Konfigurieren der Zugriffskontrollliste für MAC, IPv4 und IPv6 auf einem Wireless Access Point

Ziel

Eine Zugriffskontrollliste (Access Control List, ACL) ist eine Liste von Filtern für den Netzwerkverkehr und zugehörigen Aktionen zur Verbesserung der Sicherheit. Sie blockiert nicht autorisierte Benutzer und ermöglicht autorisierten Benutzern den Zugriff auf bestimmte Ressourcen. Eine ACL enthält die Hosts, denen der Zugriff auf das Netzwerkgerät gestattet oder verweigert wird. ACLs können auf zwei Arten definiert werden: IPv4-Adresse oder IPv6-Adresse.

In diesem Artikel erfahren Sie, wie Sie erfolgreich eine ACL erstellen und IPv4-, IPv6- und MAC-basierte Zugriffskontrolllisten (Media Access Control, MAC) auf Ihrem Wireless Access Point (WAP) konfigurieren, um die Netzwerksicherheit zu verbessern.

Anwendbare Geräte

- WAP100-Serie
- WAP300-Serie
- WAP500-Serie

Softwareversion

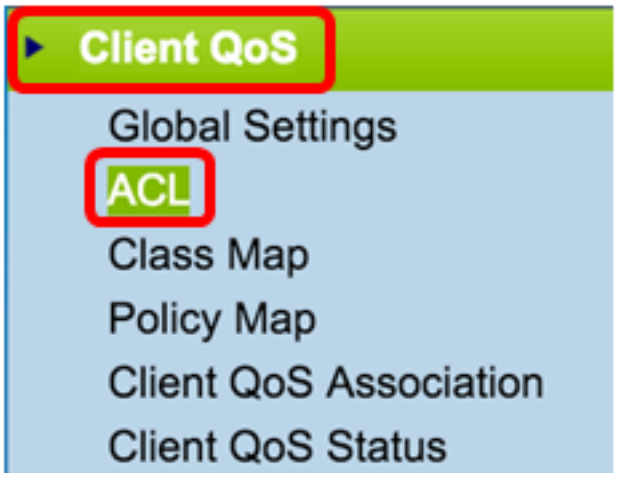
- 1.0.6.2 - WAP121, WAP321
- 1.2.0.2 - WAP371, WAP551, WAP561
- 1.0.1.4 - WAP131, WAP351
- 1.0.0.16 - WAP150, WAP361

ACL erstellen

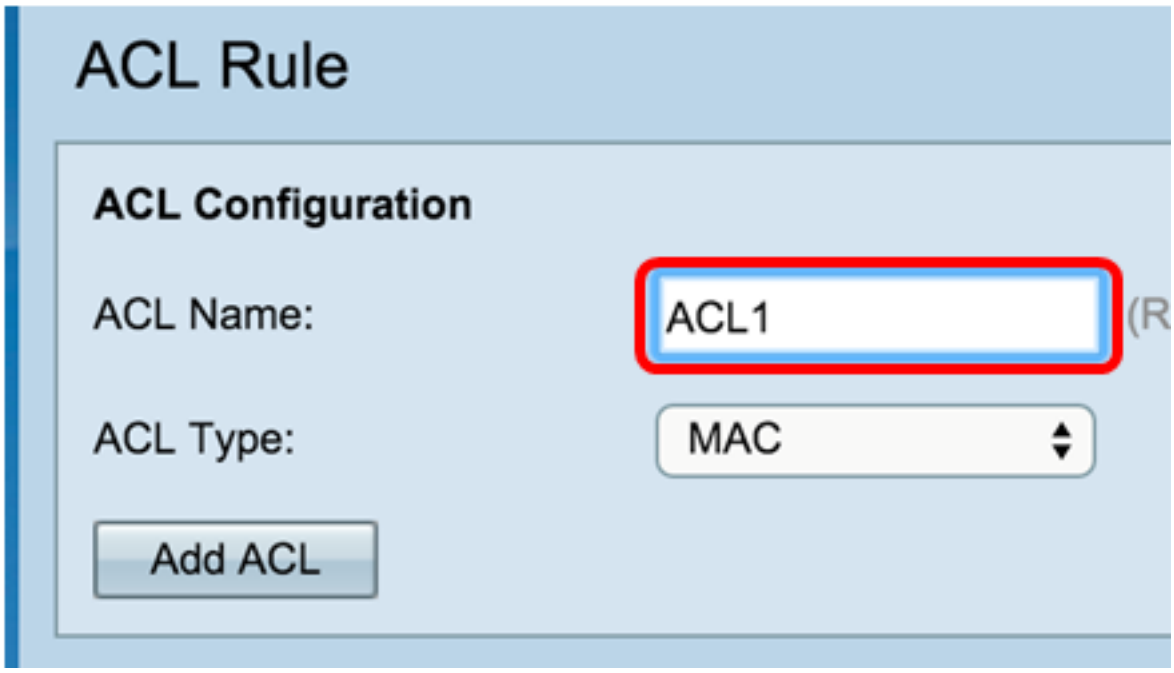
Hinweis: Die für diese Konfiguration verwendeten Bilder stammen aus dem WAP150.

Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm des Access Points an, und wählen Sie **ACL > ACL Rule (ACL > ACL-Regel)**.

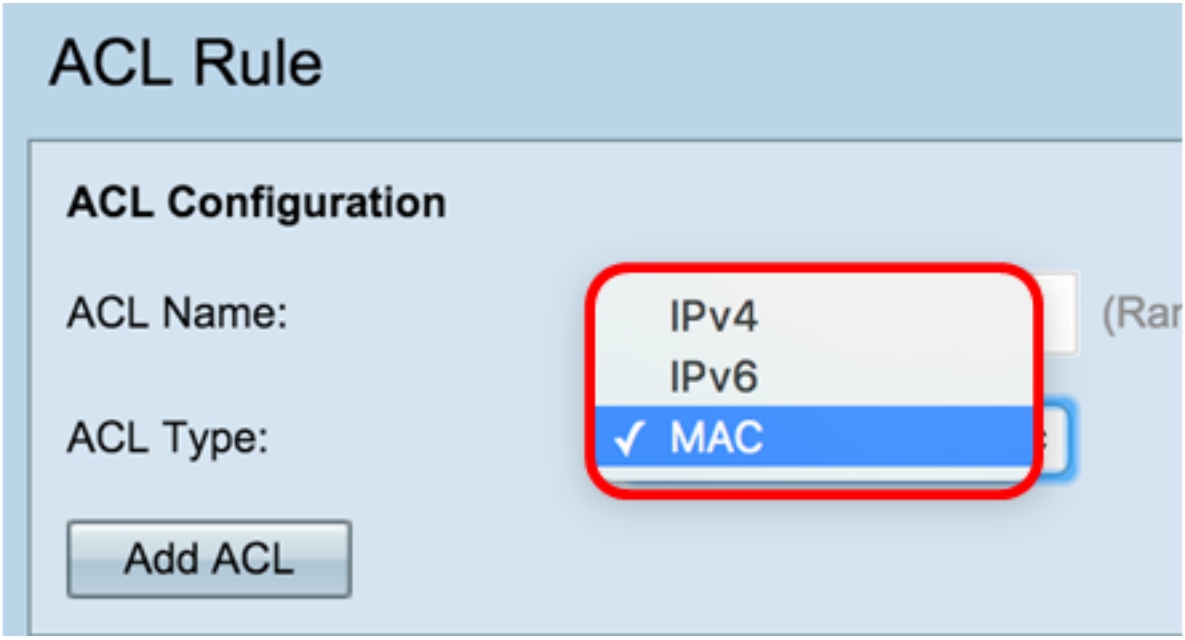
Hinweis: Für WAP121, WAP321, WAP371, WAP551 und WAP561: Melden Sie sich beim webbasierten Access Point-Dienstprogramm an, und wählen Sie Client QoS > ACL aus.



Schritt 2: Wenn die Seite "ACL Configuration" (ACL-Konfiguration) geöffnet ist, geben Sie den Namen der ACL in das Feld *ACL Name (ACL-Name*) ein.

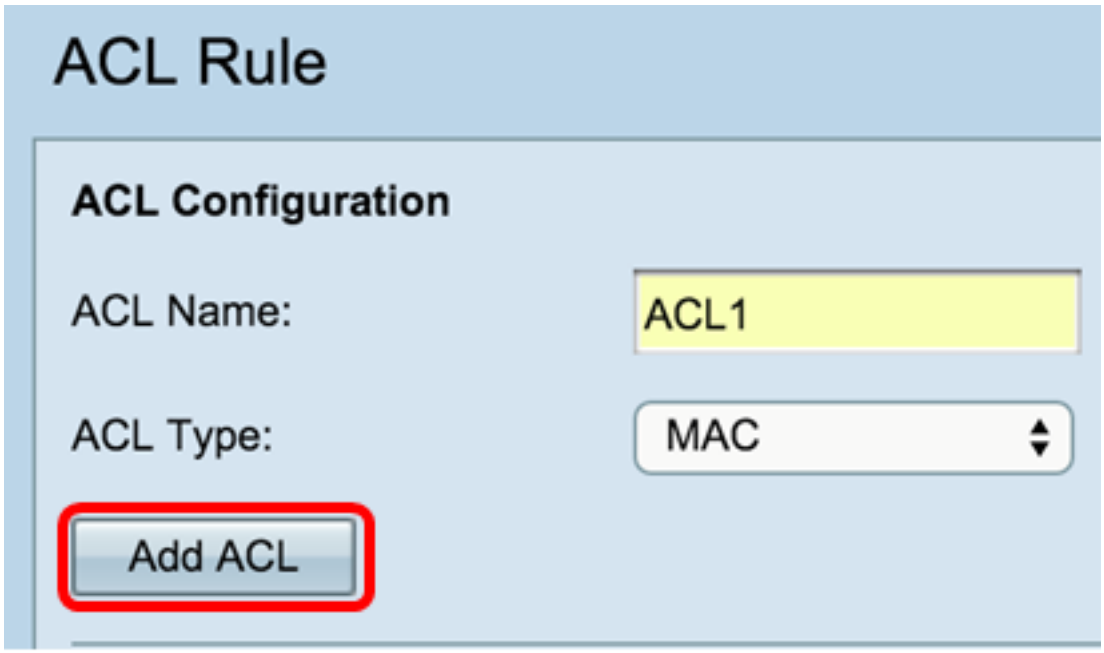


Schritt 3: Wählen Sie einen **ACL-Typ** aus der Dropdown-Liste ACL Type (ACL-Typ) aus.



- IPv4 - Eine 32-Bit-Adresse (4 Byte).
- IPv6 - Ein Nachfolger von IPv4 besteht aus einer 128-Bit-Adresse (8 Byte).
- MAC (MAC-Adresse): Die MAC-Adresse ist die eindeutige Adresse, die einer Netzwerkschnittstelle zugewiesen ist.

Schritt 4: Klicken Sie auf die Schaltfläche **ACL hinzufügen**.



Wenn Sie MAC ausgewählt haben, fahren Sie mit Konfigurieren der MAC-basierten ACL fort.

Wenn Sie IPv4 gewählt haben, fahren Sie mit Konfigurieren der IPv4-basierten Zugriffskontrollliste fort.

Wenn Sie IPv6 gewählt haben, fahren Sie mit Konfigurieren der IPv6-basierten Zugriffskontrollliste fort.

Sie sollten jetzt eine ACL erfolgreich erstellt haben.

MAC-basierte ACL konfigurieren

Schritt 1: Wählen Sie die ACL aus der Dropdown-Liste ACL Name - ACL Type (ACL-Typ) aus, der Sie Regeln hinzufügen möchten.

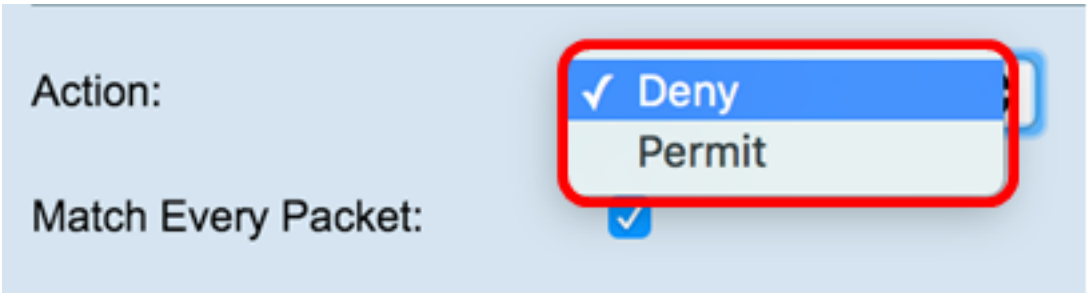
Hinweis: In der Abbildung unten wurde ACL1 MAC als Beispiel ausgewählt.

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

Hinweis: In diesem Beispiel wird eine Deny-Anweisung erstellt.

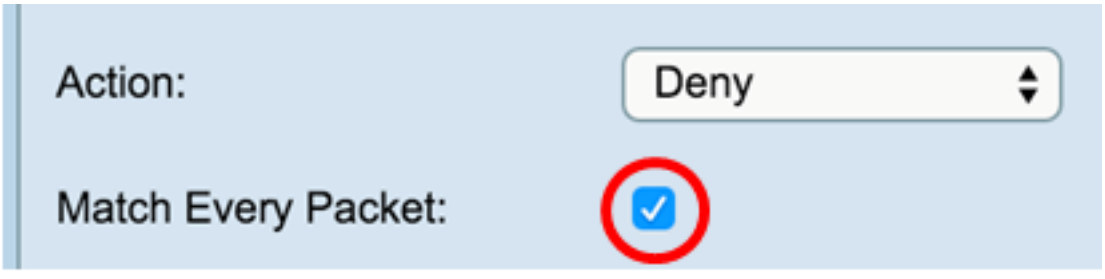


- Verweigern: Blockiert den gesamten Datenverkehr, der die Regelkriterien erfüllt, um in den WAP einzudringen oder diesen zu verlassen. Da am Ende jeder ACL eine implizite Deny-All-Regel vorhanden ist, wird nicht explizit zulässiger Datenverkehr verworfen.
- Zulassen - Ermöglicht allen Datenverkehr, der die Regelkriterien erfüllt, ein- oder auszusteigen. Datenverkehr, der die Kriterien nicht erfüllt, wird verworfen.

Hinweis: Die Schritte 4 bis 11 sind optional. Aktivierte Filter sind aktiviert. Deaktivieren Sie das Kontrollkästchen für den Filter, der nicht auf diese bestimmte Regel angewendet werden soll.

Schritt 4: Aktivieren Sie das Kontrollkästchen **Jedes Paket** zuordnen, um die Regel für jeden Frame oder jedes Paket zu übernehmen, unabhängig vom Inhalt. Deaktivieren Sie das Kontrollkästchen, um eines der zusätzlichen Kriterien für übereinstimmende Segmente zu konfigurieren.

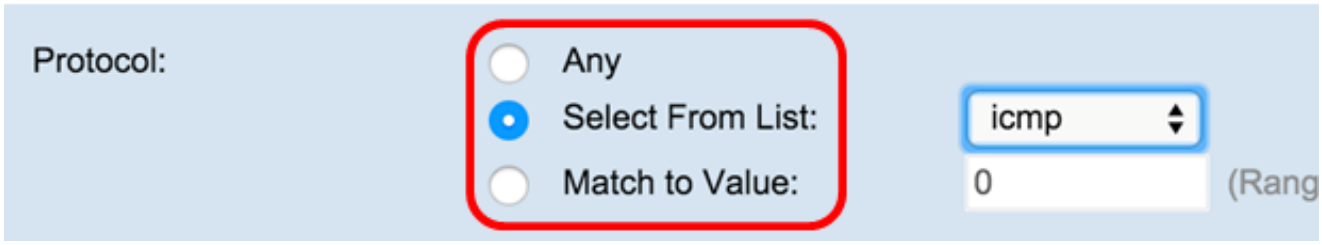
Tipp: Wenn jedes Paket bereits markiert ist, fahren Sie mit Schritt 12 fort.



Schritt 5: Wählen Sie im Bereich EtherType ein Optionsfeld, um die entsprechenden Kriterien mit dem Wert im Header eines Ethernet-Frames zu vergleichen. Sie können eine der folgenden Optionen auswählen oder Any (Beliebig) auswählen:

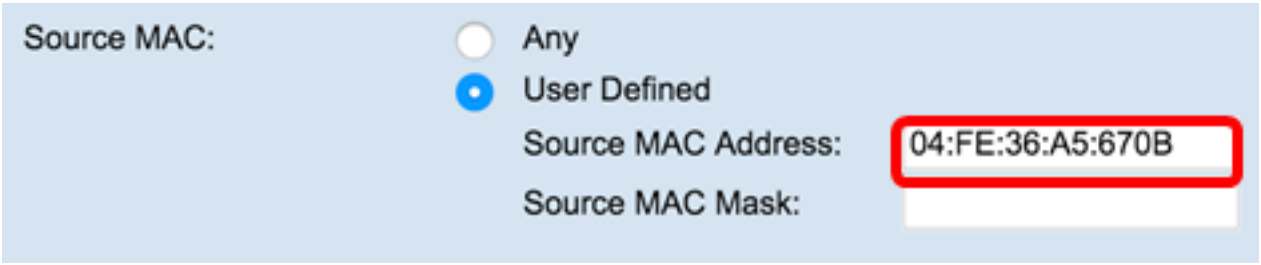
- Wählen Sie Aus Liste aus - Wählen Sie ein Protokoll aus der Dropdown-Liste aus. Die Liste bietet folgende Optionen: appletalk, arp, IPv4, IPv6, ipx, netbios, pppoe.
- Match to Value (Wert zuordnen): Geben Sie für die benutzerdefinierte Protokoll-ID den Bezeichner ein, der zwischen 0600

und FFFF liegt.



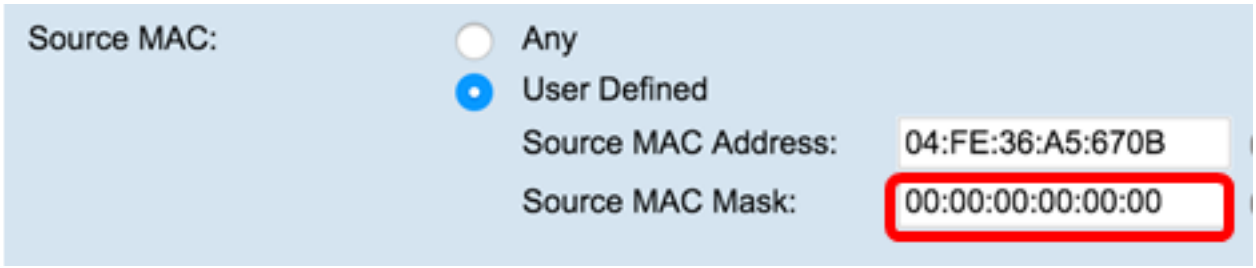
Schritt 6: Wählen Sie im Bereich Class of Service (Serviceklasse) eine Optionsschaltfläche, um die 802.1p-Benutzerpriorität einzugeben, um sie mit einem Ethernet-Frame zu vergleichen. Sie können entweder Any (Beliebig) oder eine benutzerdefinierte Priorität auswählen. Geben Sie im Feld *Benutzerdefiniert* die Priorität zwischen 0 und 7 ein.

Schritt 7: Wählen Sie im Bereich Source MAC (Quelle-MAC) eine Optionsschaltfläche, um die Quell-MAC-Adresse mit einem Ethernet-Frame zu vergleichen. Sie können **Any (Beliebig) auswählen** oder **User Defined (Benutzerdefiniert)** auswählen und die Quell-MAC-Adresse in das Feld eingeben.

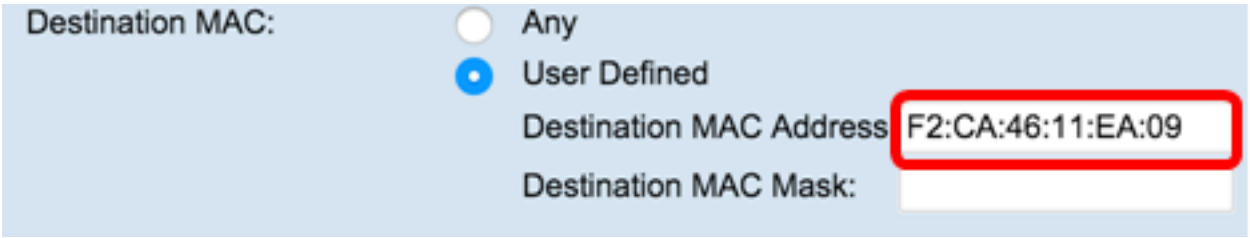


Schritt 8: Geben Sie die Quell-MAC-Adressenmaske in das Feld *Quell-MAC-Maske ein*, das angibt, welche Bits in der Quell-MAC mit einem Ethernet-Frame verglichen werden sollen.

Hinweis: Wenn die MAC-Maske 0 Bit verwendet, wird die Adresse akzeptiert, und wenn sie 1 Bit verwendet, wird die Adresse ignoriert.

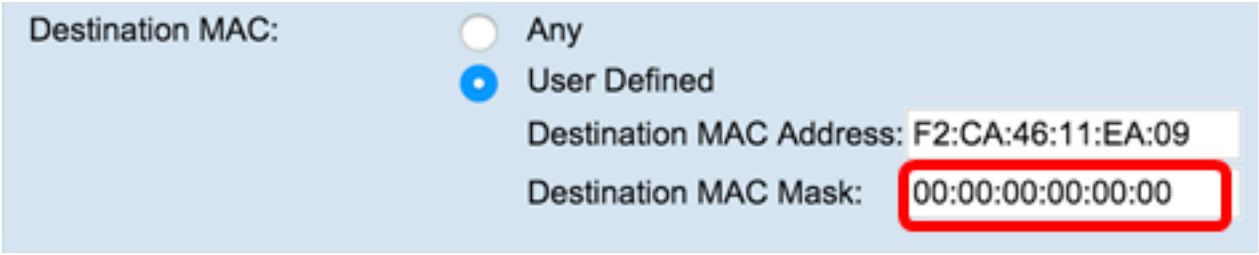


Schritt 9: Wählen Sie im Bereich Ziel MAC (Ziel-MAC) eine Optionsschaltfläche, um die Ziel-MAC-Adresse mit einem Ethernet-Frame zu vergleichen. Sie können entweder "Anyor" (Alle) auswählen oder "User Defined" (Benutzerdefiniert) auswählen und die MAC-Zieladresse in das Feld eingeben.



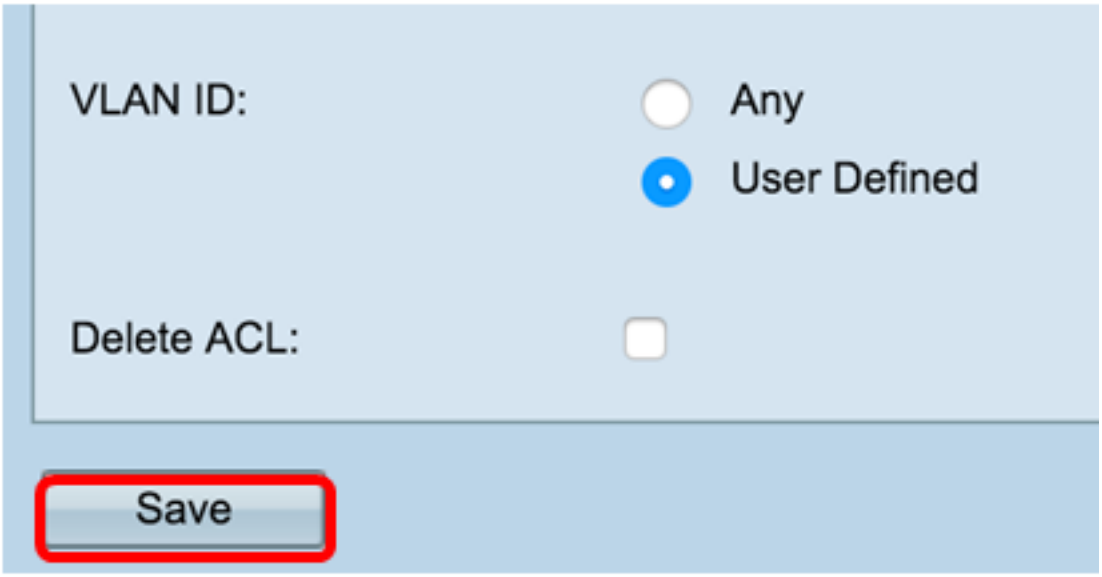
Schritt 10: Geben Sie die MAC-Zieladressenmaske im Feld *Ziel-MAC-Maske ein*, das angibt, welche Bits der MAC-Zieladresse mit einem Ethernet-Frame verglichen werden sollen.

Hinweis: Wenn die MAC-Maske 0 Bit verwendet, wird die Adresse akzeptiert, und wenn sie ein 1 Bit verwendet, wird die Adresse ignoriert.



Schritt 11: Wählen Sie im Bereich für die **VLAN-ID** ein Optionsfeld, um die VLAN-ID mit einem Ethernet-Frame zu vergleichen. Geben Sie in das angegebene Feld die VLAN-ID zwischen 0 und 4095 ein.

Schritt 12: Klicken Sie auf **Speichern**.



Schritt 13: (Optional) Um die konfigurierte ACL zu löschen, aktivieren Sie das Kontrollkästchen **ACL löschen** und klicken Sie anschließend auf **Speichern**.

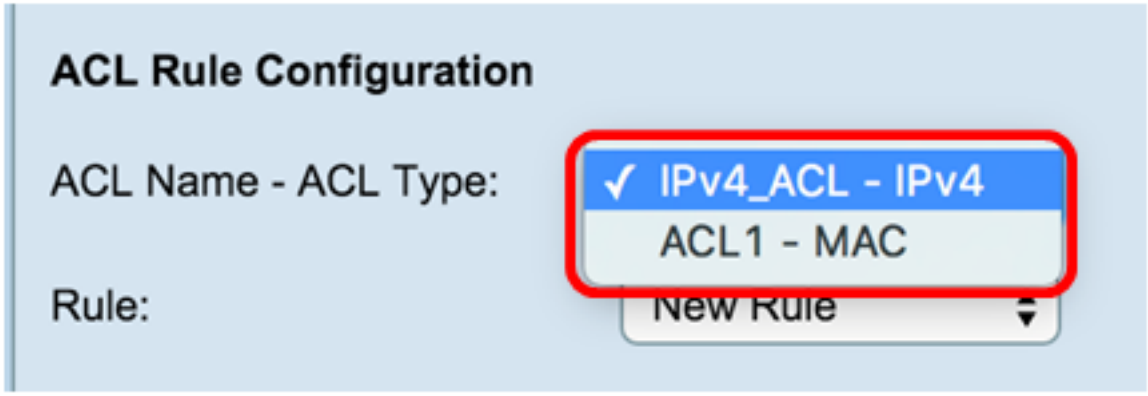
Sie sollten jetzt die MAC-ACL auf Ihrem WAP erfolgreich konfiguriert haben.

Konfigurieren der IPv4-basierten ACL

Schritt 1: Konfigurieren Sie im Bereich "ACL Rule Configuration" die folgenden Regelparameter:

ACL-Name - ACL-TypWählen Sie die ACL aus, die mit der neuen Regel konfiguriert werden soll.

Hinweis: In der Abbildung unten wurde IPv4_ACL-IPv4 als Beispiel ausgewählt.



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

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

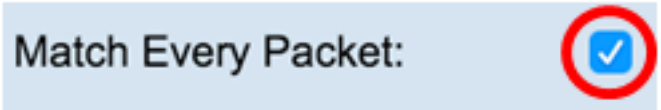
Schritt 3: Wählen Sie die Aktion für die ACL-Regel aus der Dropdown-Liste *Aktion* aus.

Hinweis: In diesem Beispiel wird eine Permit-Anweisung erstellt.

- Verweigern: Blockiert den gesamten Datenverkehr, der die Regelkriterien erfüllt, um in den WAP einzudringen oder diesen zu verlassen. Da am Ende jeder ACL eine implizite Deny-All-Regel vorhanden ist, wird nicht explizit zulässiger Datenverkehr verworfen.
- Zulassen - Ermöglicht allen Datenverkehr, der die Regelkriterien erfüllt, ein- oder auszusteigen. Datenverkehr, der die Kriterien nicht erfüllt, wird verworfen.

Hinweis: Die Schritte 4 bis 9 sind optional. Aktivierte Filter sind aktiviert. Deaktivieren Sie das Kontrollkästchen für den Filter, wenn er nicht auf diese bestimmte Regel angewendet werden soll.

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



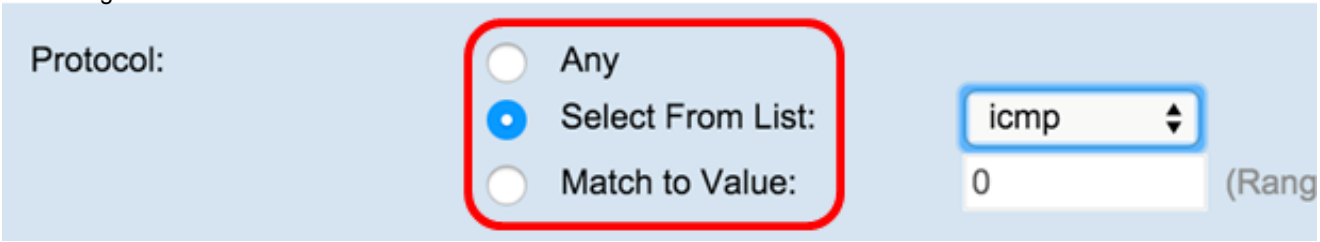
Tipp: Jedes Paket zuordnen ist standardmäßig aktiviert. Wenn Sie diese Einstellung beibehalten möchten, fahren Sie mit Schritt 11 fort.

Schritt 5: Wählen Sie im Bereich Protocol (Protokoll) ein Optionsfeld, um die entsprechenden Kriterien mit dem Wert im Header eines Ethernet-Frames zu vergleichen. Sie können Any (Beliebig) auswählen oder aus der Dropdown-Liste auswählen.

- Aus Liste auswählen - Wählen Sie eines der folgenden Protokolle aus:

— IP — Das Kommunikationsprotokoll, das in der Internet Protocol Suite für die Übertragung von Daten über Netzwerke hinweg verwendet wird.
— ICMP — Ein Protokoll in der Internet Protocol Suite, das von Geräten wie Routern verwendet wird, um Fehlermeldungen zu senden.
— IGMP - Ein Kommunikationsprotokoll, das vom Host verwendet wird, um Multicast-Gruppenzugehörigkeiten in IPv4-Netzwerken einzurichten.
— TCP — Ermöglicht zwei Hosts, eine Verbindung herzustellen und Datenströme auszutauschen.
— UDP — Ein Protokoll in der Internet Protocol Suite, das ein verbindungsloses Übertragungsmodell verwendet.

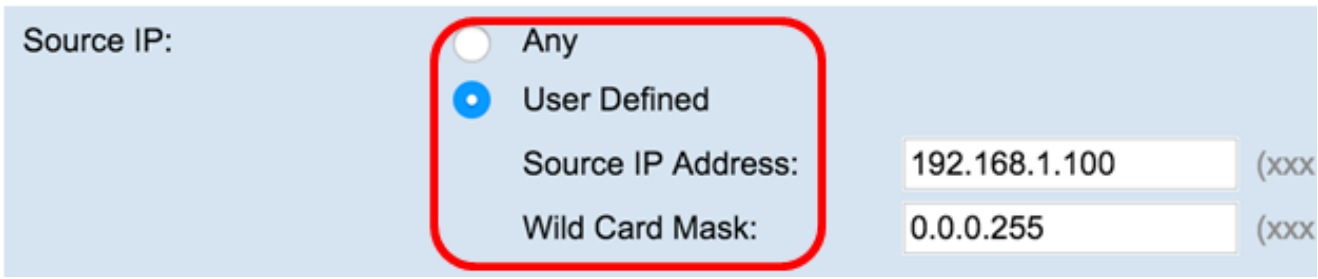
- Match to Value (Wert zuordnen) - Geben Sie eine standardmäßige IANA-zugeordnete Protokoll-ID zwischen 0 und 255 ein. Wählen Sie diese Methode aus, um ein Protokoll zu identifizieren, das in der Liste Select From (Aus auswählen) nicht nach Namen aufgeführt ist.



Schritt 6: Wählen Sie im Bereich Source IP (Quell-IP) ein Optionsfeld aus, um die IP-Adresse der Quelle in der Übereinstimmung-Bedingung einzuschließen. Sie können Any (Beliebig) oder User Defined (Benutzerdefiniert) auswählen und dann die IP-Adresse und die Platzhaltermaske der Quelle in die entsprechenden Felder eingeben.

- Quell-IP-Adresse - Geben Sie eine IP-Adresse ein, um diese Kriterien anzuwenden.
- Wild Card Mask (Platzhaltermaske): Geben Sie die Platzhaltermaske für die IP-Zieladresse ein. Die Platzhaltermaske bestimmt, welche Bits verwendet und welche ignoriert werden. Die Platzhaltermaske 255.255.255.255 gibt an, dass kein Bit wichtig ist. Eine Platzhalterkarte von 0.0.0.0 gibt an, dass alle Bits wichtig sind. Dieses Feld ist erforderlich, wenn Quell-IP-Adresse ausgewählt ist.

Hinweis: Eine Platzhaltermaske ist im Grunde das Umkehren einer Subnetzmaske. Um beispielsweise die Kriterien einer einzelnen Hostadresse zuzuordnen, verwenden Sie die Platzhaltermaske 0.0.0.0. Um die Kriterien mit einem 24-Bit-Subnetz (z. B. 192.168.10.0/24) abzugleichen, verwenden Sie die Maske der Platzhalterkarte 0.0.0.255.



Schritt 7: Wählen Sie im Bereich Source Port (Quellport) ein Optionsfeld aus, um einen Quellport in den Match-Zustand einzuschließen. Sie können Any (Alle) auswählen, um eine Übereinstimmung mit einem beliebigen Quellport herzustellen, oder Sie können Folgendes auswählen:

- Wählen Sie Aus Liste aus: Wählen Sie einen Quellport aus der Dropdown-Liste "Aus Liste auswählen" aus. Folgende

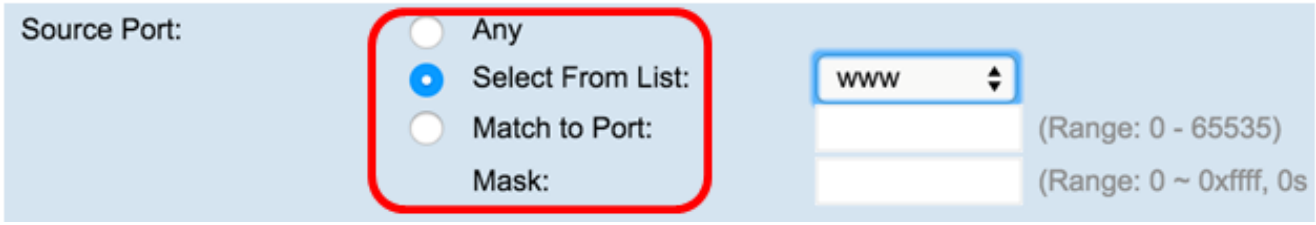
Optionen sind verfügbar:

— File Transfer Protocol (FTP) - FTP ist ein Standard-Netzwerkprotokoll, das verwendet wird, um Dateien von einem Host zu einem anderen über ein TCP-basiertes Netzwerk (Transmission Control Protocol) wie das Internet zu übertragen.
— FTP-Daten — Ein Datenkanal, der vom Server initiiert wird, der mit einem Client verbunden ist, in der Regel über Port 20.
- Hypertext Transfer Protocol (HTTP) - HTTP ist ein Anwendungsprotokoll, das die Grundlage der Datenkommunikation für das World Wide Web bildet.
— Simple Mail Transfer Protocol (SMTP) - SMTP ist ein Internet-Standard für die Übertragung von E-Mails (E-Mail).
— Simple Network Management Protocol (SNMP) - SNMP ist ein Internetstandardprotokoll für die Verwaltung von Geräten in IP-Netzwerken.
— Telnet — Ein Sitzungsschichtprotokoll, das im Internet oder in lokalen Netzwerken verwendet wird, um bidirektionale interaktive textorientierte Kommunikation bereitzustellen.
— Trivial File Transfer Protocol (TFTP) - TFTP ist ein Internet-Software-Dienstprogramm zum Übertragen von Dateien, das einfacher zu verwenden ist als FTP, aber weniger fähig ist.
— World Wide Web (WWW) - WWW ist ein System von Internetservern, die HTTP-formatierte Dokumente unterstützen.

- Match to Port (Zuordnung zum Port) - Geben Sie die Portnummer ein, die nicht in der Liste angezeigt wird. Portnummern liegen im Feld *Übereinstimmung mit Port* zwischen 0 und 65535 für nicht aufgeführte Quell-Ports. Der Bereich umfasst drei verschiedene Port-Typen. Die Bereiche werden wie folgt beschrieben:

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

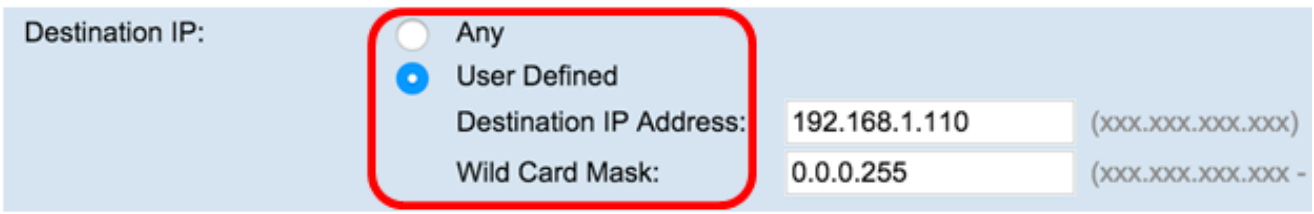
- Maske - Geben Sie die Portmaske ein. Die Maske bestimmt, welche Bits verwendet und welche ignoriert werden. Nur die Hexadezimalziffer (0 - 0xFFFF) ist zulässig. 0 bedeutet, dass das Bit zählt und 1 bedeutet, dass Sie dieses Bit ignorieren sollten.



Schritt 8: Wählen Sie im Bereich Destination IP (Ziel-IP) ein Optionsfeld aus, um die IP-Adresse des Ziels in der Übereinstimmung-Bedingung einzuschließen. Sie können Any (Beliebig) oder User Defined (Benutzerdefiniert) auswählen und dann die IP-Adresse und die Platzhaltermaske des Ziels in die entsprechenden Felder eingeben.

- Ziel-IP-Adresse - Geben Sie eine IP-Adresse ein, um diese Kriterien anzuwenden.
- Wild Card Mask (Platzhaltermaske): Geben Sie die Platzhaltermaske für die IP-Zieladresse ein. Die Platzhaltermaske bestimmt, welche Bits verwendet und welche ignoriert werden. Die Platzhaltermaske 255.255.255.255 gibt an, dass kein Bit wichtig ist. Eine Platzhalterkarte von 0.0.0.0 gibt an, dass alle Bits wichtig sind. Dieses Feld ist erforderlich, wenn die Ziel-IP-Adresse ausgewählt wurde.

Hinweis: Eine Platzhaltermaske ist im Grunde das Umkehren einer Subnetzmaske. Um beispielsweise die Kriterien einer einzelnen Hostadresse zuzuordnen, verwenden Sie die Platzhaltermaske 0.0.0.0. Um die Kriterien mit einem 24-Bit-Subnetz (z. B. 192.168.10.0/24) abzugleichen, verwenden Sie die Maske der Platzhalterkarte 0.0.0.255.



Schritt 9: Wählen Sie im Bereich "Destination Port" (Zielport) ein Optionsfeld aus, um einen Zielport in den Abgleichzustand einzuschließen. Sie können Any (Beliebig) auswählen, um eine Übereinstimmung mit einem beliebigen Zielport

herzustellen, oder Sie können Folgendes auswählen:

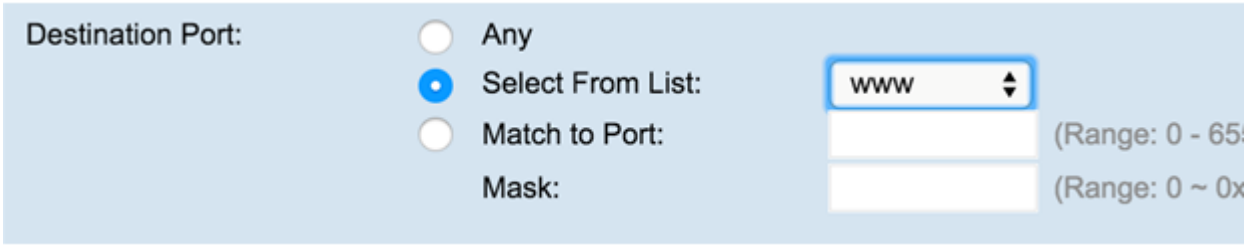
- Wählen Sie Aus Liste aus: Wählen Sie einen Zielport aus der Dropdown-Liste aus. Folgende Optionen sind verfügbar:

— FTP — Ein Standard-Netzwerkprotokoll, das verwendet wird, um Dateien über ein TCP-basiertes Netzwerk wie das Internet von einem Host zu einem anderen zu übertragen.
— FTP-Daten — Ein Datenkanal, der vom Server initiiert wird, der mit einem Client verbunden ist, in der Regel über Port 20.
— HTTP — Ein Anwendungsprotokoll, das die Grundlage der Datenkommunikation für das World Wide Web bildet.
— SMTP — Ein Internetstandard für die elektronische Post (E-Mail)-Übertragung.
— SNMP — Ein Internetstandardprotokoll zur Verwaltung von Geräten in IP-Netzwerken.
— Telnet — Ein Sitzungsschichtprotokoll, das im Internet oder in lokalen Netzwerken verwendet wird, um bidirektionale interaktive textorientierte Kommunikation bereitzustellen.
— TFTP — Ein Internet-Software-Dienstprogramm zum Übertragen von Dateien, die einfacher zu verwenden als FTP, aber weniger leistungsfähig sind.
— WWW — Ein System von Internetservern, die HTTP-formatierte Dokumente unterstützen.

- Match to Port (Zuordnung zum Port) - Geben Sie die Portnummer ein, die nicht in der Liste angezeigt wird. Portnummern liegen im Feld *Übereinstimmung mit Port* zwischen 0 und 65535 für nicht aufgeführte Quell-Ports. Der Bereich umfasst drei verschiedene Port-Typen. Die Bereiche werden wie folgt beschrieben:

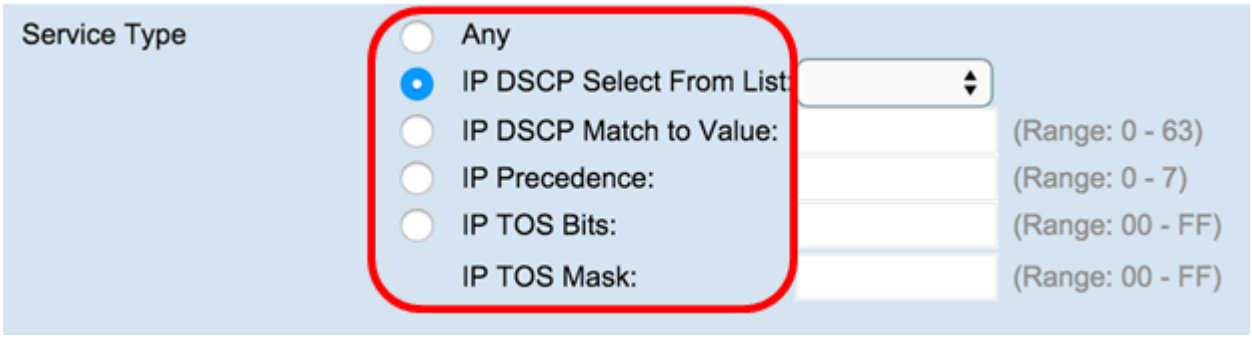
— 0 bis 1023 — Bekannte Ports
— 1024 bis 49151 — Registrierte Ports
— 49152 bis 65535 — Dynamische und/oder private Ports

- Maske - Geben Sie die Portmaske ein. Die Maske bestimmt, welche Bits verwendet und welche ignoriert werden. Nur die Hexadezimalziffer (0-0xFFFF) ist zulässig. 0 bedeutet, dass das Bit zählt und 1 bedeutet, dass Sie dieses Bit ignorieren sollten.

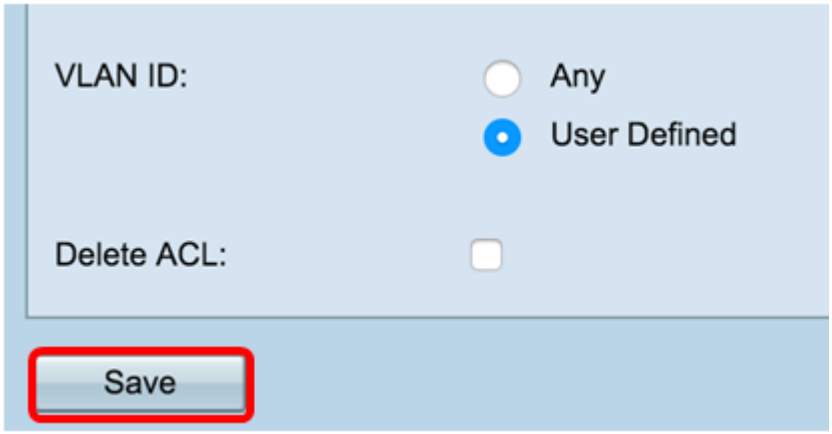


Schritt 10: Wählen Sie im Bereich "Service Type" (Servicetyp) eine Optionsschaltfläche, um Pakete basierend auf einem bestimmten Servicetyp zuzuordnen. Sie können Any (Beliebig) auswählen oder aus den folgenden Optionen auswählen:

- IP DSCP Select From List (IP-DSCP-Auswahl aus Liste): Entspricht den Paketen basierend auf den Werten für AS (Assured Forwarding), CS (Class of Service) oder EF (Expedited Forwarding).
- IP DSCP Match to Value (IP-DSCP-Übereinstimmung mit Wert): Ordnet die Pakete auf der Grundlage eines benutzerdefinierten DSCP-Werts zu. Wenn ausgewählt, geben Sie in diesem Feld einen Wert zwischen 0 und 63 ein.
- IP Precedence (IP-Rangfolge): Ordnet die Pakete ihrem IP-Rangfolgewert zu. Wenn ausgewählt, geben Sie einen Wert für die IP-Rangfolge zwischen 0 und 7 ein.
- IP TOS Bits - Gibt einen Wert an, der die TOS-Bits der Pakete im IP-Header als Abgleichskriterien verwendet.
- Das IP TOS-Feld in einem Paket ist als alle acht Bit des Service Type-Oktetts im IP-Header definiert. Der IP TOS Bits-Wert ist eine zweistellige Hexadezimalzahl zwischen 00 und ff. Die drei Bits höherer Ordnung stellen den Wert für die IP-Rangfolge dar. Die sechs Bit in hoher Reihenfolge stellen den IP-DSCP-Wert dar.
- IP TOS Mask (IP-TOS-Maske): Geben Sie einen IP TOS Mask-Wert ein, um die Bitpositionen im IP TOS Bits-Wert zu identifizieren, die für den Vergleich mit dem IP TOS-Feld in einem Paket verwendet werden.
- Der IP TOS Mask-Wert ist eine zweistellige Hexadezimalzahl von 00 bis FF, die eine invertierte (d. h. wilde Karten) Maske darstellt. Die Null-Werte-Bits in der IP-TOS-Maske geben die Bitpositionen im IP-TOS-Bits-Wert an, die für den Vergleich mit dem IP-TOS-Feld eines Pakets verwendet werden. Um z. B. zu prüfen, ob ein IP TOS-Wert mit den Bits 7 und 5 festgelegt und Bit 1 eindeutig ist, wobei Bit 7 für den höchsten Wert steht, verwenden Sie einen IP TOS Bits-Wert von 0 und eine IP TOS Mask von 00.



Schritt 11: Klicken Sie auf Speichern.



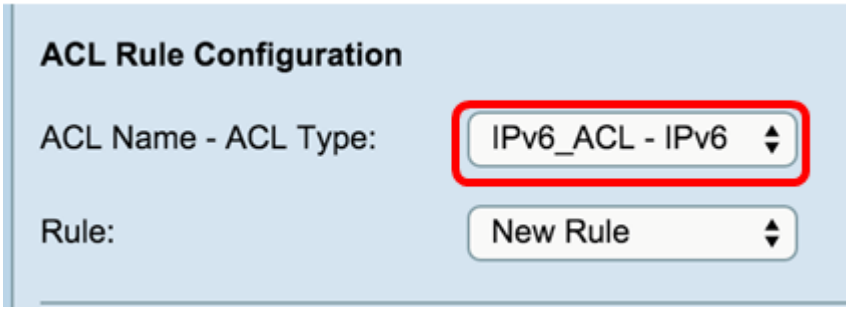
Sie sollten jetzt eine IPv4-basierte ACL erfolgreich konfiguriert haben.

Konfigurieren der IPv6-basierten ACL

Schritt 1: Konfigurieren Sie im Bereich "ACL Rule Configuration" die folgenden Regelparameter:

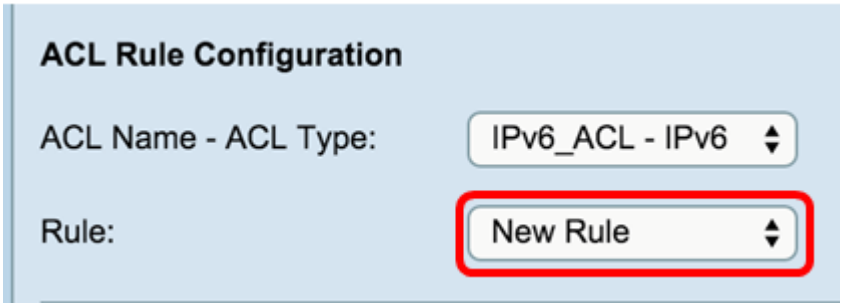
ACL Name (ACL-Name) - ACL Type (ACL-Typ) - Wählen Sie die ACL aus, die mit der neuen Regel konfiguriert werden soll.

Hinweis: In der Abbildung unten wurde IPv6_ACL — IPv6 als Beispiel ausgewählt.



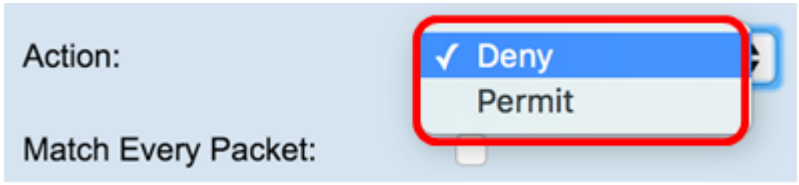
Schritt 2: Wenn für die ausgewählte ACL eine neue Regel konfiguriert werden muss, wählen Sie in der Dropdown-Liste Regel die Option Neue Regel aus. Wählen Sie andernfalls eine der aktuellen Regeln aus der Dropdown-Liste Regel aus.

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



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

- Verweigern: Blockiert den gesamten Datenverkehr, der die Regelkriterien erfüllt, um in den WAP einzudringen oder diesen zu verlassen. Da am Ende jeder ACL eine implizite Deny-All-Regel vorhanden ist, wird nicht explizit zulässiger Datenverkehr verworfen.
- Zulassen - Ermöglicht allen Datenverkehr, der die Regelkriterien erfüllt, ein- oder auszusteigen. Datenverkehr, der die Kriterien nicht erfüllt, wird verworfen.



Hinweis: Die Schritte 4 bis 11 sind optional. Aktivierte Filter sind aktiviert. Deaktivieren Sie das Kontrollkästchen für den Filter, wenn er nicht auf diese bestimmte Regel angewendet werden soll.

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

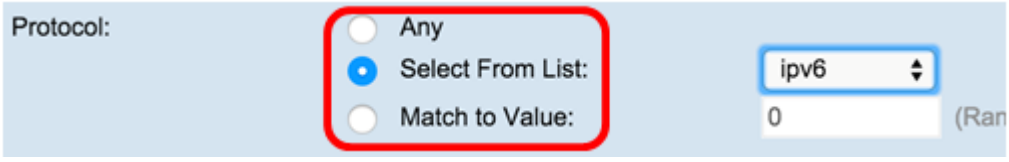
Tipp: Jedes Paket zuordnen ist standardmäßig aktiviert. Wenn Sie diese Einstellung beibehalten möchten, fahren Sie mit Schritt 12 fort.

Schritt 5: Wählen Sie im Bereich Protocol (Protokoll) ein Optionsfeld, um die entsprechenden Kriterien mit dem Wert im Header eines Ethernet-Frames zu vergleichen. Sie können eine der folgenden Optionen auswählen oder Any (Beliebig) auswählen:

- Aus Liste auswählen - Wählen Sie eines der folgenden Protokolle aus:

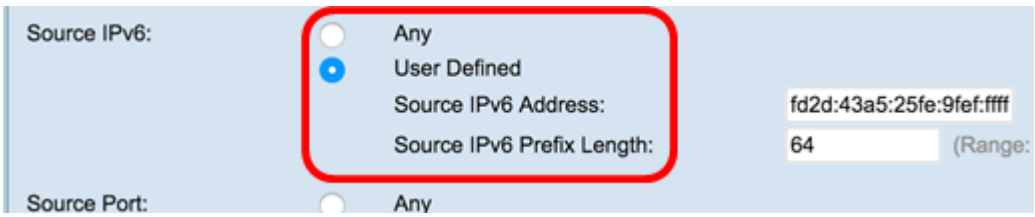
— IP — Das Kommunikationsprotokoll, das in der Internet Protocol Suite für die Übertragung von Daten über Netzwerke hinweg verwendet wird.
— ICMP — Ein Protokoll in der Internet Protocol Suite, das von Geräten wie Routern verwendet wird, um Fehlermeldungen zu senden.
— IGMP - Ein Kommunikationsprotokoll, das vom Host verwendet wird, um Multicast-Gruppenzugehörigkeiten in IPv4-Netzwerken einzurichten.
— TCP — Ermöglicht zwei Hosts, eine Verbindung herzustellen und Datenströme auszutauschen.
— UDP — Ein Protokoll in der Internet Protocol Suite, das ein verbindungsloses Übertragungsmodell verwendet.

- Match to Value (Wert zuordnen) - Geben Sie eine standardmäßige IANA-zugeordnete Protokoll-ID zwischen 0 und 255 ein. Wählen Sie diese Methode aus, um ein Protokoll zu identifizieren, das in der Liste Select From (Aus auswählen) nicht nach Namen aufgeführt ist.



Schritt 6: Wählen Sie im Bereich Source IPv6 (Quelle: IPv6) ein Optionsfeld aus, um die IP-Adresse der Quelle in den Match-Zustand einzubeziehen. Sie können Any (Beliebig) oder User Defined (Benutzerdefiniert) auswählen und dann die IPv6-Adresse und die IPv6-Quell-Präfixlänge eingeben.

- IPv6-Quelladresse - Geben Sie eine IPv6-Adresse ein, um diese Kriterien anzuwenden.
- Quell-IPv6-Präfixlänge - Geben Sie die Präfixlänge der Quell-IPv6-Adresse ein.



Schritt 7: Wählen Sie im Bereich *Quellport* ein Optionsfeld aus, um einen Quellport in den Match-Zustand einzuschließen. Sie

können Any (Beliebig) auswählen, um eine Übereinstimmung mit einem beliebigen Quellport herzustellen, oder Sie können Folgendes auswählen:

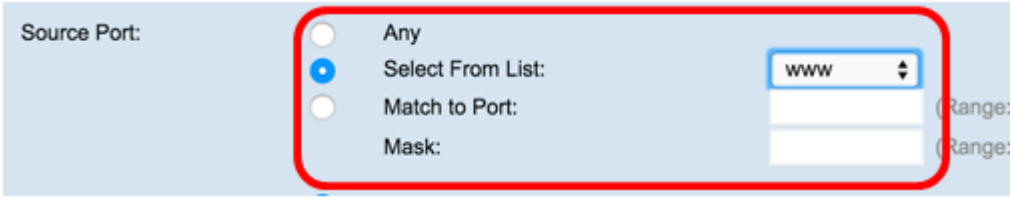
- Wählen Sie Aus Liste aus: Wählen Sie einen Quellport aus der Dropdown-Liste *Wählen Sie aus*. Folgende Optionen sind verfügbar:

— FTP — Ein Standard-Netzwerkprotokoll, das verwendet wird, um Dateien über ein TCP-basiertes Netzwerk wie das Internet von einem Host zu einem anderen zu übertragen.
— FTP-Daten — Ein Datenkanal, der vom Server initiiert wird, der mit einem Client verbunden ist, in der Regel über Port 20.
— HTTP — Ein Anwendungsprotokoll, das die Grundlage der Datenkommunikation für das World Wide Web bildet.
— SMTP — Ein Internetstandard für die elektronische Post (E-Mail)-Übertragung.
— SNMP — Ein Internetstandardprotokoll zur Verwaltung von Geräten in IP-Netzwerken.
— Telnet — Ein Sitzungsschichtprotokoll, das im Internet oder in lokalen Netzwerken verwendet wird, um bidirektionale interaktive textorientierte Kommunikation bereitzustellen.
— TFTP — Ein Internet-Software-Dienstprogramm zum Übertragen von Dateien, die einfacher zu verwenden als FTP, aber weniger leistungsfähig sind.
— WWW — Ein System von Internetservern, die HTTP-formatierte Dokumente unterstützen.

- Match to Port (Zuordnung zum Port) - Geben Sie die Portnummer ein, die nicht in der Liste angezeigt wird. Portnummern liegen im Feld *Übereinstimmung mit Port* zwischen 0 und 65535 für nicht aufgeführte Quell-Ports. Der Bereich umfasst drei verschiedene Port-Typen. Die Bereiche werden wie folgt beschrieben:

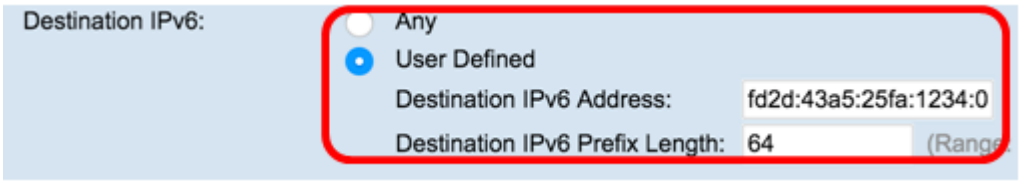
— 0 bis 1023 — Bekannte Ports
— 1024 bis 49151 — Registrierte Ports
— 49152 bis 65535 — Dynamische und/oder private Ports

- Maske - Geben Sie die Portmaske ein. Die Maske bestimmt, welche Bits verwendet und welche ignoriert werden. Nur die Hexadezimalziffer (0 â 0xFFFF) ist zulässig. 0 bedeutet, dass das Bit zählt und 1 bedeutet, dass Sie dieses Bit ignorieren sollten.



Schritt 8: Wählen Sie im Bereich Destination IPv6 (Ziel-IPv6) ein Optionsfeld aus, um die IP-Adresse des Ziels in der Match-Bedingung einzuschließen. Sie können Any (Beliebig) auswählen oder User Defined (Benutzerdefiniert) auswählen. Geben Sie die IPv6-Adresse und die Ziel-IPv6-Präfixlänge ein.

- Ziel-IPv6-Adresse - Geben Sie eine IPv6-Adresse ein, um diese Kriterien anzuwenden.
- Ziel-IPv6-Präfixlänge - Geben Sie die Präfixlänge der Ziel-IPv6-Adresse ein.

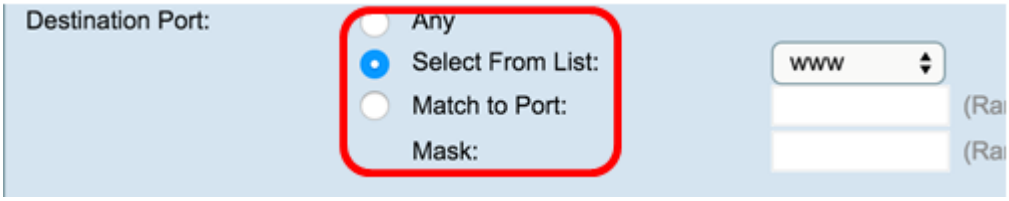


Schritt 9: Wählen Sie im Bereich "Destination Port" (Zielport) ein Optionsfeld aus, um einen Zielport in den Abgleichzustand einzuschließen. Sie können Any (Beliebig) auswählen, um eine Übereinstimmung mit einem beliebigen Zielport herzustellen, oder Sie können Folgendes auswählen:

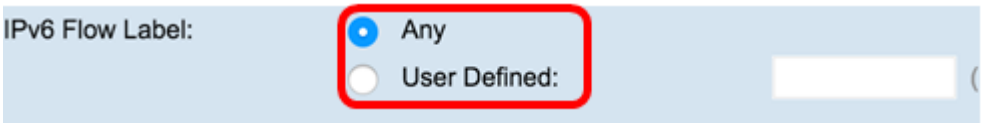
- Wählen Sie Aus Liste aus: Wählen Sie einen Zielport aus der Dropdown-Liste *Select From List (Aus Liste auswählen)* aus. Die Optionen sind FTP, FTP-Daten, HTTP, SNMP, SMTP, TFTP, Telnet, WWW.
- Match to Port (Zuordnung zum Port) - Geben Sie die Portnummer ein, die nicht in der Liste angezeigt wird. Portnummern liegen im Feld *Übereinstimmung mit Port* zwischen 0 und 65535 für nicht aufgeführte Quell-Ports. Der Bereich umfasst drei verschiedene Port-Typen. Die Bereiche werden wie folgt beschrieben:

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

- Maske - Geben Sie die Portmaske ein. Die Maske bestimmt, welche Bits verwendet und welche ignoriert werden. Nur die Hexadezimalziffer (0-0xFFFF) ist zulässig. 0 bedeutet, dass das Bit zählt und 1 bedeutet, dass Sie dieses Bit ignorieren sollten.

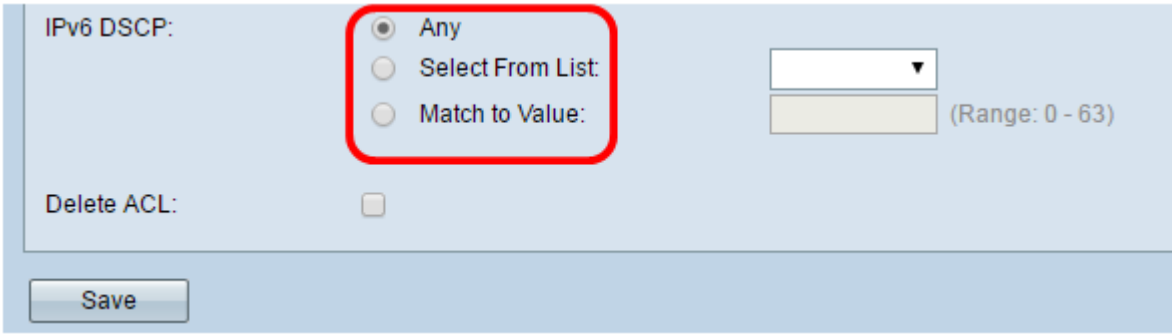


Schritt 10: Wählen Sie im Bereich "IPv6 Flow Label" (IPv6-Flussbezeichnung) ein Optionsfeld aus, um die IPv6-Flussbezeichnung in den Abgleichzustand aufzunehmen. Sie können Any (Beliebig) oder User Defined (Benutzerdefiniert) auswählen und eine 20-Bit-Nummer eingeben, die für ein IPv6-Paket eindeutig ist. Der Bereich liegt zwischen 0 und 0xffff.

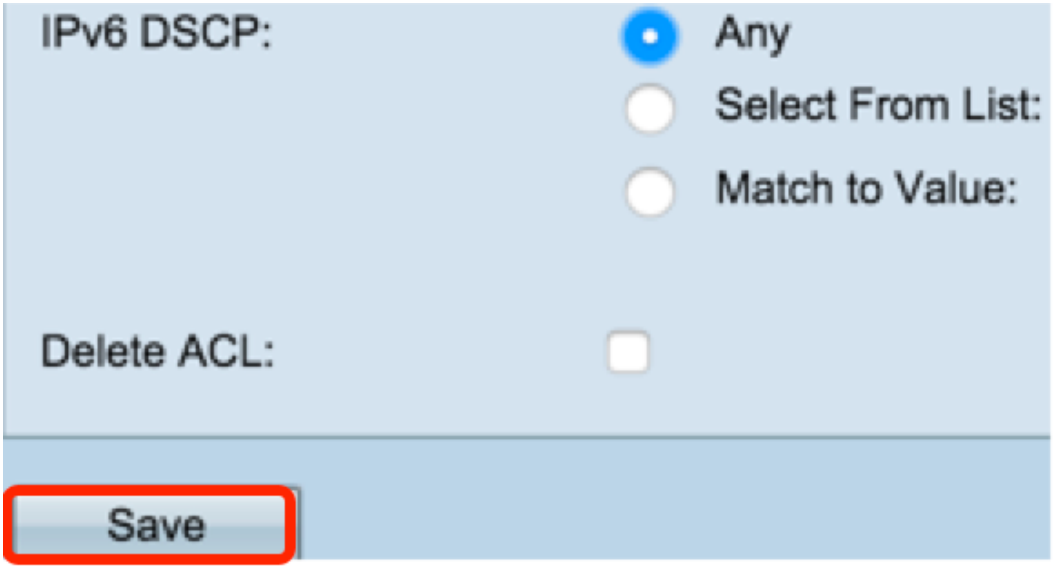


Schritt 11: Wählen Sie im IPv6 DSCP-Bereich eine Optionsschaltfläche, um Pakete ihrem IP-DSCP-Wert zuzuordnen. Sie können Any (Beliebig) auswählen oder Folgendes auswählen:

- Aus Liste auswählen - Wählen Sie einen der folgenden Werte aus: DSCP Assured Forwarding (AF), Class of Service (CS) oder Expedited Forwarding (EF).
- Match to Value (Dem Wert zuordnen): Geben Sie einen benutzerdefinierten DSCP-Wert zwischen 0 und 63 ein.



Schritt 12: Klicken Sie auf Speichern.



Schritt 13: (Optional) Um eine ACL zu löschen, stellen Sie sicher, dass der ACL-Name in der Liste ACL Name-ACL Type (ACL-Namen - ACL-Typ) ausgewählt ist. Aktivieren Sie dann die Option Delete ACL (ACL löschen).

Sie sollten jetzt eine IPv6-basierte ACL erfolgreich konfiguriert haben.