Konfigurieren der IPv6-Zugriffskontrollliste (ACL) auf dem WAP125

Ziel

Internet Protocol Version 4 (IPv4) und Internet Protocol Version 6 (IPv6) Access Control Lists (ACLs) sind eine Reihe von Regeln, die auf Pakete angewendet werden, die vom Wireless Access Point (WAP) empfangen werden. Anhand jeder Regel wird festgelegt, ob der Zugriff auf das Netzwerk zugelassen oder verweigert werden soll. Die ACLs können so konfiguriert werden, dass sie Felder eines Frames wie die Quell- oder Ziel-IP-Adresse, den Virtual Local Area Network (VLAN) Identifier (ID) oder die Class of Service (CoS) überprüfen. Wenn ein Frame in den WAP-Geräteport eingeht, prüft er den Frame und überprüft die ACL-Regeln auf den Inhalt des Frames. Wenn eine der Regeln mit dem Inhalt übereinstimmt, wird im Frame eine Aktion für "Zulassen" oder "Ablehnen" ausgeführt.

Die Konfiguration von ACLs wird häufig verwendet, um den Zugriff auf Netzwerkressourcen zu autorisieren. In einer Unternehmensumgebung sind diejenigen, denen der Zugriff auf die Ressourcen zur Auswahl von Geräten im Netzwerk gewährt wird, in der Regel Manager oder diejenigen, die autorisiert sind, auf die Ressourcen zuzugreifen. Dadurch wird der Ressourcenserver effizienter und das Netzwerk sicherer.

In diesem Artikel erfahren Sie, wie Sie eine IPv6-ACL auf einem WAP125-Access Point konfigurieren.

Hinweis: In diesem Beispiel darf der gesamte Datenverkehr von ausgewählten Hosts mit der IP-Adresse 2001:DB8::22:F673:FF3B:AC99/10 auf das Netzwerk zugreifen. Alle anderen Zugriffe von anderen Hosts werden abgelehnt.

Anwendbare Geräte

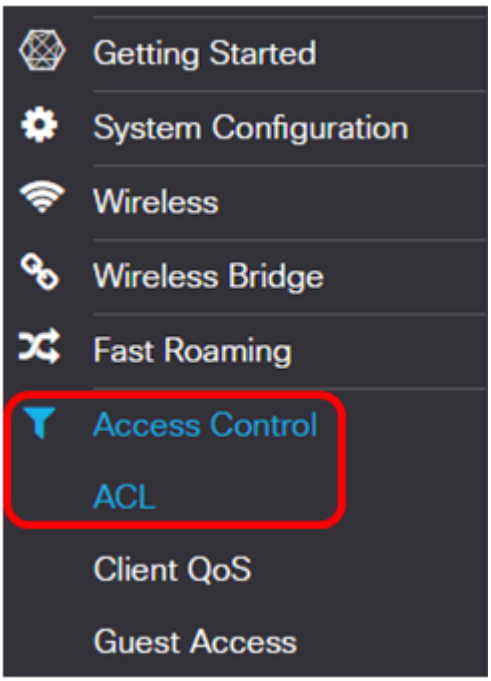
- WAP125

Softwareversion

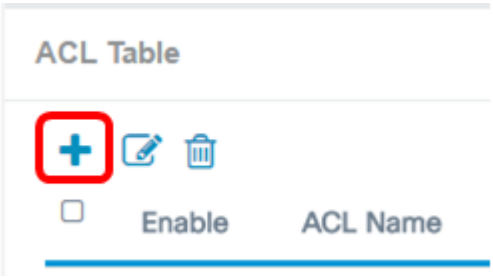
- 1,0/0,3

Konfigurieren einer IPv6-ACL

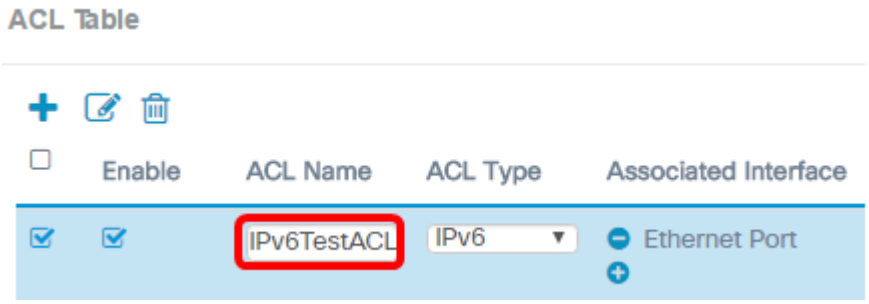
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des WAP125 an, und wählen Sie **Zugriffskontrolle > ACL aus**.



Schritt 2: Klicken Sie auf die Schaltfläche, um eine ACL hinzuzufügen.

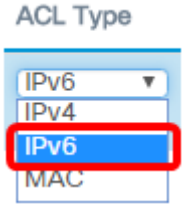


Schritt 3: Geben Sie im Feld *ACL Name* einen Namen für die ACL ein.



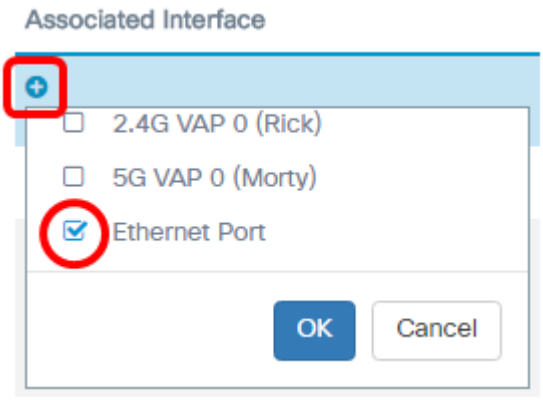
Hinweis: In diesem Beispiel wird IPv6TestACL eingegeben.

Schritt 4: Wählen Sie IPv6 aus der Dropdown-Liste ACL Type (ACL-Typ) aus.



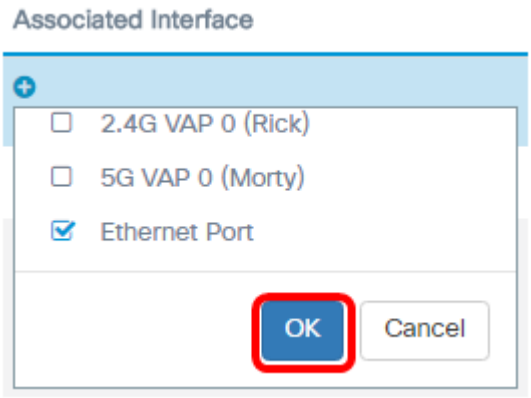
Schritt 5: Klicken Sie auf die Schaltfläche, und wählen Sie in der Dropdown-Liste Associated Interface (Zugeordnete Schnittstelle) eine Schnittstelle aus. Folgende Optionen stehen zur Verfügung:

- 2.4G VAP 0 (SSID-Name): Mit dieser Option wird die MAC-ACL auf den 2,4 GHz Virtual Access Point (VAP) angewendet. Der Abschnitt "SSID Name" kann sich je nach dem auf dem WAP konfigurierten SSID-Namen ändern.
- 5G VAP 0 (SSID-Name): Mit dieser Option wird die MAC-ACL auf den 5-GHz-VAP angewendet.
- Ethernet Port (Ethernet-Port): Mit dieser Option wird die MAC-ACL auf die Ethernet-Schnittstelle des WAP angewendet.

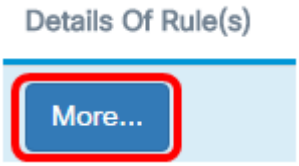


Hinweis: Mehrere Schnittstellen können einer ACL zugeordnet werden. Sie kann jedoch nicht einer anderen ACL zugeordnet werden, wenn sie bereits einer ACL zugeordnet wurde. In diesem Beispiel wird der Ethernet-Port mit IPv6TestACL verknüpft. Deaktivieren Sie das Kontrollkästchen, um die Schnittstelle von der ACL zu trennen.

Schritt 6: Klicken Sie auf **OK**.



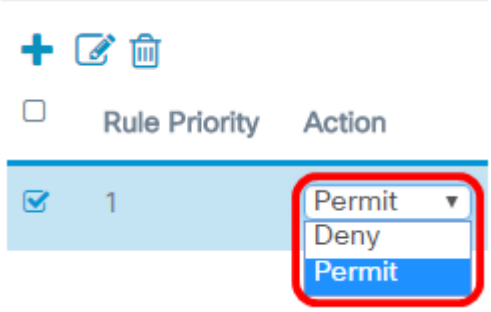
Schritt 7: Klicken Sie auf die Schaltfläche **More..** (Mehr), um die Parameter der ACL zu konfigurieren.



Schritt 8: Klicken Sie auf die Schaltfläche, um eine neue Regel hinzuzufügen.

Schritt 9: Wählen Sie eine Aktion aus der Dropdown-Liste Aktion aus. Folgende Optionen stehen zur Verfügung:

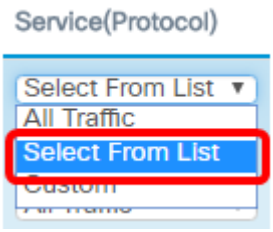
- Zulassen: Mit dieser Option können Pakete, die die ACL-Kriterien erfüllen, eine Verbindung zum Netzwerk herstellen.
- Verweigern: Diese Option verhindert, dass Pakete, die die ACL-Kriterien erfüllen, eine Verbindung zum Netzwerk herstellen.



Hinweis: In diesem Beispiel wird Permit (Zulassen) ausgewählt.

Schritt 10: Wählen Sie aus der Dropdown-Liste Service (Protocol) einen Service oder ein Protokoll aus, der bzw. das gefiltert werden soll. Folgende Optionen stehen zur Verfügung:

- Gesamter Datenverkehr: Diese Option behandelt alle Pakete als Übereinstimmung mit dem ACL-Filter.
- Wählen Sie From List (Von Liste auswählen): Mit dieser Option können Sie ipv6, icmpv6, igmp, tcp oder udp als Filter für die ACL auswählen. Wenn diese Option ausgewählt ist, fahren Sie mit Schritt 11 fort.
- Custom (Benutzerdefiniert): Mit dieser Option können Sie eine benutzerdefinierte Protokoll-ID als Filter für die Pakete eingeben. Der Wert ist eine vierstellige Hexadezimalzahl. Der Bereich liegt zwischen 0 und 255.



Hinweis: In diesem Beispiel wird Select From List (Aus Liste auswählen) ausgewählt.

Schritt 11: Wählen Sie in der Dropdown-Liste Service(Protocol) ein Protokoll aus. Folgende Optionen stehen zur Verfügung:

- ipv6: Mit dieser Option können die Hosts, die auf das Netzwerk zugreifen, mithilfe ihrer IPv6-Adresse als Filter gefiltert werden.
- icmpv6 - Mit dieser Option können die Access Points Pakete der Version 6 (ICMPv6) des Internet Control Message Protocol filtern, die über den Access Point in das Netzwerk gelangen.
- igmp: Mit dieser Option können die Access Points IGMP-Pakete (Internet Group Management Protocol) filtern, die über den Access Point in das Netzwerk gelangen.
- tcp (tcp): Mit dieser Option werden vom Access Point eingehende TCP-Pakete (Transmission Control Protocol) gefiltert, die über den Access Point in das Netzwerk

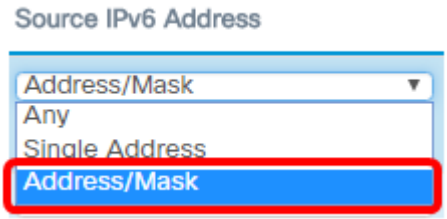
gelangen.

- udp (udp): Mit dieser Option können vom Access Point Pakete aus dem User Datagram Protocol (UDP) gefiltert werden, die über den Access Point in das Netzwerk gelangen.

Hinweis: In diesem Beispiel wird ipv6 ausgewählt.

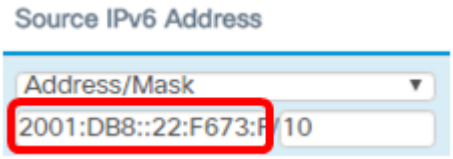
Schritt 12: Definieren Sie die IPv6-Quelladresse aus der Dropdown-Liste IPv6-Adresse der Quelle. Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Mit dieser Option kann der WAP den Filter auf Pakete aus einer beliebigen IP-Adresse anwenden.
- Single Address (Einzeladresse): Mit dieser Option kann der WAP den Filter auf Pakete aus einer angegebenen IP-Adresse anwenden.
- Address/Mask (Adresse/Maske): Mit dieser Option kann der WAP den Filter auf Pakete mit einer IP-Adresse und der IP-Maske anwenden.



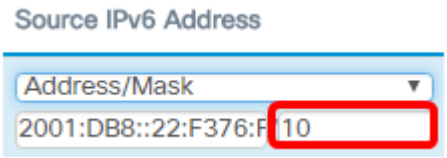
Hinweis: In diesem Beispiel wird Adresse/Maske ausgewählt.

Schritt 13: Geben Sie die IPv6-Quelladresse in das Feld *IPv6-Quelladresse ein*.



Hinweis: In diesem Beispiel wird 2001:DB8::22:F673:FF3B:AC20 eingegeben.

Schritt 14: Geben Sie die IPv6-Maske in das Feld *Maske ein*.

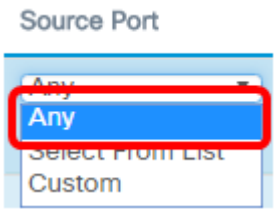


Hinweis: In diesem Beispiel wird 10 eingegeben.

Schritt 15: Wählen Sie einen Quellport für die Bedingung aus. Folgende Optionen stehen zur

Verfügung:

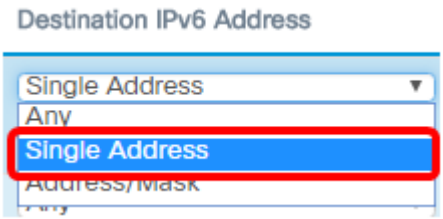
- Any (Beliebig): Mit dieser Option werden alle Pakete vom Quellport zugelassen, die die Kriterien erfüllen.
- Wählen Sie From List (Von Liste auswählen) aus. Mit dieser Option können Sie ftp, ftp data, http, smtp, snmp, telnet, tftp und www auswählen.
- Custom (Benutzerdefiniert): Mit dieser Option können Sie eine IANA-Portnummer eingeben, die mit dem im Datagram-Header angegebenen Quellport übereinstimmt. Der Port-Bereich liegt zwischen 0 und 65535 und umfasst Folgendes:
- 0 bis 1023 - Bekannte Ports
- 1024-49151 — Registrierte Ports
- 49152-65535 - Dynamische und/oder private Ports



Hinweis: In diesem Beispiel wird Any (Beliebig) ausgewählt.

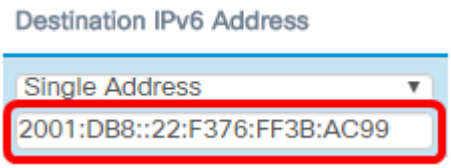
Schritt 16: Wählen Sie in der Dropdown-Liste Destination IPv6 Address (IPv6-Adresse des Ziels) eine Zieladresse aus. Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Bei dieser Option wird jede IP-Adresse als Übereinstimmung mit der ACL-Anweisung behandelt.
- Single Address (Einzeladresse): Mit dieser Option können Sie eine bestimmte IP-Adresse für die ACL-Bedingung eingeben.
- Adresse/Maske (Adresse/Maske): Mit dieser Option können Sie einen IP-Adressbereich eingeben.



Hinweis: In diesem Beispiel wird die Einzeladresse ausgewählt.

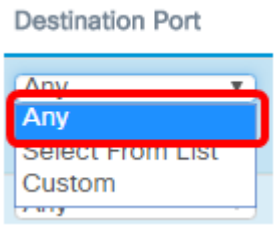
Schritt 17: Geben Sie die Ziel-IPv6-Adresse im Feld *Ziel-IPv6-Adresse ein*.



Hinweis: In diesem Beispiel wird 2001:DB8::22:F376:FF3B:AC99 eingegeben.

Schritt 18: Wählen Sie in der Dropdown-Liste Destination Port (Zielport) einen Zielport aus. Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Bei dieser Option werden alle Zielports der Pakete mit der Anweisung in der ACL verglichen.
- Select From List (Von Liste auswählen): Mit dieser Option können Sie ein Schlüsselwort auswählen, das dem Zielport zugeordnet ist. Folgende Optionen stehen zur Verfügung: ftp, ftpdata, http, smtp, snmp, telnet, tftp und www. Diese Schlüsselwörter werden in die entsprechenden Portnummern übersetzt.
- Custom (Benutzerdefiniert): Mit dieser Option können Sie eine IANA-Portnummer eingeben, die mit dem im Datagram-Header angegebenen Quellport übereinstimmt. Der Port-Bereich liegt zwischen 0 und 65535 und umfasst Folgendes:
- 0 bis 1023 - Bekannte Ports
- 1024-49151 — Registrierte Ports
- 49152 - 65535 - Dynamische und/oder private Ports



Hinweis: In diesem Beispiel wird Any (Beliebig) ausgewählt.

Schritt 19: Wählen Sie aus der Dropdown-Liste Flow Label (Flow-Label) eine IPv6-Flussbezeichnung aus. Diese gibt eine 20-Bit-Nummer an, die für ein IPv6-Paket eindeutig ist. Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Diese Option gibt eine beliebige 20-Bit-Zahl an.
- DSCP Value (DSCP-Wert): Diese Option entspricht den Paketen basierend auf ihrem benutzerdefinierten DSCP-Wert. Wenn Sie diese Option wählen, geben Sie im Feld DSCP Value (DSCP-Wert) einen Wert zwischen 0 und 63 ein.

Hinweis: In diesem Beispiel wird Any (Beliebig) ausgewählt.

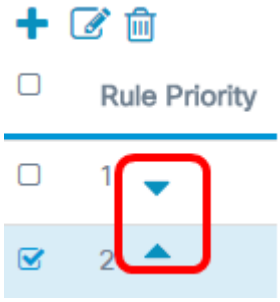
Schritt 20: Wählen Sie in der Dropdown-Liste DSCP eine DSCP-Einstellung (Differentiated Services Code Point) aus. Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Bei dieser Option werden alle Services als Übereinstimmung behandelt.
- Select From List (Von Liste auswählen): Mit dieser Option können Sie einen DSCP-Filter aus der DSCP-Liste auswählen. Die Auswahl hängt von der DSCP-Konfiguration ab.
- Benutzerdefiniert: Mit dieser Option können Sie einen benutzerdefinierten DSCP-Wert zwischen 0 und 63 eingeben.

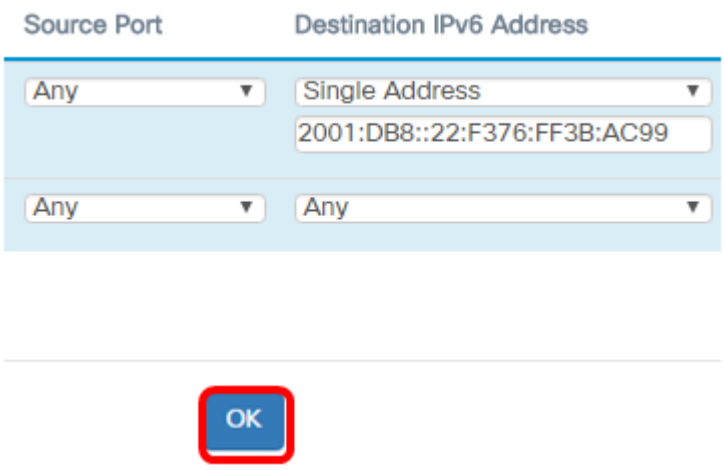
Hinweis: In diesem Beispiel wird Any (Beliebig) ausgewählt.

Schritt 21: (Optional) Wiederholen Sie die Schritte 8 bis 20, bis die Zugriffskontrollliste vollständig ist.

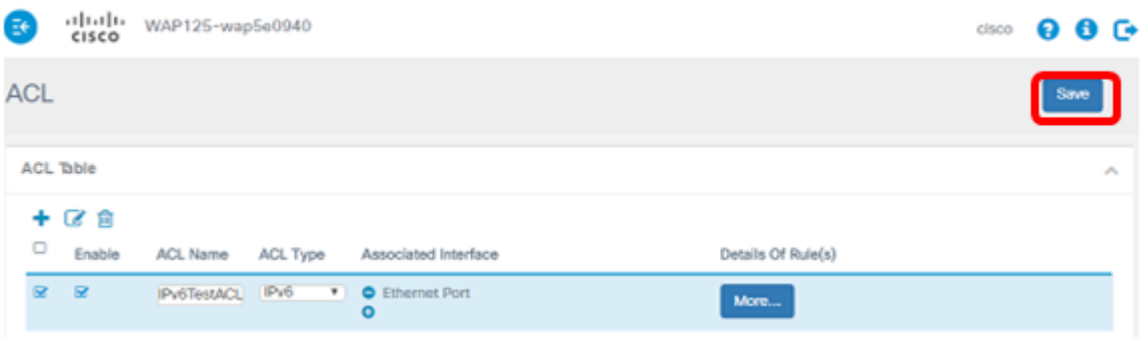
Schritt 22: (Optional) Ändern Sie die Reihenfolge der Bedingungen in der ACL, indem Sie auf die Auf- und Abwärtstasten klicken, bis sie in der richtigen Reihenfolge sind.



Schritt 23: Klicken Sie auf **OK**.



Schritt 24: Klicken Sie auf **Speichern**.



Sie sollten jetzt die IPv6-ACL am WAP125 Access Point abgeschlossen haben.