Erstellen und Konfigurieren einer Regel für eine IPv6-basierte Zugriffskontrollliste (ACL) auf den Access Points WAP121 und WAP321

Ziel

Eine Zugriffskontrollliste (Access Control List, ACL) ist eine Liste von Filtern für den Netzwerkverkehr und zugehörigen Aktionen zur Verbesserung der Sicherheit. Eine Zugriffskontrollliste enthält die Hosts, denen der Zugriff auf das Netzwerkgerät gestattet oder verweigert wird. Die QoS-Funktion umfasst Differentiated Services (DiffServ)-Unterstützung, die die Klassifizierung von Datenverkehr in Streams und die Bereitstellung bestimmter QoS-Behandlungen gemäß definiertem PoS-Verhalten pro Hop ermöglicht.

In diesem Artikel wird erläutert, wie IPv6 ACL auf WAP121- und WAP321-Access Points erstellt und konfiguriert wird.

Anwendbare Geräte

WAP121
WAP321

Softwareversion

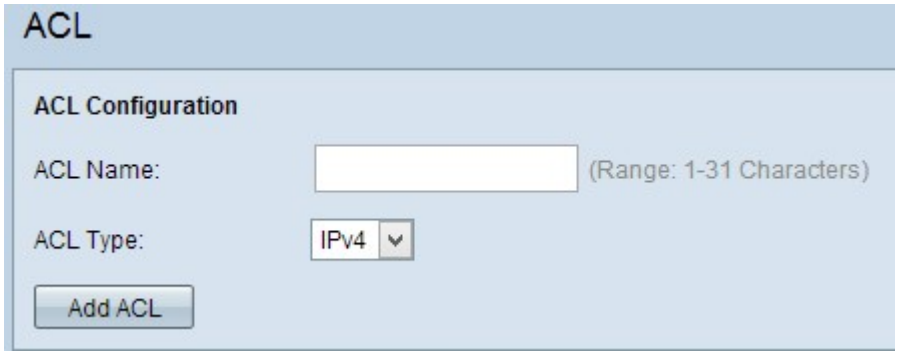
·v1.0.3.4

IPv6-basierte ACL-Konfiguration

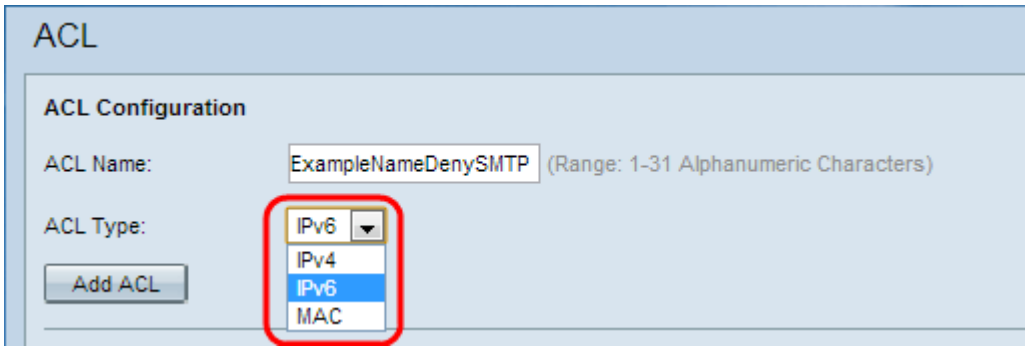
IP-ACLs klassifizieren den Datenverkehr für Layer 3 im IP-Stack. Jede ACL ist ein Satz von bis zu 10 Regeln, die auf Datenverkehr angewendet werden, der entweder von einem Wireless-Client gesendet oder von einem Wireless-Client empfangen wird. Jede Regel legt fest, ob der Inhalt eines Felds verwendet werden soll, um den Zugriff auf das Netzwerk zu ermöglichen oder zu verweigern. Regeln können auf verschiedenen Kriterien basieren und können für ein oder mehrere Felder innerhalb eines Pakets gelten, z. B. die Quell- oder Ziel-IP-Adresse, den Quell- oder Zielport oder das im Paket übertragene Protokoll.

Erstellung von IPv6-ACLs

Schritt 1: Melden Sie sich beim Konfigurationsprogramm für Access Points an, und wählen Sie **Client QoS > ACL aus**. Die Seite *ACL* wird geöffnet.



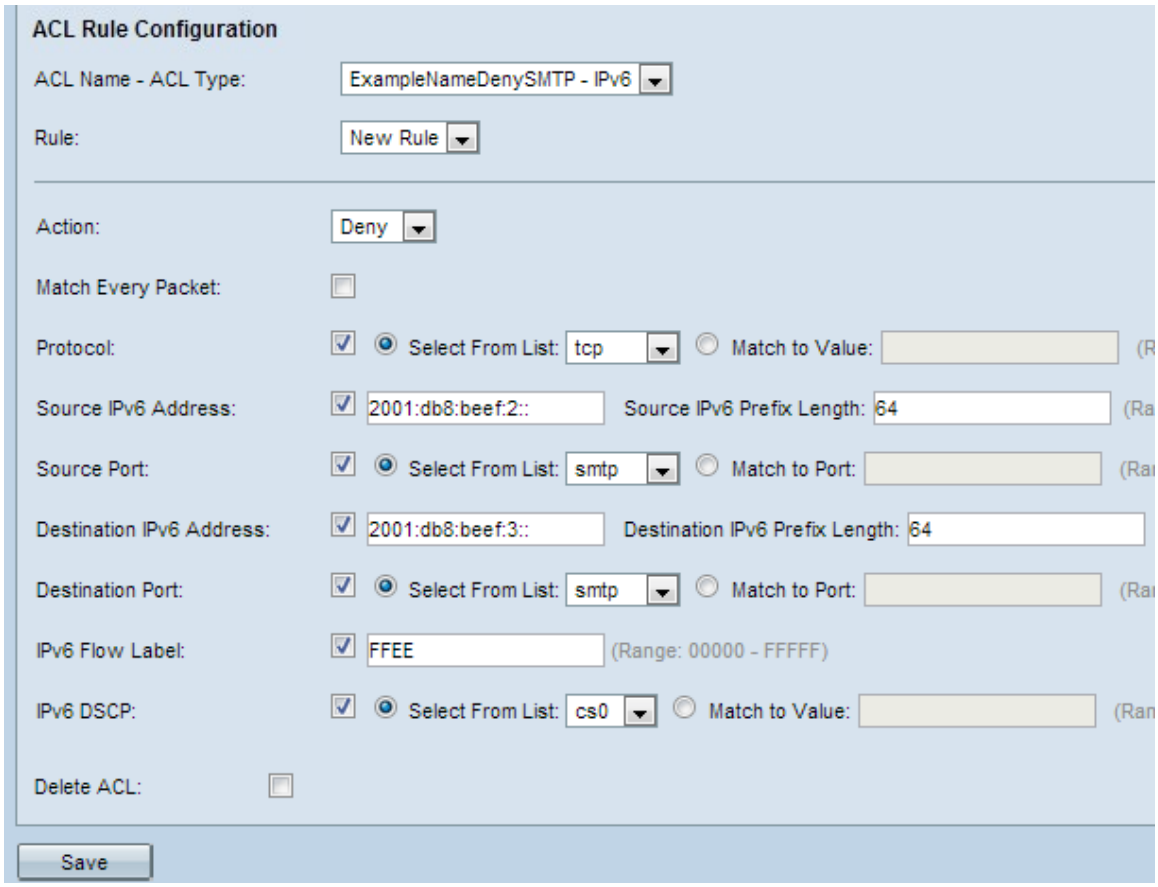
Schritt 2: Geben Sie im Feld *ACL Name* den Namen der ACL ein.



Schritt 3: Wählen Sie den **IPv6-**Typ für die ACL aus der Dropdown-Liste *ACL Type (ACL-Typ*) aus.

Schritt 4: Klicken Sie auf **ACL hinzufügen**, um eine neue IPv6-ACL zu erstellen.

Konfiguration einer Regel für IPv6-ACL



Schritt 1: Wählen Sie die ACL aus der Dropdown-Liste "*ACL Name-ACL Type*" aus, für die

die Regel konfiguriert werden muss.

Schritt 2: Wenn für die ausgewählte ACL eine neue Regel konfiguriert werden muss, wählen Sie **Neue Regel** aus der Dropdown-Liste *Regel*. Wählen Sie andernfalls eine der aktuellen Regeln aus der Dropdown-Liste *Regel*.

Hinweis: Es können maximal 10 Regeln für eine einzige ACL erstellt werden.

Schritt 3: Wählen Sie die Aktion für die ACL-Regel aus der Dropdown-Liste *Aktion* aus.

·Verweigern: Blockiert den gesamten Datenverkehr, der die Regelkriterien für die Ein- bzw. Ausfahrt des WAP-Geräts erfüllt.

·Zulassen - Ermöglicht allen Datenverkehr, der die Regelkriterien erfüllt, ein- oder auszusteigen.

Vorsicht: Sie müssen eine Zulassen-Regel hinzufügen, um den Datenverkehr zu genehmigen, da bei Auswahl einer Berechtigung oder Ablehnung am Ende jeder Regel immer eine implizite Ablehnung vorliegt.

Schritt 4: Aktivieren Sie das Kontrollkästchen *Jedes Paket* zuordnen, um die Regel für jeden Frame oder jedes Paket zu übernehmen, unabhängig vom Inhalt. Wenn Sie eines der zusätzlichen Entsprechungskriterien konfigurieren möchten, deaktivieren Sie das Kontrollkästchen *Jedes Paket* zuordnen.

Zeitgeber: Wenn Sie das Kontrollkästchen *Jedes Paket* zuordnen aktivieren, fahren Sie mit Schritt 12 fort.

Schritt 5: Aktivieren Sie das Kontrollkästchen *Protocol* (*Protokoll*), um die Protokollkonformität L3 oder L4 (Netzwerk- und Transportschicht des IP-Stacks) basierend auf dem Wert des *IP-Protokollfelds* in IPv6-Paketen zu aktivieren. Wenn das Kontrollkästchen Protokoll aktiviert ist, klicken Sie auf eines dieser Optionsfelder.

·Aus Liste auswählen: Wählen Sie ein Protokoll aus der Dropdown-Liste "Aus Liste auswählen" aus. Die Dropdown-Liste enthält die Protokolle ip, icmp, igmp, tcp und udp.

·Dem Wert zuordnen - Für Protokolle, die nicht in der Liste aufgeführt sind. Geben Sie einen standardmäßigen, IANA zugewiesenen Protokoll-ID-Bereich zwischen 0 und 255 ein.

Schritt 6: Aktivieren Sie das Kontrollkästchen *Quell-IPv6-Adresse*, um eine IP-Adresse der Quelle in den Match-Zustand einzubeziehen. Geben Sie die IPv6-Adresse und die IPv6-Präfixlänge der Quelle in die relativen Felder ein.

Schritt 7: Aktivieren Sie das Kontrollkästchen *Quellport*, um einen Quellport in die Übereinstimmung einzubeziehen. Wenn das Kontrollkästchen Quellport aktiviert ist, klicken Sie auf eines dieser Optionsfelder.

·Aus Liste auswählen: Wählen Sie einen Quellport aus der Dropdown-Liste "Aus Liste auswählen" aus. Die Dropdown-Liste enthält ftp, ftpdata, http, smtp, snmp, telnet, tftp und www-Ports.

·"Match to Port" (Zuordnung zum Port) - Für Quellport, der nicht in der Liste aufgeführt ist. Geben Sie die Portnummer zwischen 0 und 65535 ein, die drei verschiedene Porttypen umfasst.

- 0 bis 1023 — Bekannte Ports. Der vom Serverprozess als Kontakt-Port verwendete

Port. Der Kontakt-Port wird manchmal auch als bekannter Port bezeichnet.

- 1024 bis 49151 — Registrierte Ports Es handelt sich um einen Netzwerkport für ein bestimmtes Protokoll oder eine Anwendung.

- 49152 bis 65535 - Dynamische und/oder private Ports Dynamische Ports werden nicht von einem Leitungsorgan wie IANA verwaltet und unterliegen keinen besonderen Nutzungsbeschränkungen.

Schritt 8: Aktivieren Sie das Kontrollkästchen *Ziel-IPv6-Adresse*, um die IP-Adresse des Ziels in die Übereinstimmung einzubeziehen. Geben Sie die IPv6-Adresse und die IPv6-Präfixlänge des Ziels in den relativen Feldern ein.

Schritt 9: Aktivieren Sie das Kontrollkästchen *Ziel-Port*, um einen Zielport in die Übereinstimmung einzubeziehen. Wenn das Kontrollkästchen Destination Port (Zielport) aktiviert ist, klicken Sie auf eine dieser Optionsfelder.

·Aus Liste auswählen: Wählen Sie aus der Dropdown-Liste "Select From List" (Von Liste auswählen) einen Zielport aus. Die Dropdown-Liste enthält ftp, ftpdata, http, smtp, snmp, telnet, tftp und www-Ports.

·"Match to Port" (Zuordnung zum Port) - Für Zielport, der nicht in der Liste aufgeführt ist. Geben Sie die Portnummer zwischen 0 und 65535 ein, die drei verschiedene Porttypen umfasst.

- 0 bis 1023 — Bekannte Ports.

- 1024 bis 49151 — Registrierte Ports

- 49152 bis 65535 - Dynamische und/oder private Ports

Schritt 10: Aktivieren Sie das Kontrollkästchen *IPv6 Flow Label (*IPv6-*Flow-Label*), um die IPv6-Flowbezeichnung in den Match-Zustand aufzunehmen. Das 20-Bit-Flow-Label-Feld im IPv6-Header kann von einer Quelle verwendet werden, um eine Gruppe von Paketen zu kennzeichnen, die demselben Fluss angehören. Geben Sie die Zahl zwischen 00000 und FFFFF im Feld "IPv6 Flow Label" ein.

Schritt 11: Aktivieren Sie das Kontrollkästchen *IP DSCP*, um die IP-DSCP-Werte in die Übereinstimmung einzubeziehen. Wenn das Kontrollkästchen IP DSCP aktiviert ist, klicken Sie auf eines dieser Optionsfelder.

·Wählen Sie aus der Liste auswählen - Der IP-DSCP-Wert, der aus der Dropdown-Liste "Select From List" (Von Liste auswählen) ausgewählt werden soll. In der Dropdown-Liste sind die Werte für "DSCP Assured Forwarding (AS)", "Class of Service" (CS) oder "Expedited Forwarding (EF)" angegeben.

·Dem Wert zuordnen - Zum Anpassen des DSCP-Werts zwischen 0 und 63

Schritt 12: (Optional) Wenn Sie die konfigurierte Zugriffskontrollliste löschen möchten, aktivieren Sie das Kontrollkästchen *Zugriffskontrollliste löschen*.

Schritt 13: Klicken Sie auf **Speichern**, um die Einstellungen zu speichern.