Création et configuration d'une règle pour la liste de contrôle d'accès IPv6 sur les points d'accès WAP121 et WAP321

Objectif

Une liste de contrôle d’accès (ACL) est une liste de filtres de trafic réseau et d’actions corrélées utilisées pour améliorer la sécurité. Une liste de contrôle d’accès contient les hôtes auxquels l’accès au périphérique réseau est autorisé ou refusé. 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 IPv6 sur les points d'accès WAP121 et WAP321.

Périphériques pertinents

·WAP121
· WAP321

Version du logiciel

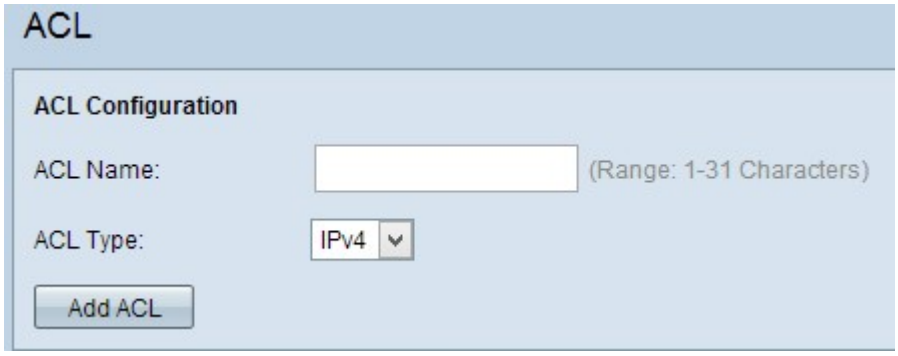
•v 1.0.3.4

Configuration des listes de contrôle d'accès IPv6

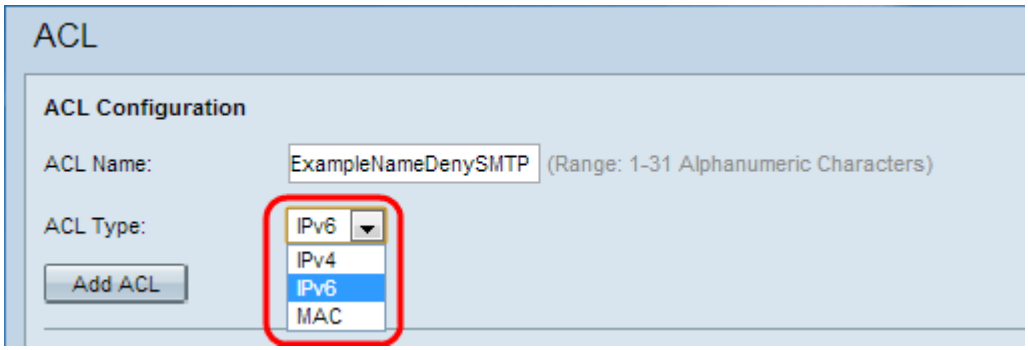
Les listes de contrôle d’accès IP classent le trafic des couches 3 dans la pile IP. Chaque liste de contrôle d’accès est un ensemble de 10 règles maximum appliquées au trafic envoyé par un client sans fil ou reçu par un client sans fil. Chaque règle spécifie si le contenu d'un champ donné doit être utilisé 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.

Création d'une liste de contrôle d'accès IPv6

Étape 1. Connectez-vous à l'utilitaire de configuration du point d'accès et choisissez **Client QoS > ACL**. La page *ACL* s'affiche.



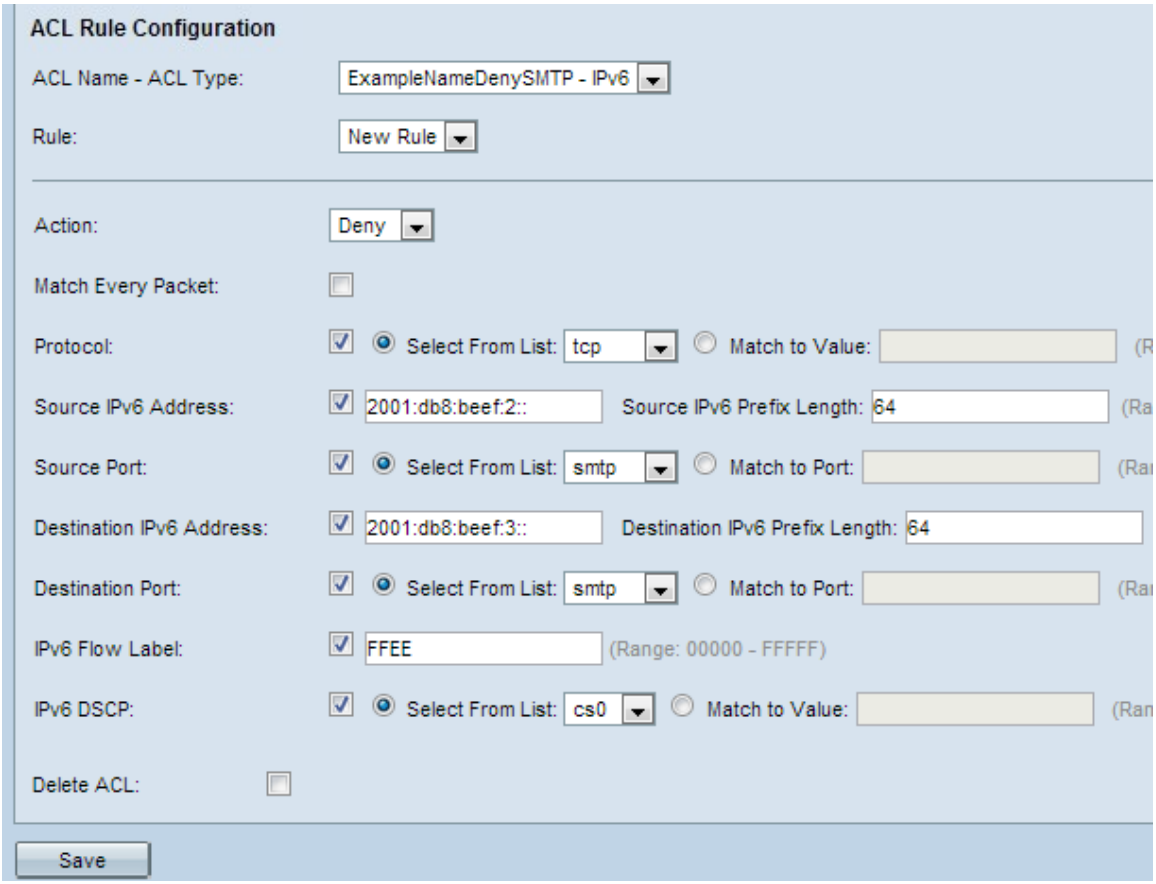
Étape 2. Entrez le nom de la liste de contrôle d'accès dans le champ *Nom de la liste de contrôle d'accès*.



Étape 3. Choisissez le type **IPv6** de la liste de contrôle d'accès dans la liste déroulante *Type de liste de contrôle d'accès*.

Étape 4. Cliquez sur **Ajouter une liste de contrôle d'accès** pour créer une nouvelle liste de contrôle d'accès IPv6.

Configuration d'une règle pour une liste de contrôle d'accès IPv6



Étape 1. Choisissez la liste de contrôle d'accès dans la liste déroulante *Nom de la liste de contrôle d'accès -Type* de liste de contrôle d'accès pour laquelle la règle doit être configurée.

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. Choisissez 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.

Attention : Vous devez ajouter une règle d'autorisation autorise le trafic car si une autorisation ou un refus est sélectionné, il y a toujours un refus implicite à la fin de chaque règle.

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. Si vous souhaitez configurer l'un des critères de correspondance supplémentaires, décochez la case *Correspondance de chaque paquet*.

Économiseur de temps : Si vous cochez la case *Correspondre à chaque paquet*, passez à l' étape 12.

Étape 5. Cochez la case *Protocol* pour activer la condition de correspondance de protocole L3 ou L4 (couche réseau et couche transport de la pile IP) en fonction de la valeur du champ

IP Protocol dans les paquets IPv6. Si la case Protocole est cochée, cliquez sur l'une de ces cases d'option.

·Select From List : sélectionnez un protocole dans la liste déroulante Select From List. La liste déroulante contient les protocoles ip, icmp, igmp, tcp et udp.

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

Étape 6. Cochez la case *Adresse IPv6 source* pour inclure une adresse IP de la source dans la condition de correspondance. Entrez l'adresse IPv6 et la longueur de préfixe IPv6 de la source dans les champs relatifs.

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 de ces cases d'option.

·Select From List : sélectionnez un port source dans la liste déroulante Select From List. La liste déroulante contient les ports ftp, ftpdata, http, smtp, snmp, telnet, tftp et www.

·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. Port utilisé par le processus serveur comme port de contact. Le port de contact est parfois appelé un port réservé.

- 1024 à 49151 — Ports enregistrés. Il s'agit d'un port réseau utilisé pour certains protocoles ou pour une application.

- 49152 à 65535 — Ports dynamiques et/ou privés. Les ports dynamiques ne sont gérés par aucun organe de gouvernance comme IANA et n'ont aucune restriction d'utilisation particulière.

Étape 8. Cochez la case *Adresse IPv6 de destination* pour inclure l'adresse IP de destination dans la condition de correspondance. Saisissez l'adresse IPv6 et la longueur de préfixe IPv6 de la destination dans les champs relatifs.

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 : sélectionnez un port de destination dans la liste déroulante Select From List. La liste déroulante contient les ports ftp, ftpdata, http, smtp, snmp, telnet, tftp et www.

·faire correspondre au port : pour le port de destination 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 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 *IP DSCP* pour inclure les valeurs IP DSCP 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. La liste déroulante contient des valeurs DSCP Asened Forwarding (AS), Class of Service (CS) ou Expeded Forwarding (EF).

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

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

Étape 13. Cliquez sur **Save pour enregistrer les paramètres.**