

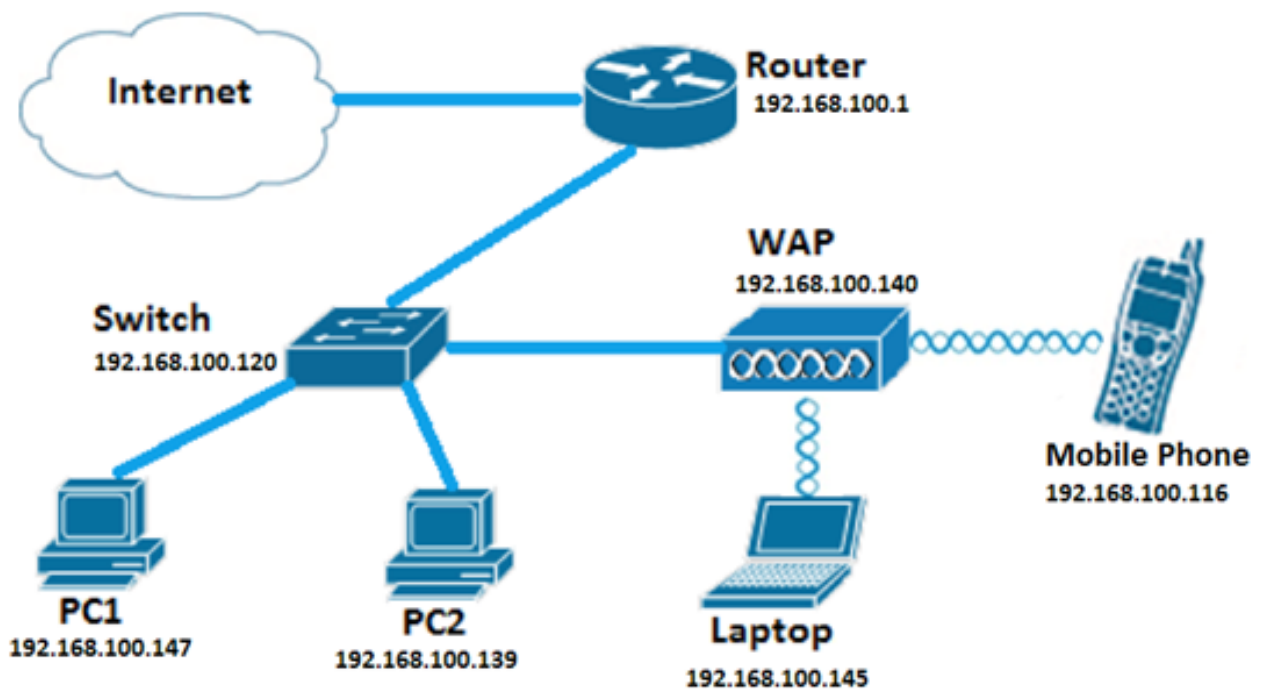
# Konfigurieren der IPv4-ACL auf dem WAP125 und WAP581

## Einführung

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 IPv4-ACLs wird in der Regel verwendet, um den Zugriff auf Netzwerkressourcen für ausgewählte Geräte im Netzwerk zu autorisieren.

**Hinweis:** Am Ende jeder erstellten Regel wird eine implizite Ablehnung ausgegeben.



**Hinweis:** In diesem Szenario ist der gesamte Datenverkehr von PC2 für den Netzwerkzugriff zugelassen. Alle anderen Zugriffe von anderen Hosts werden abgelehnt.

## Ziel

In diesem Artikel erfahren Sie, wie Sie eine IPv4-ACL auf einem WAP125 und WAP581 Access Point konfigurieren.

## Anwendbare Geräte

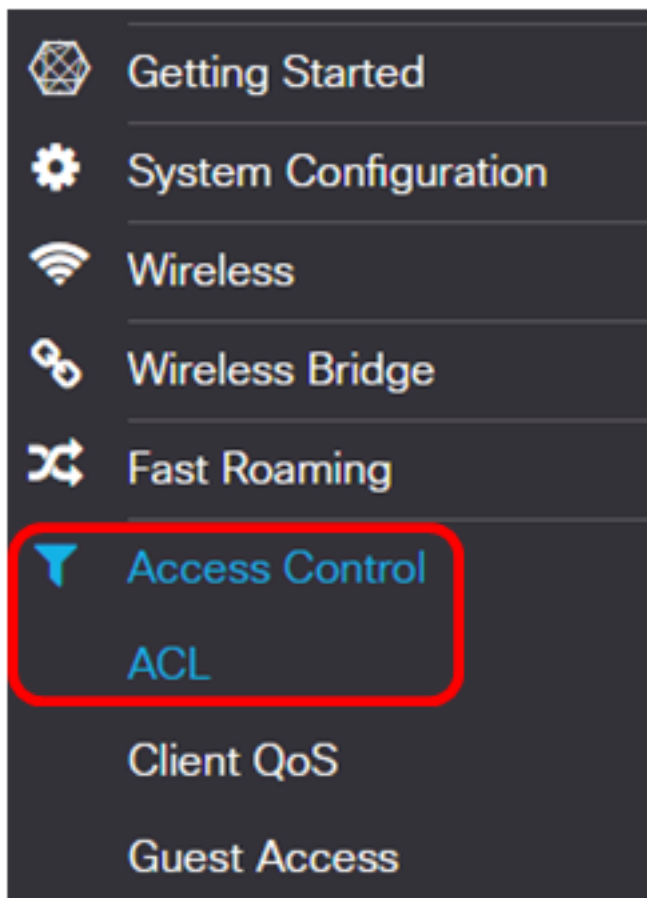
- WAP125
- WAP581

## Softwareversion

- 1.0.0.5 — WAP125
- 1.0.0.4 — WAP581

## Konfigurieren einer IPv4-ACL

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

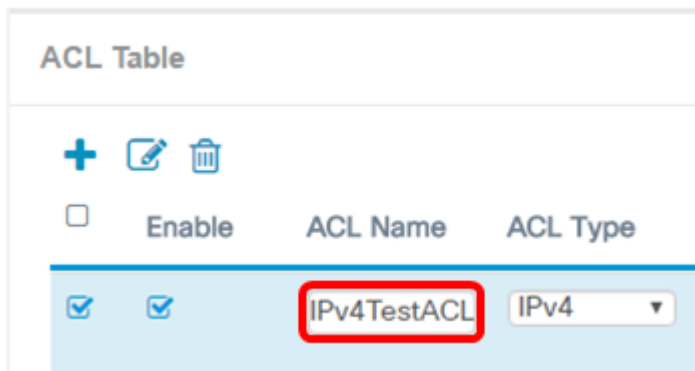


Schritt 2: Klicken Sie auf die **+** Schaltfläche, um eine neue ACL zu erstellen.

ACL Table

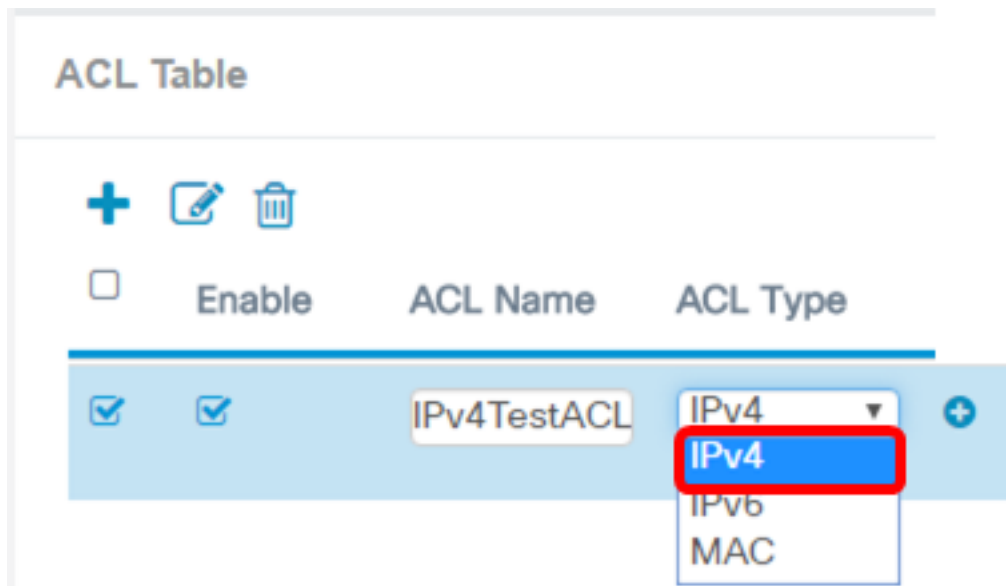



Schritt 3: Geben Sie im Feld *ACL Name* einen Namen für die ACL ein.



**Hinweis:** In diesem Beispiel wird IPv4TestACL eingegeben.

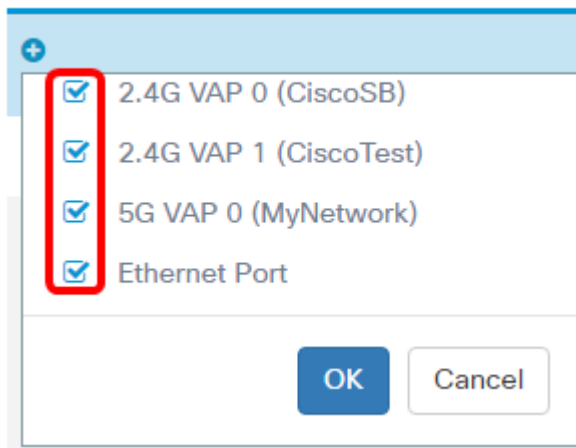
Schritt 4: Wählen Sie IPv4 aus der Dropdown-Liste ACL Type (ACL-Typ) aus.



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 VAP0 (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.

### Associated Interface



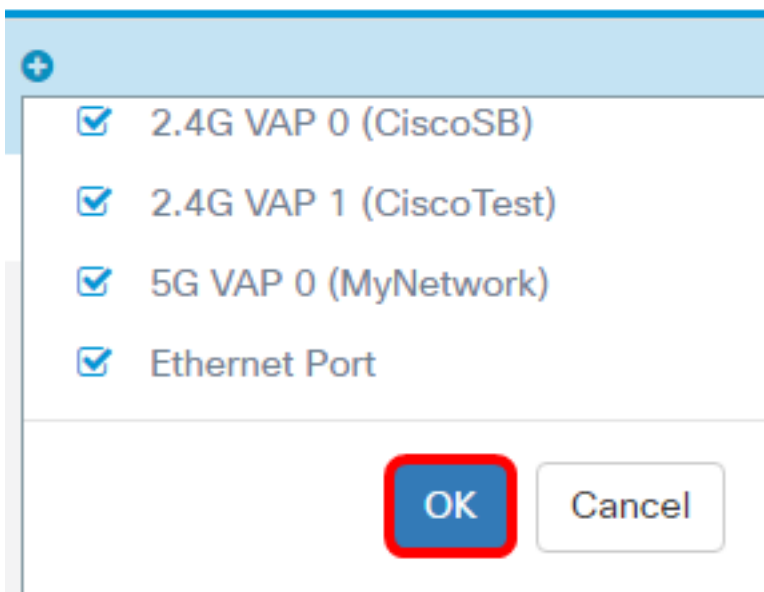
2.4G VAP 0 (CiscoSB)  
 2.4G VAP 1 (CiscoTest)  
 5G VAP 0 (MyNetwork)  
 Ethernet Port

OK Cancel

**Hinweis:** Mehrere Schnittstellen können einer ACL zugeordnet werden. Sie kann jedoch nicht einer ACL zugeordnet werden, wenn sie bereits einer anderen ACL zugeordnet wurde. In diesem Beispiel werden alle Schnittstellen IPv4TestACL zugeordnet. Deaktivieren Sie das Kontrollkästchen, um die Schnittstelle von der ACL zu trennen.

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

### Associated Interface

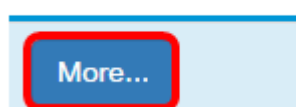


2.4G VAP 0 (CiscoSB)  
 2.4G VAP 1 (CiscoTest)  
 5G VAP 0 (MyNetwork)  
 Ethernet Port

OK Cancel

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

### Details Of Rule(s)



More...

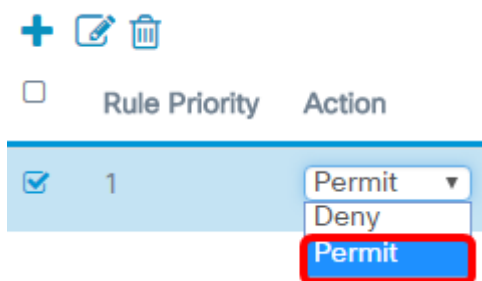
Schritt 8: Klicken Sie auf die **+** Schaltfläche, um eine neue Regel hinzuzufügen.



Rule Priority

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

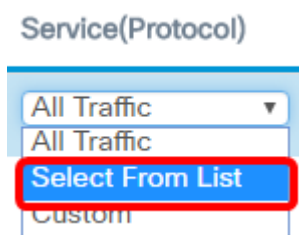
- Zulassen - Mit dieser Option können Pakete, die die ACL-Kriterien erfüllen, eine Verbindung zum Netzwerk herstellen.
- Verweigern: Diese Option verhindert, dass Pakete, die die ACL-Kriterien erfüllen, eine Verbindung zum Netzwerk herstellen.



**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.
- Select From List (Von Liste auswählen): Mit dieser Option können Sie IP, ICMP, 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: Definieren Sie das Protokoll, das mit dem Netzwerk verbunden werden soll. Folgende Optionen stehen zur Verfügung:

- ip - Mit dieser Option können die Hosts, die auf das Netzwerk zugreifen, vom Access Point mithilfe ihrer IP-Adresse als Filter gefiltert werden.
- icmp: Mit dieser Option können vom Access Point eingehende ICMP-Pakete (Internet Control Message Protocol), die über den Access Point in das Netzwerk gelangen, gefiltert werden.
- 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.

Service(Protocol)	Source IPv4 Address
Select From List ▼	Any ▼
ip ▼	
icmp	
igmp	
tcp	
udp	

**Hinweis:** In diesem Beispiel wird ip ausgewählt.

Schritt 12: Definieren Sie die IPv4-Quelladresse aus der Dropdown-Liste Source IPv4 Address (IPv4-Quelladresse). 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.

Source IPv4 Address	Source Port
Any ▼	All Traffic ▼
Any	
Single Address	
Address/Mask	

**Hinweis:** In diesem Beispiel wird die Einzeladresse ausgewählt.

Schritt 13: Geben Sie die IP-Adresse des Hosts ein, der beim Zugriff auf das Netzwerk zugelassen werden soll.

Source IPv4 Address
Single Address ▼
192.168.100.139

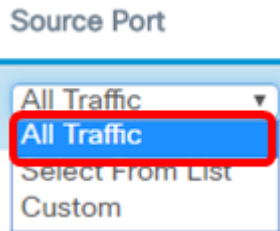
**Hinweis:** In diesem Beispiel wird 192.168.100.139 eingegeben. Dies ist die IP-Adresse von PC2.

Schritt 14: Wählen Sie einen Quellport für die Bedingung aus. Folgende Optionen stehen zur Verfügung:

- All Traffic (Gesamter Datenverkehr): Mit dieser Option werden alle Pakete vom Quellport zugelassen, der die Kriterien erfüllt.
- Wählen Sie From List (Von Liste auswählen) - Mit dieser Option können Sie ftp, ftpdata, 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:

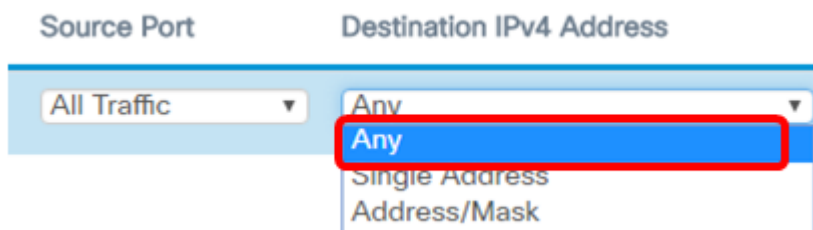
- 0 bis 1023 — Bekannte Ports
- 1024-49151 — Registrierte Ports
- 49152 - 65535 - Dynamische und/oder private Ports



**Hinweis:** In diesem Beispiel wird All Traffic (Gesamter Datenverkehr) ausgewählt.

Schritt 15: Wählen Sie in der Dropdown-Liste Destination IPv4 Address (IPv4-Zieladresse) 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: Mit dieser Option können Sie einen IP-Adressbereich oder eine IP-Maske eingeben.



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

Schritt 16: 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

Schritt 17: Wählen Sie in der Dropdown-Liste Type of Service (Servicetyp) einen Servicetyp aus, der dem Pakettyp entspricht. Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Bei dieser Option werden alle Services als Übereinstimmung für die Pakete behandelt.
- Wählen Sie From List (Von Liste auswählen) aus: Diese Option entspricht den Paketen basierend auf den Werten Differentiated Services Code Point (DSCP), Class of Service (CoS) oder Expedited Forwarding (EF).
- DSCP: Die Option stimmt die Pakete basierend auf ihrem benutzerdefinierten DSCP-Wert zu. Wenn Sie diese Option wählen, geben Sie im Feld DSCP Value (DSCP-Wert) einen Wert zwischen 0 und 63 ein.
- Precedence (Rangfolge) - Diese Option stimmt mit den Paketen auf Basis ihres IP-Rangfolgewerts überein. Wenn diese Option ausgewählt ist, geben Sie einen Wert für die IP-Rangfolge zwischen 0 und 7 ein.
- ToS/Mask (ToS/Maske): Mit dieser Option können Sie eine IP-ToS-Maske eingeben, um die Bitpositionen im IP-ToS-Bits-Wert zu identifizieren, die zum Vergleich mit dem IP-ToS-Feld in einem Paket verwendet werden.

Destination Port	Type Of Service
Any	Any

Any

Select From List

DSCP

Precedence

ToS/Mask

Schritt 18: (Optional) Wiederholen Sie die Schritte 8 bis 17, bis die Zugriffskontrollliste vollständig ist.

**Hinweis:** Da am Ende jeder erstellten Regel eine implizite Verweigerung vorliegt, muss der ACL keine Deny-Regel hinzugefügt werden, um den Zugriff von anderen Geräten im Netzwerk zu verhindern.

Schritt 19: (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.

+
✎
🗑️

Rule Priority

<input type="checkbox"/>	1	▼
<input checked="" type="checkbox"/>	2	▲

Schritt 20: Klicken Sie auf **OK**.



Source Port

Destination IPv4 Address

All Traffic ▾ Any ▾



Schritt 21: Klicken Sie auf **Speichern**.

The screenshot shows the Cisco WAP configuration interface for WAP125-wap5e0940. The "ACL" section is active, and a "Save" button is highlighted with a red box. Below the "ACL Table" header, there is a table with columns for "Enable", "ACL Name", "ACL Type", "Associated Interface", and "Details Of Rule(s)". A single rule is listed with "TestIPv4ACL" as the name and "IPv4" as the type. The associated interfaces are 2.4G VAP 0 (CiscoSB), 2.4G VAP 1 (CiscoTest), 5G VAP 0 (MyNetwork), and Ethernet Port. A "More..." button is visible next to the rule.

Enable	ACL Name	ACL Type	Associated Interface	Details Of Rule(s)
<input checked="" type="checkbox"/>	TestIPv4ACL	IPv4	<ul style="list-style-type: none"><li>2.4G VAP 0 (CiscoSB)</li><li>2.4G VAP 1 (CiscoTest)</li><li>5G VAP 0 (MyNetwork)</li><li>Ethernet Port</li></ul>	<a href="#">More...</a>

Sie sollten jetzt die Einrichtung einer IPv4-ACL abgeschlossen haben, die nur einem Host den Zugriff auf das Netzwerk ermöglicht, wenn er mit dem WAP verbunden ist.