déroulante Nom de la liste de contrôle d'accès - Type de liste.



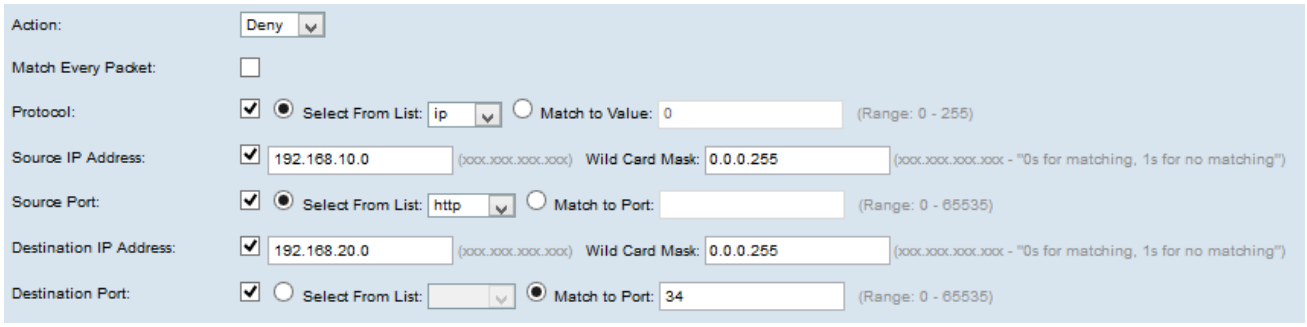
Étape 2. Si une nouvelle règle doit être configurée et s'il y a moins de 10 règles pour la liste de contrôle d'accès sélectionnée, sélectionnez **Nouvelle règle** dans la liste déroulante Règle. Sinon, choisissez l'une des règles actuelles dans la liste déroulante Règle.

Remarque : un maximum de 10 règles peuvent être créées pour une seule liste de contrôle d'accès.

Étape 3. Sélectionnez l'action de la règle ACL dans la liste déroulante Action.

·Deny : bloque tout le trafic qui satisfait aux critères de la règle pour entrer ou sortir du périphérique WAP.

·Permit : permet à tout le trafic qui satisfait aux critères de la règle d'entrer ou de sortir du périphérique WAP.



Note: Toutes les étapes suivantes sont facultatives. Les cases cochées seront activées. Décochez cette case si vous ne voulez pas appliquer une règle spécifique.

Étape 4. Cochez la case **Correspondance de chaque paquet** pour qu'elle corresponde à la règle de chaque trame ou paquet, quel que soit son contenu. Décochez la case **Correspondance de chaque paquet** pour configurer des critères de correspondance supplémentaires.

Économie de temps : si Correspondance à chaque paquet est cochée, passez à l'étape 10.

Étape 5. 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. Si la case Protocol est cochée, cliquez sur l'un des boutons d'option suivants :

·Select From List : protocole à choisir dans la liste déroulante Select From List.

·Match to Value : pour le protocole non présenté dans la liste. Entrez une plage d'ID de protocole IANA standard comprise entre 0 et 255.

Étape 6. Cochez la case **Adresse IP source** pour inclure l'adresse IP de la source dans la condition de correspondance. Saisissez l'adresse IP et le masque générique de la source dans les champs respectifs.

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

·Select From List : port source à choisir dans la liste déroulante Select From List.

·faire correspondre au port : pour le port source non présenté dans la liste. Saisissez le numéro de port compris entre 0 et 65535 et comprenant trois types de ports différents.

- 0 à 1023 — Ports réservés.

- 1024 à 49151 — Ports enregistrés.

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

Étape 8. 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 les champs correspondants.

Étape 9. 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, cliquez sur l'une de ces cases d'option.

·Select From List : port de destination à choisir dans la liste déroulante Select From List.

·faire correspondre au port : pour le port de destination non présenté dans la liste. Entrez le numéro de port compris entre 0 et 65535 dans le champ Correspondance au port. La plage comprend trois types de ports différents.

- 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.

Étape 10. Cochez la case **IP DSCP** pour qu'elle corresponde aux paquets basés sur les valeurs IP DSCP. Si la case IP DSCP est cochée, cliquez sur l'une des cases d'option suivantes :

·Select From List : sélectionnez la valeur DSCP IP souhaitée dans la liste déroulante Select From List.

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

Étape 11. Cochez la case **Priorité IP** pour inclure une valeur de priorité IP dans la condition de correspondance. Si la case Priorité IP est cochée, entrez une valeur de priorité IP comprise entre 0 et 7. Les valeurs de priorité IP et la description de valeur correspondante peuvent être expliquées comme suit :

·0 — Routine ou Best Effort

·1 — Priorité

·2 - Immédiat

·3 - Flash (principalement utilisé pour la signalisation vocale ou pour la vidéo)

·4 — Remplacement Flash

·5 — Critique (principalement utilisé pour le protocole RTP voix)

·6 - Internet

·7 — Réseau

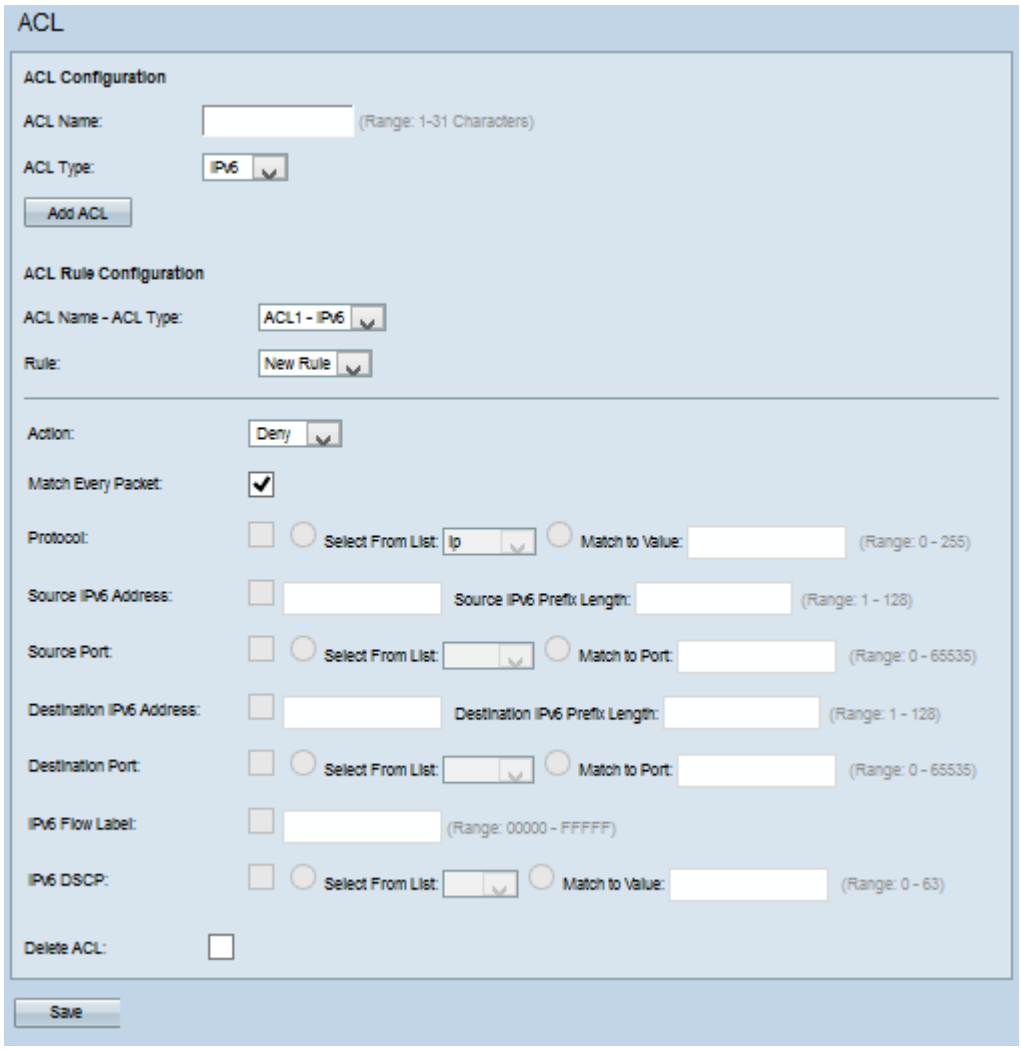
Étape 12. Cochez la case **Bits TOS IP** pour utiliser le type de bits de service dans l'en-tête IP comme critère de correspondance. Si la case à cocher IP TOS Bits est activée, entrez les bits IP TOS compris entre 00 et FF et le masque IP TOS compris entre 00 et FF dans les

champs respectifs.

Étape 13. Pour supprimer la liste de contrôle d'accès configurée, cochez la case **Supprimer la liste de contrôle d'accès**, puis cliquez sur **Enregistrer**.

Configuration de la liste de contrôle d'accès IPv6

Note: Si IPv6 est sélectionné dans la liste déroulante Type de liste de contrôle d'accès, suivez les étapes ci-dessous pour configurer les règles de liste de contrôle d'accès IPv6.



Étape 1. Sélectionnez la liste de contrôle d’accès créée dans la liste déroulante Nom de la liste de contrôle d’accès - Type de liste.

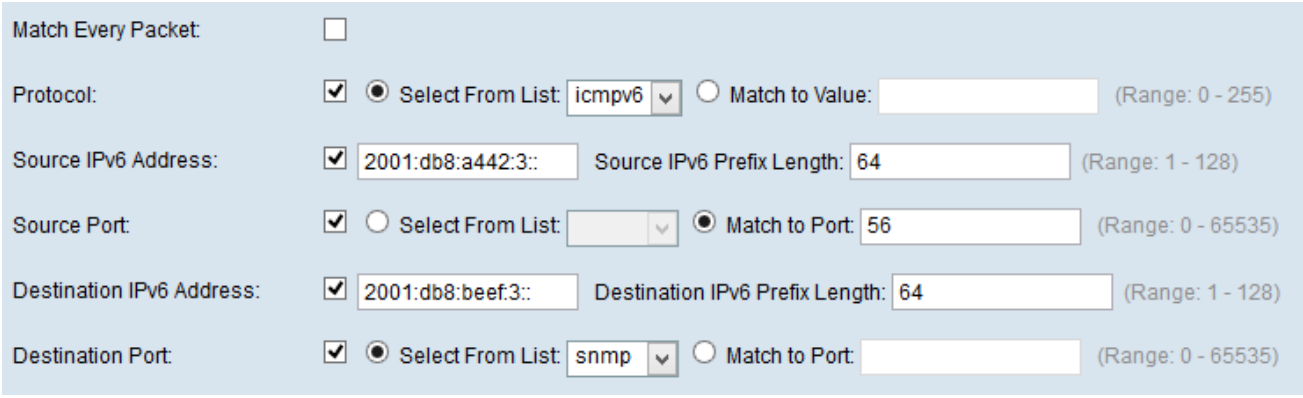
Étape 2. Si une nouvelle règle doit être configurée pour la liste de contrôle d'accès sélectionnée, sélectionnez **Nouvelle règle** dans la liste déroulante Règle. Sinon, choisissez l'une des règles actuelles dans la liste déroulante Règle.

Note: Vous pouvez créer jusqu'à 10 règles pour une seule liste de contrôle d'accès.

Étape 3. Sélectionnez l'action de la règle ACL dans la liste déroulante Action.

·Deny : bloque tout le trafic qui satisfait aux critères de la règle pour entrer ou sortir du périphérique WAP.

·Permit : permet à tout le trafic qui satisfait aux critères de la règle d'entrer ou de sortir du périphérique WAP.



Note: Toutes les étapes suivantes sont facultatives. Les cases cochées seront activées. Décochez cette case si vous ne voulez pas appliquer une règle spécifique.

Étape 4. Cochez la case **Correspondance de chaque paquet** pour qu'elle corresponde à la règle de chaque trame ou paquet, quel que soit son contenu. Décochez la case **Correspondance de chaque paquet** pour configurer des critères de correspondance supplémentaires.

Économie de temps : si Correspondance à chaque paquet est cochée, passez à l'étape 12.

Étape 5. 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 IPv6. Si la case Protocol est cochée, cliquez sur l'un des boutons d'option suivants.

·Select From List : protocole à choisir dans la liste déroulante Select From List.

·Match to Value : pour le protocole non présenté dans la liste. Entrez une plage d'ID de protocole IANA standard comprise entre 0 et 255.

Étape 6. 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 les champs respectifs.

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

·Select From List : port source à choisir dans la liste déroulante Select From List.

·Associer au port : pour les ports sources non présentés dans la liste. Saisissez le numéro de port compris entre 0 et 65535 et comprenant trois types de ports différents.

- 0 à 1023 — Ports réservés.

- 1024 à 49151 — Ports enregistrés.

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

Étape 8. 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 les champs correspondants.

Étape 9. 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, cliquez sur l'une des cases d'option suivantes :

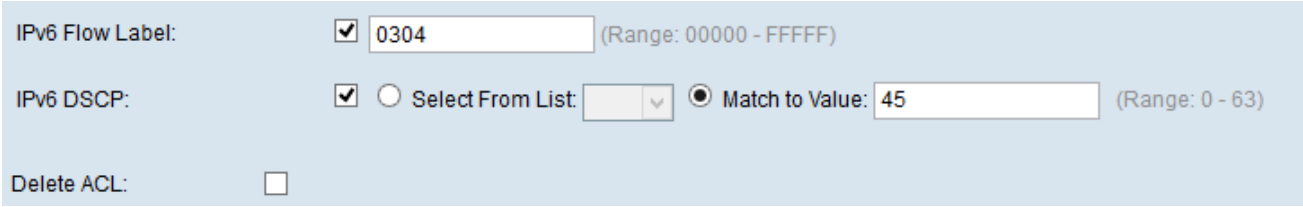
·Select From List : port de destination à choisir dans la liste déroulante Select From List.

·faire correspondre au port : pour le port de destination non présenté dans la liste. Entrez le numéro de port compris entre 0 et 65535 dans le champ Correspondance au port. La plage comprend trois types de ports différents.

- 0 à 1023 — Ports réservés.

- 1024 à 49151 — Ports enregistrés.

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



Étape 10. Cochez la case **Étiquette de flux IPv6** pour inclure l'étiquette de flux IPv6 dans la condition de correspondance. Le champ d'étiquette de flux de 20 bits de l'en-tête IPv6 peut être utilisé par une source pour étiqueter un ensemble de paquets appartenant au même flux. Saisissez le nombre compris entre 00000 et FFFF dans le champ IPv6 Flow label.

Étape 11. Cochez la case **DSCP IPv6** pour inclure les valeurs DSCP IP dans la condition de correspondance. Si la case IP DSCP est cochée, cliquez sur l'une de ces cases d'option.

·Select From List : valeur DSCP IP à choisir dans la liste déroulante Select From List.

·faire correspondre à la valeur : pour personnaliser la valeur DSCP qui varie de 0 à 63.

Étape 12. (Facultatif) Pour supprimer la liste de contrôle d'accès configurée, cochez la case **Supprimer la liste de contrôle d'accès**.

Étape 13. Click Save.