Konfiguration von IPv6-basierten Zugriffskontrolllisten (ACLs) und Zugriffskontrolllisten (ACEs) auf einem Switch

Ziel

Eine Zugriffskontrollliste (Access Control List, ACL) ist eine Liste von Filtern für den Netzwerkverkehr und zugehörigen Aktionen zur Verbesserung der Sicherheit. Sie blockiert oder ermöglicht Benutzern den Zugriff auf bestimmte Ressourcen. Eine ACL enthält die Hosts, denen der Zugriff auf das Netzwerkgerät gestattet oder verweigert wird.

Die typische ACL-Funktionalität in IPv6 ähnelt der von ACLs in IPv4. ACLs bestimmen, welcher Datenverkehr blockiert und welcher Datenverkehr an den Switch-Schnittstellen weitergeleitet werden soll. ACLs ermöglichen eine Filterung nach Quell- und Zieladressen, ein- und ausgehend zu bestimmten Schnittstellen. Jede ACL verfügt am Ende über eine implizite Ablehnungsanweisung. Die Regeln für die ACLs werden in den Zugriffskontrolleinträgen (ACEs) konfiguriert.

Sie sollten Zugriffslisten verwenden, um eine grundlegende Sicherheitsstufe für den Zugriff auf Ihr Netzwerk bereitzustellen. Wenn Sie keine Zugriffslisten für Ihre Netzwerkgeräte konfigurieren, können alle Pakete, die über den Switch oder Router übertragen werden, in alle Teile Ihres Netzwerks gelangen.

Dieser Artikel enthält Anweisungen zur Konfiguration von IPv6-basierten ACLs und ACEs auf einem Switch.

Anwendbare Geräte

- Serie Sx350
- SG350X-Serie
- Serie Sx500
- Serie Sx550X

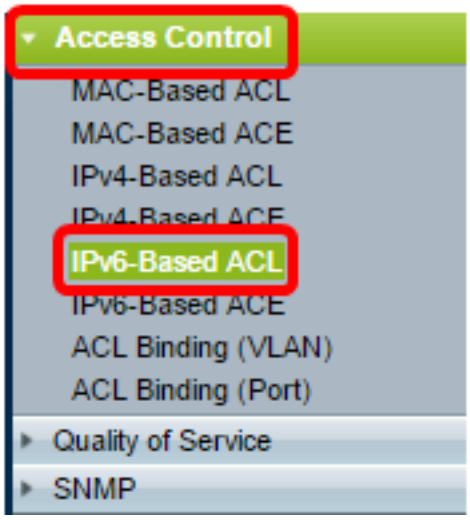
Softwareversion

- 1.4.5.02 - Serie Sx500
- 2.2.5.68 - Serie Sx350, Serie SG350X, Serie Sx550X

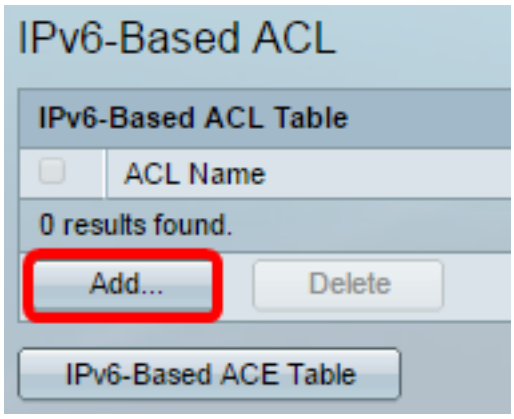
Konfiguration von IPv6-basierter ACL und ACE

Konfigurieren der IPv6-basierten ACL

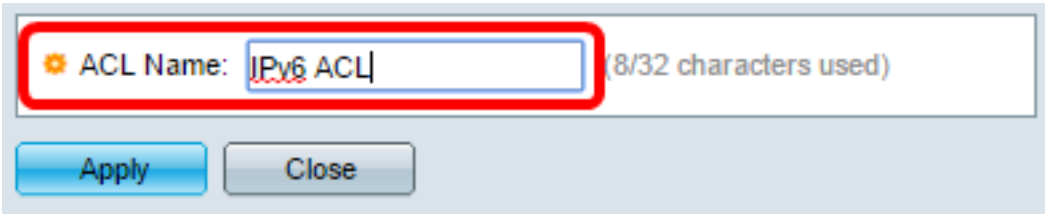
Schritt 1: Melden Sie sich beim webbasierten Dienstprogramm an, und wählen Sie **Zugriffskontrolle > IPv6-basierte Zugriffskontrollliste**.



Schritt 2: Klicken Sie auf die Schaltfläche **Hinzufügen**.

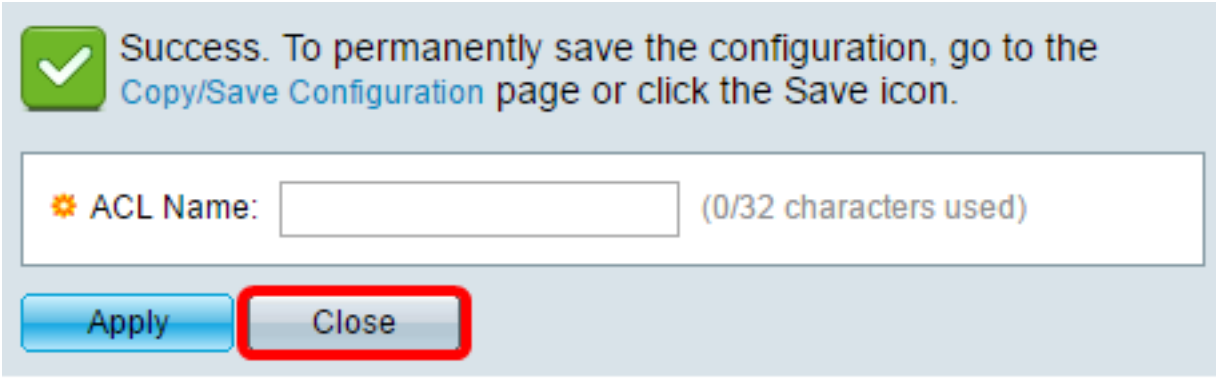


Schritt 3: Geben Sie den Namen der neuen Zugriffskontrollliste in das Feld *ACL Name ein*.



Hinweis: In diesem Beispiel wird die IPv6-ACL verwendet.

Schritt 4: Klicken Sie auf **Übernehmen** und dann auf **Schließen**.



Schritt 5: (Optional) Klicken Sie auf **Speichern**, um die Einstellungen in der Startkonfigurationsdatei zu speichern.

Sie sollten jetzt eine IPv6-basierte ACL auf Ihrem Switch konfiguriert haben.

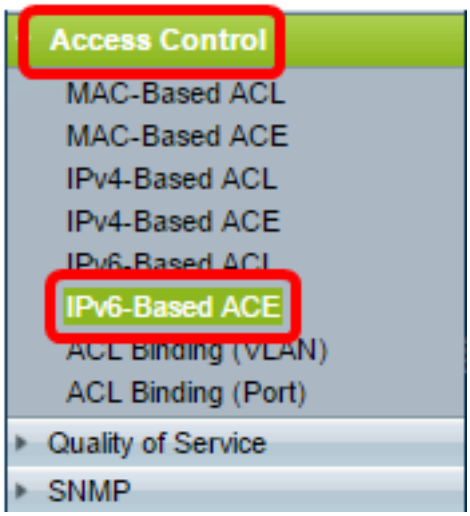
IPv6-basierter ACE konfigurieren

Wenn ein Paket auf einem Port empfangen wird, verarbeitet der Switch den Frame über die erste ACL. Wenn das Paket mit einem ACE-Filter der ersten ACL übereinstimmt, wird die ACE-Aktion ausgeführt. Wenn das Paket keinem der ACE-Filter entspricht, wird die nächste ACL verarbeitet. Wenn in allen relevanten ACLs keine Übereinstimmung mit einem ACE gefunden wird, wird das Paket standardmäßig verworfen.

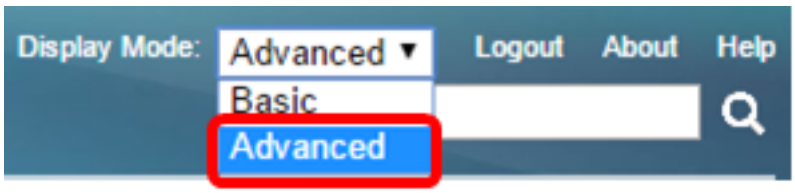
In diesem Szenario wird ein ACE erstellt, um Datenverkehr zu verweigern, der von einer bestimmten benutzerdefinierten IPv6-Quelladresse an beliebige Zieladressen gesendet wird.

Hinweis: Diese Standardaktion kann vermieden werden, indem ein ACE mit niedriger Priorität erstellt wird, der den gesamten Datenverkehr zulässt.

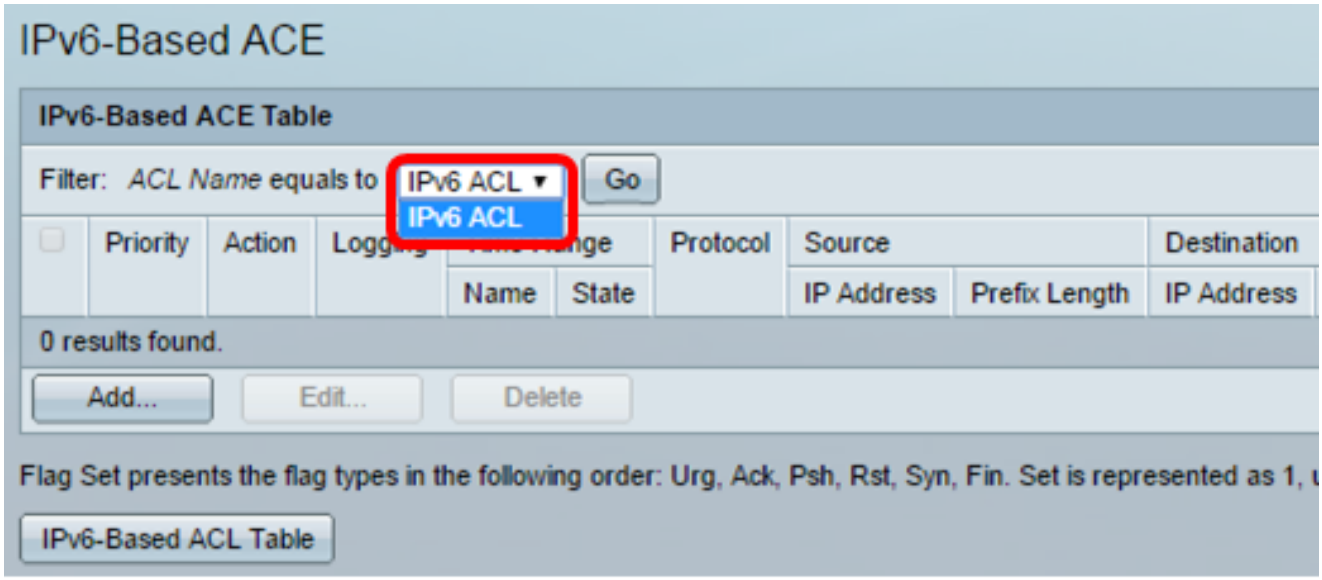
Schritt 1: Gehen Sie im webbasierten Dienstprogramm zu **Access Control > IPv6-Based ACE**.



Wichtig: Wenn Sie über einen Switch Sx350, SG350X oder Sx550X verfügen, wechseln Sie in den erweiterten Modus, indem Sie in der Dropdown-Liste "Anzeigemodus" oben rechts auf der Seite **Advanced** auswählen.

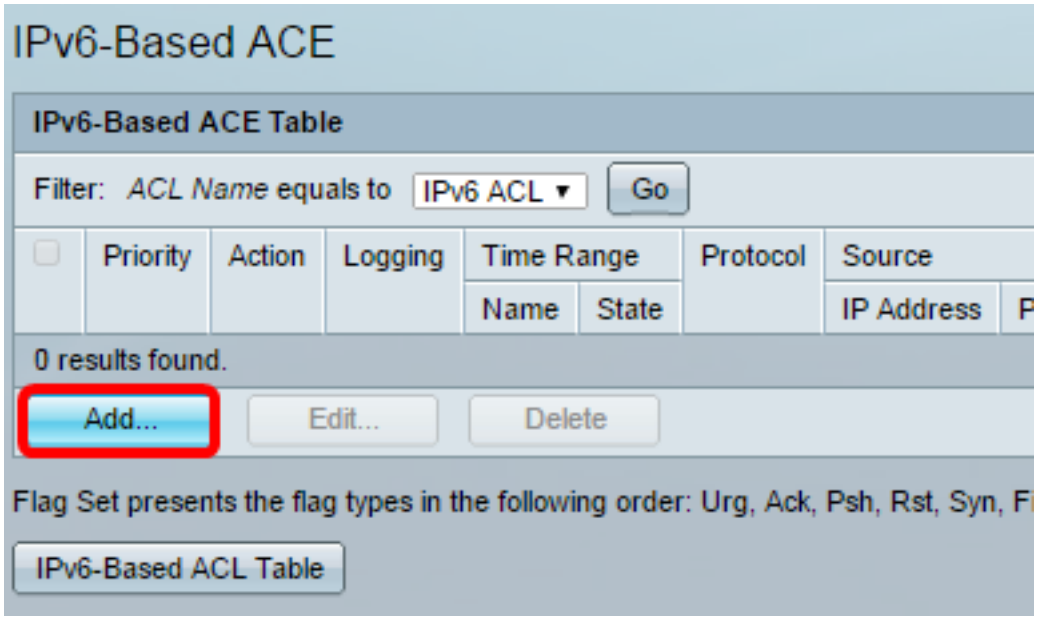


Schritt 2: Wählen Sie eine ACL aus der Dropdown-Liste ACL Name (ACL-Name) aus, und klicken Sie dann auf **Go (Los)**.



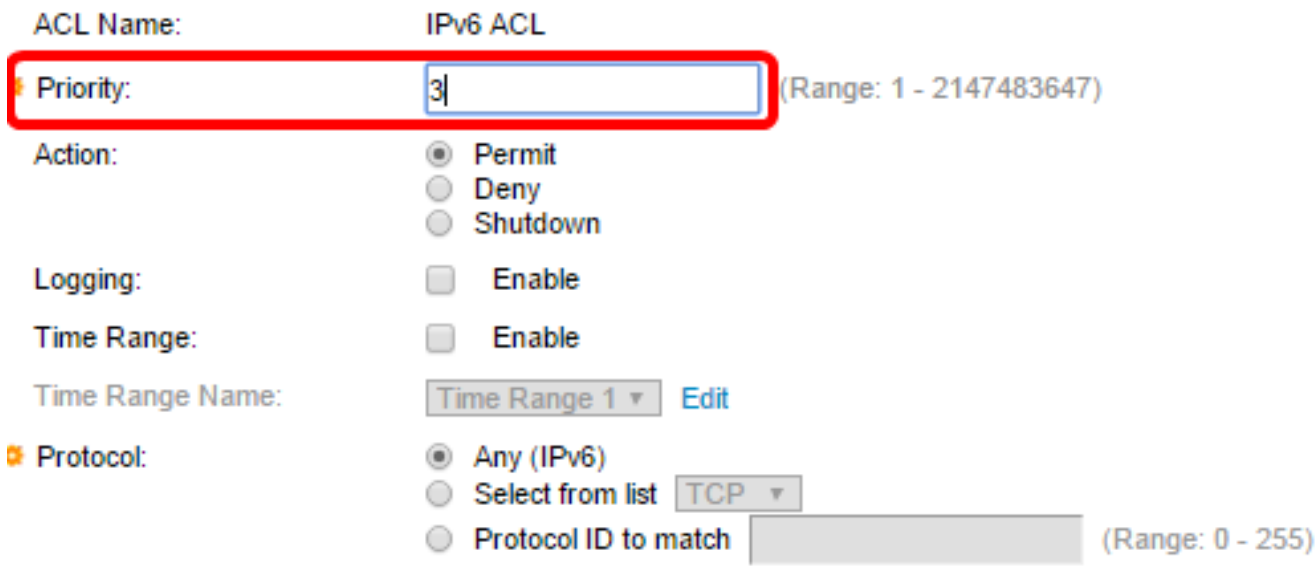
Hinweis: Die bereits für die ACL konfigurierten ACEs werden in der Tabelle angezeigt.

Schritt 3: Klicken Sie auf die Schaltfläche **Hinzufügen**, um der ACL eine neue Regel hinzuzufügen.



Hinweis: Im Feld *ACL Name* wird der Name der ACL angezeigt.

Schritt 4: Geben Sie den Prioritätswert für den ACE im Feld *Priorität ein*. ACEs mit einem höheren Prioritätswert werden zuerst verarbeitet. Der Wert 1 ist die höchste Priorität. Sie umfasst einen Bereich von 1 bis 2147483647.



Hinweis: In diesem Beispiel wird 3 verwendet.

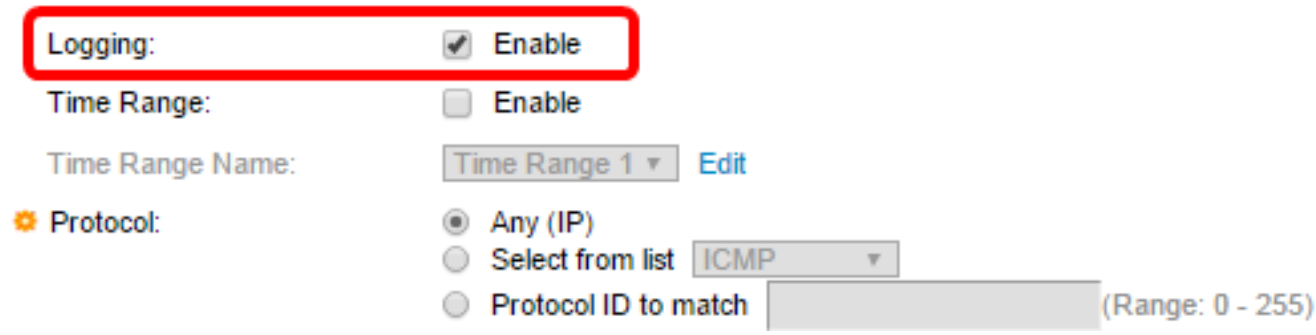
Schritt 5: Klicken Sie auf das Optionsfeld für die gewünschte Aktion, die ausgeführt wird, wenn ein Frame die erforderlichen Kriterien des ACE erfüllt.

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

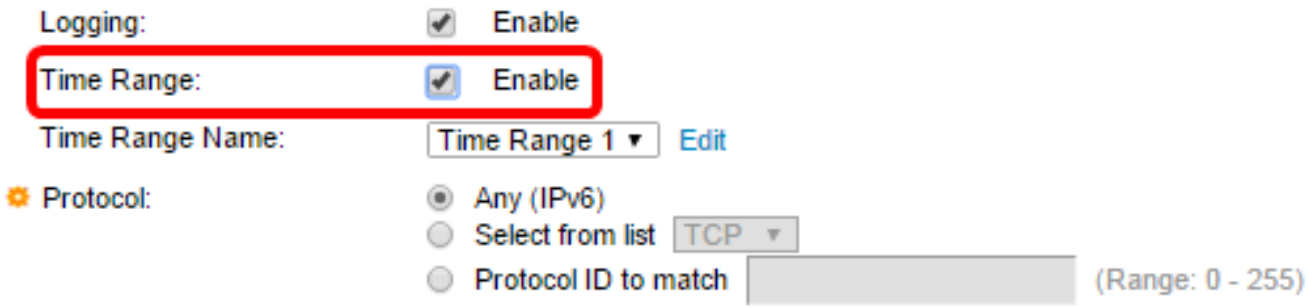
- Zulassen - Der Switch leitet Pakete weiter, die die erforderlichen Kriterien des ACE erfüllen.
- Deny (Verweigern): Der Switch verwirft Pakete, die die erforderlichen Kriterien des ACE erfüllen.

Herunterfahren - Der Switch verwirft Pakete, die nicht die erforderlichen ACE-Kriterien erfüllen, und deaktiviert den Port, an dem die Pakete empfangen wurden. Deaktivierte Ports können auf der Seite Porteinstellungen erneut aktiviert werden.

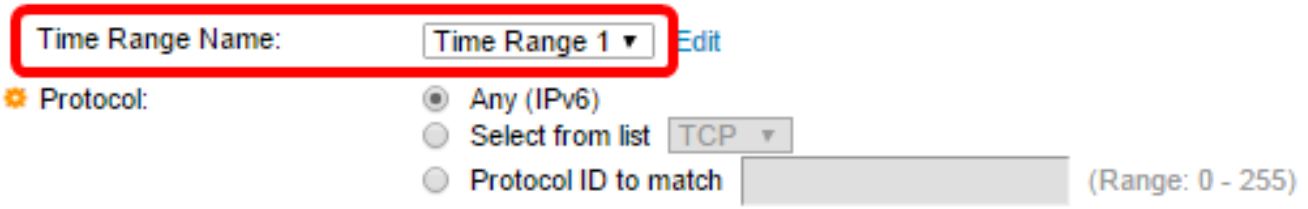
Schritt 6: (Optional) Aktivieren Sie das Kontrollkästchen **Enable** Logging (Protokollierung aktivieren), um die Protokollierung von ACL-Flüssen zu aktivieren, die der ACL-Regel entsprechen.



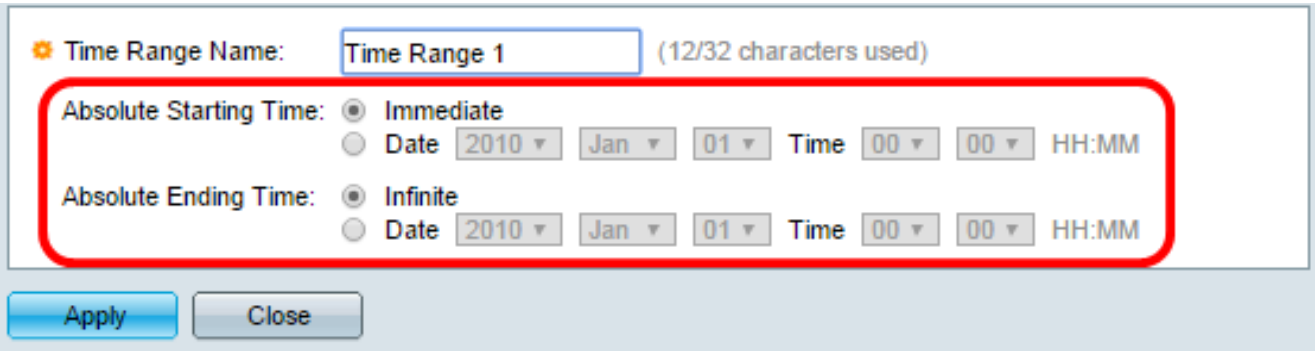
Schritt 7: (Optional) Aktivieren Sie das Kontrollkästchen **Enable** Time Range (Zeitbereich aktivieren), um eine Konfiguration eines Zeitbereichs für den ACE zu ermöglichen. Zeitbereiche werden verwendet, um die Zeitspanne zu begrenzen, in der ein ACE aktiv ist. Wenn dies deaktiviert bleibt, funktioniert der ACE jederzeit.



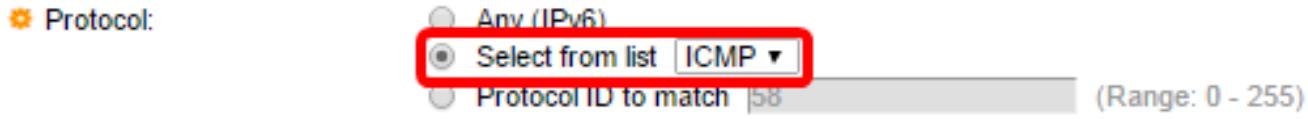
Schritt 8: (Optional) Wählen Sie aus der Dropdown-Liste "Time Range Name" (Zeitbereichsname) einen Zeitraum aus, der auf den ACE angewendet werden soll.



Hinweis: Sie können auf **Bearbeiten** klicken, um auf der Seite "Time Range" (Zeitbereich) zu navigieren und einen Zeitbereich zu erstellen.



Schritt 9: Wählen Sie im Bereich Protocol (Protokoll) einen Protokolltyp aus. Der ACE wird auf der Grundlage einer spezifischen Protokoll- oder Protokoll-ID erstellt.

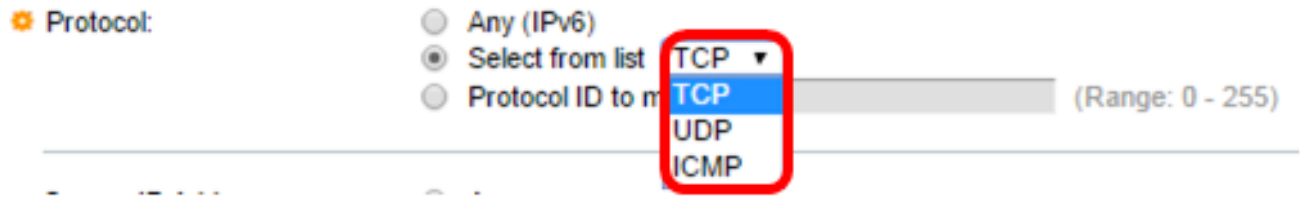


Folgende Optionen stehen zur Verfügung:

- Any (IP) (Beliebig) - Diese Option konfiguriert den ACE, um alle IP-Protokolle zu akzeptieren.
- Wählen Sie aus der Liste aus. Diese Option ermöglicht Ihnen, ein Protokoll aus einer Dropdown-Liste auszuwählen. Wenn Sie diese Option bevorzugen, fahren Sie mit Schritt 10 fort.
- Protokoll-ID zur Übereinstimmung: Mit dieser Option können Sie eine Protokoll-ID eingeben. Wenn Sie diese Option bevorzugen, fahren Sie mit Schritt 11 fort.

Hinweis: In diesem Beispiel wird Select from list (Aus Liste auswählen) ausgewählt.

Schritt 10: (Optional) Wenn Sie in Schritt 9 die Option Wählen Sie aus der Liste Wählen Sie ein Protokoll aus der Dropdown-Liste aus.

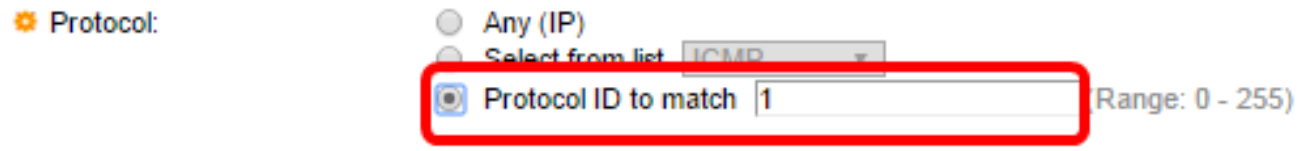


Folgende Optionen stehen zur Verfügung:

- TCP - Transmission Control Protocol (TCP) ermöglicht zwei Hosts die Kommunikation und den Austausch von Datenströmen. TCP garantiert die Paketübermittlung und garantiert, dass Pakete in der Reihenfolge übertragen und empfangen werden, in der sie gesendet wurden.
- UDP - Das User Datagram Protocol (UDP) überträgt Pakete, garantiert jedoch nicht deren Übermittlung.
- ICMP - Gleicht Pakete an das Internet Control Message Protocol (ICMP) an.

Hinweis: In diesem Beispiel wird TCP verwendet.

Schritt 11: (Optional) Wenn Sie in Schritt 9 Protokoll-ID für Übereinstimmung ausgewählt haben, geben Sie die Protokoll-ID in das Feld *Protokoll-ID für Übereinstimmung ein*.



Hinweis: In diesem Beispiel wird 1 verwendet.

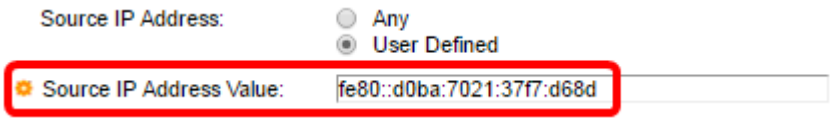
Schritt 12: Klicken Sie auf das Optionsfeld, das den gewünschten Kriterien des ACE im Bereich Quell-IP-Adresse entspricht.

Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Alle IPv6-Quelladressen gelten für den ACE.
- User Defined (Benutzerdefiniert) - Geben Sie eine IP-Adresse und eine IP-Platzhaltermaske ein, die auf den ACE in den Feldern *Source IP Address Value* und *Source IP Prefix Length* angewendet werden sollen.

Hinweis: In diesem Beispiel wird User Defined (Benutzerdefiniert) ausgewählt. Wenn Sie Any (Beliebig) auswählen, fahren Sie mit Schritt 15 fort.

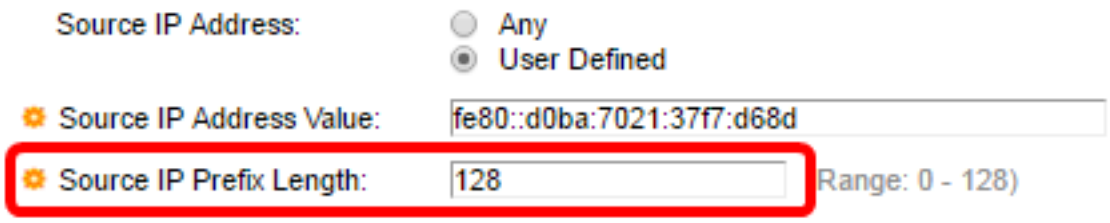
Schritt 13: Geben Sie die Quell-IP-Adresse im Feld *Quell-IP-Adressenwert ein*.



Hinweis: In diesem Beispiel wird fe80::d0ba:7021:37f7:d68d verwendet.

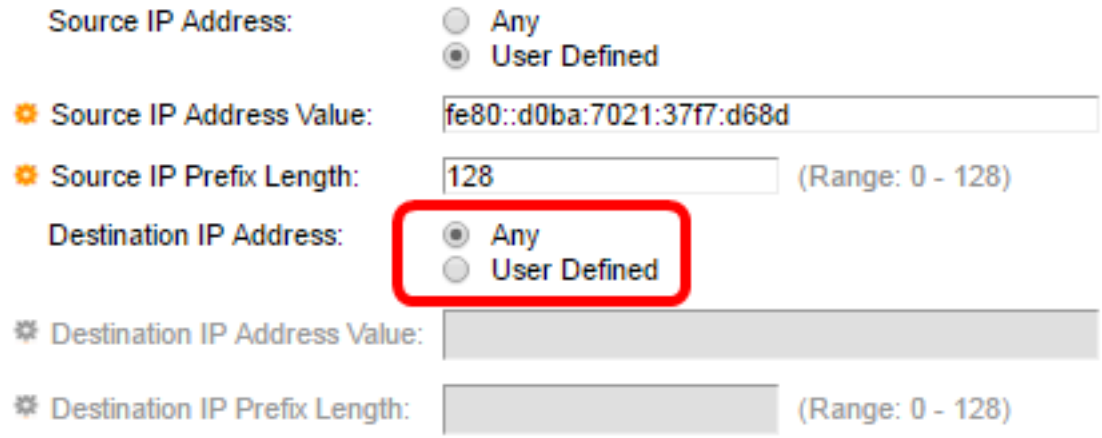
Schritt 14: Geben Sie die Länge des Quell-IP-Präfixes in das Feld *Länge des Quell-IP-*

Präfixes ein.



Hinweis: In diesem Beispiel wird 128 verwendet.

Schritt 15: Klicken Sie auf das Optionsfeld, das den gewünschten Kriterien des ACE im Bereich ZielIP-Adresse entspricht.



Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Alle Ziel-IPv6-Adressen gelten für den ACE.
- User Defined (Benutzerdefiniert) - Geben Sie eine IP-Adresse und eine IP-Platzhaltermaske ein, die auf den ACE in den Feldern *Ziel-IP-Adresswert* und *Ziel-IPrefix-Länge* angewendet werden sollen.

Hinweis: In diesem Beispiel wird Any (Beliebig) ausgewählt. Bei Auswahl dieser Option wird der zu erstellende ACE den ACE-Datenverkehr von der angegebenen IPv6-Adresse zu einem beliebigen Ziel zulassen.

Schritt 16: (Optional) Klicken Sie im Bereich Quellport auf ein Optionsfeld. Der Standardwert ist Any (Beliebig).

- Any (Beliebig): Übereinstimmung mit allen Quellports
- Single from list (Nur aus): Sie können einen einzelnen TCP/UDP-Quellport auswählen, dem

Pakete zugeordnet werden. Dieses Feld ist nur dann aktiv, wenn im Dropdown-Menü "Wählen aus Liste" 800/6-TCP oder 800/17-UDP ausgewählt ist.

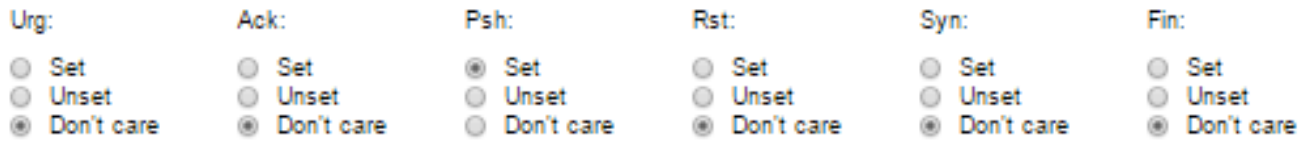
- Single by Number (Einfach nach Nummer): Sie können einen einzelnen TCP/UDP-Quellport auswählen, dem Pakete zugeordnet werden. Dieses Feld ist nur dann aktiv, wenn im Dropdown-Menü "Wählen aus Liste" 800/6-TCP oder 800/17-UDP ausgewählt ist.
- Bereich - Sie können einen Bereich von TCP/UDP-Quellports auswählen, denen das Paket zugeordnet ist. Es gibt acht verschiedene Port-Bereiche, die konfiguriert werden können (für Quell- und Zielports gemeinsam genutzt). TCP- und UDP-Protokolle verfügen jeweils über acht Port-Bereiche.

Schritt 17: (Optional) Klicken Sie im Bereich Zielport auf ein Optionsfeld. Der Standardwert ist Any (Beliebig).

- Any (Beliebig) - Übereinstimmung mit allen Quellports
- Single from list (Nur aus): Sie können einen einzelnen TCP/UDP-Quellport auswählen, dem Pakete zugeordnet werden. Dieses Feld ist nur dann aktiv, wenn im Dropdown-Menü "Wählen aus Liste" 800/6-TCP oder 800/17-UDP ausgewählt ist.
- Single by Number (Einfach nach Nummer): Sie können einen einzelnen TCP/UDP-Quellport auswählen, dem Pakete zugeordnet werden. Dieses Feld ist nur dann aktiv, wenn im Dropdown-Menü "Wählen aus Liste" 800/6-TCP oder 800/17-UDP ausgewählt ist.
- Bereich - Sie können einen Bereich von TCP/UDP-Quellports auswählen, denen das Paket zugeordnet ist. Es gibt acht verschiedene Port-Bereiche, die konfiguriert werden können (für Quell- und Zielports gemeinsam genutzt). TCP- und UDP-Protokolle verfügen jeweils über acht Port-Bereiche.

Schritt 18: (Optional) Wählen Sie im Bereich TCP Flags (TCP-Flags) eine oder mehrere TCP-Flags aus, mit denen Pakete gefiltert werden sollen. Gefilterte Pakete werden entweder weitergeleitet oder verworfen. Das Filtern von Paketen durch TCP-Flags erhöht die Paketkontrolle, was die Netzwerksicherheit erhöht.

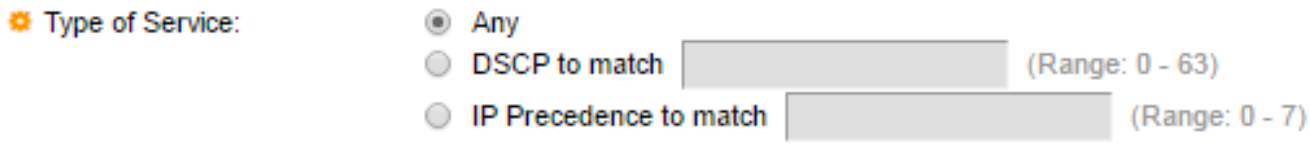
- Set (Festlegen): Match (Übereinstimmung), wenn das Flag festgelegt ist.
- Unset (Nicht festgelegt): Übereinstimmung, wenn das Flag nicht gesetzt ist.
- Keine Sorge - die TCP-Flag ignorieren.



Die TCP-Flags sind:

- Urg - Dieses Flag wird verwendet, um eingehende Daten als Dringend zu identifizieren.
- Ack - Dieses Flag wird verwendet, um den erfolgreichen Empfang von Paketen zu bestätigen.
- Psh - Dieses Flag wird verwendet, um sicherzustellen, dass die Daten die Priorität erhalten (die sie verdienen) und am sendenden oder empfangenden Ende verarbeitet werden.
- Rst - Dieses Flag wird verwendet, wenn ein Segment ankommt, das nicht für die aktuelle Verbindung vorgesehen ist.
- Syn - Dieses Flag wird für TCP-Kommunikation verwendet.
- Fin (Fin): Dieses Flag wird verwendet, wenn die Kommunikation oder Datenübertragung beendet ist.

Schritt 19: (Optional) Klicken Sie im Bereich Type of Service (Servicetyp) auf den Servicetyp des IP-Pakets.



Folgende Optionen stehen zur Verfügung:

- Any (Beliebig): Bei Verkehrsstaus kann es sich um einen beliebigen Service handeln.
- DSCP to Match (Übereinstimmung mit DSCP) - Differentiated Services Code Point ist ein Mechanismus zur Klassifizierung und Verwaltung des Netzwerkverkehrs. Zur Auswahl des Per-Hop-Verhaltens werden sechs Bit (0-63) verwendet, um die Paketerfahrung an jedem Knoten festzulegen.
- Abgleich der IP-Rangfolge - Die IP-Rangfolge ist ein Modell des Type of Service (TOS), das das Netzwerk verwendet, um die entsprechenden Quality of Service (QoS)-Verpflichtungen bereitzustellen. Dieses Modell verwendet die drei wichtigsten Bits des Diensttypbytes im IP-Header, wie in RFC 791 und RFC 1349 beschrieben. Das Schlüsselwort mit IP-Voreinstellungswerten ist wie folgt:

    - 0 - Routine

    - 1 - Priorität

    - 2 - für sofortige Zwecke

    - 3 — Flash

    - 4 — für Flash-Override

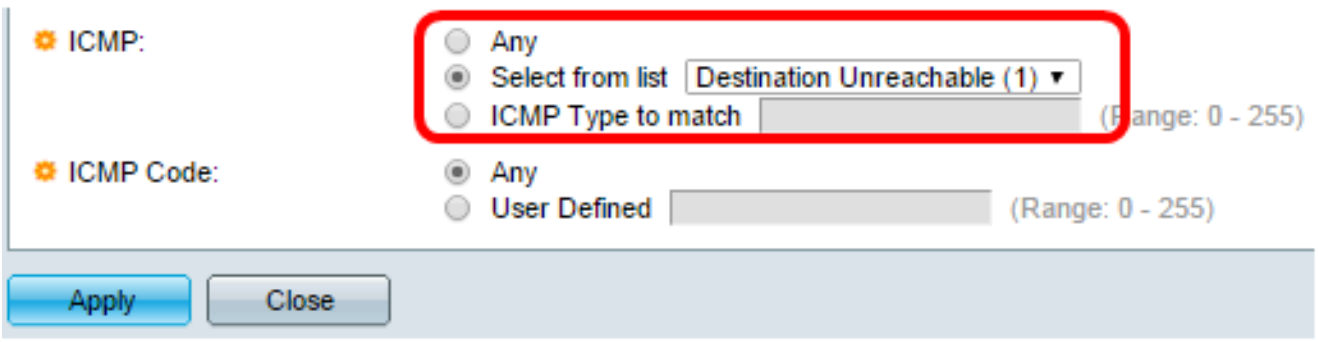
    - 5 - Kritisch

    - 6 - für das Internet

    - 7 - für das Netzwerk

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

Schritt 20: (Optional) Wenn das IP-Protokoll der ACL ICMP ist, klicken Sie auf den für Filterzwecke verwendeten ICMP-Meldungstyp. Wählen Sie entweder den Nachrichtentyp nach Namen aus, oder geben Sie die Nummer des Nachrichtentyps ein:

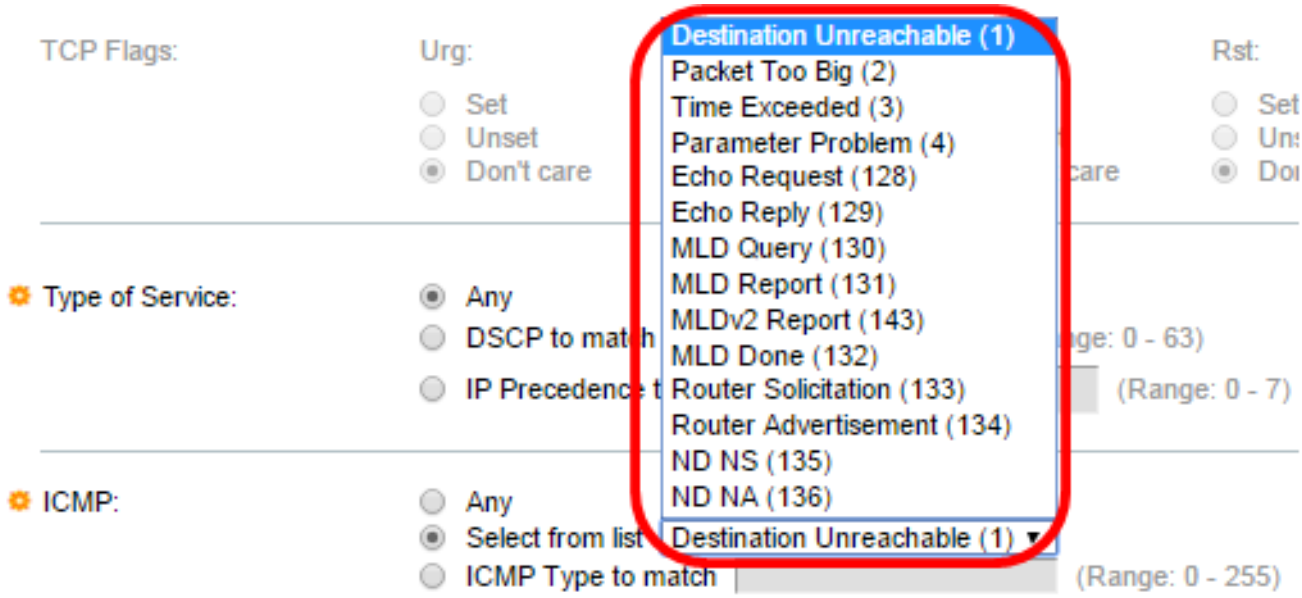


- Any (Beliebig): Alle Meldungstypen werden akzeptiert.

- Aus Liste auswählen: Sie können Nachrichtentyp nach Name auswählen.
- ICMP Type to match (Zu übereinstimmender ICMP-Typ): Die Anzahl der Meldungstypen, die zu Filterzwecken verwendet werden.

Hinweis: In diesem Beispiel wird Select from list (Aus Liste auswählen) ausgewählt.

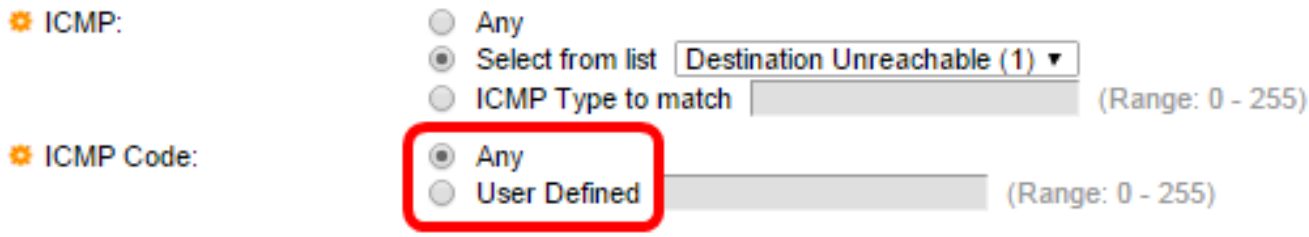
Schritt 21: (Optional) Wenn unter Schritt 20 die Option Wählen Sie Aus Liste auswählen ausgewählt ist, wählen Sie die Steuerelementmeldungen aus, die aus den möglichen Optionen in der Dropdown-Liste gefiltert werden sollen:



- Destination Unreachable (1) (Ziel nicht erreichbar) (1) - Dieser wird vom Host oder seinem Gateway generiert, um dem Client mitzuteilen, dass das Ziel aus irgendeinem Grund nicht erreichbar ist (Beispiel: Fehler: Netzwerk oder Host nicht erreichbar).
- Packet Too Big (2) - Die Größe des Datagrams überschreitet die angegebene MTU.
- Time Overceeded (3) (Zeitüberschreitung) (3)) - Diese wird von einem Gateway generiert, um die Quelle eines verworfenen Datagramms zu informieren, da die Zeit bis zum Live-Feld 0 erreicht.
- Parameterproblem (4) - Es wird als Antwort auf Fehler generiert, die nicht speziell durch eine andere ICMP-Meldung abgedeckt werden.
- Echo Request (128) - Ein Ping, dessen Daten voraussichtlich in einer Echo-Antwort empfangen werden.
- Echo Reply (129) (Echoantwort) (Echoantwort) (129)): Diese Antwort wird als Antwort auf eine Echoanfrage generiert.
- MLD Query (130) (MLD-Abfrage) (MLD-Abfrage) (130)): Mit dieser Abfrage wird ermittelt, welche Multicast-Adressen Listener auf einer angeschlossenen Verbindung haben. Geben Sie 130 als Dezimalzahl ein.
- MLD Report (131) (MLD-Bericht): Dieser Bericht wird generiert, wenn IPv6-Multicast-Adressen, an die der Absender der Nachricht lauscht, empfangen.
- MLD v2 Report (143): Dieser Bericht ist mit MLD Report (Version 2) identisch.
- MLD Done (132) - Wenn der Host eine Gruppe verlässt, sendet er eine fertig gestellte Nachricht für einen Multicast-Listener an Multicast-Router im Netzwerk.
- Router Solicitation (133) - Dies ist eine Router Discovery-Nachricht. Hosts können die Adressen der benachbarten Router einfach erkennen, wenn sie auf Werbung hören. Der Standardwert ist 224.0.0.2 für Multicast, ansonsten 255.255.255.

- Router Advertisement (134) (Routerwerbung) - Der Router sendet regelmäßig Multicast-Signale von jeder seiner Multicast-Schnittstellen aus und kündigt die IP-Adressen dieser Schnittstelle an.
- ND NS (135) - Meldungen werden von Knoten generiert, um die Link Layer-Adresse eines anderen Knotens anzufordern. Sie dienen auch für Funktionen wie doppelte Adresserkennung und Erkennung von Nachbar-Unerreichbarkeit.
- ND NA (136) — Nachrichten werden als Antwort auf NS-Nachrichten gesendet. Wenn ein Knoten seine Link-Layer-Adresse ändert, kann er eine unaufgefordert erstellte NA senden, um die neue Adresse anzukündigen.

Schritt 22: (Optional) Die ICMP-Meldungen können ein Codefeld enthalten, das angibt, wie die Nachricht verarbeitet wird. Dies ist aktiviert, wenn Sie in Schritt 10 das ICMP-Protokoll auswählen. Klicken Sie auf eine der folgenden Optionen, um zu konfigurieren, ob für diesen Code gefiltert werden soll:

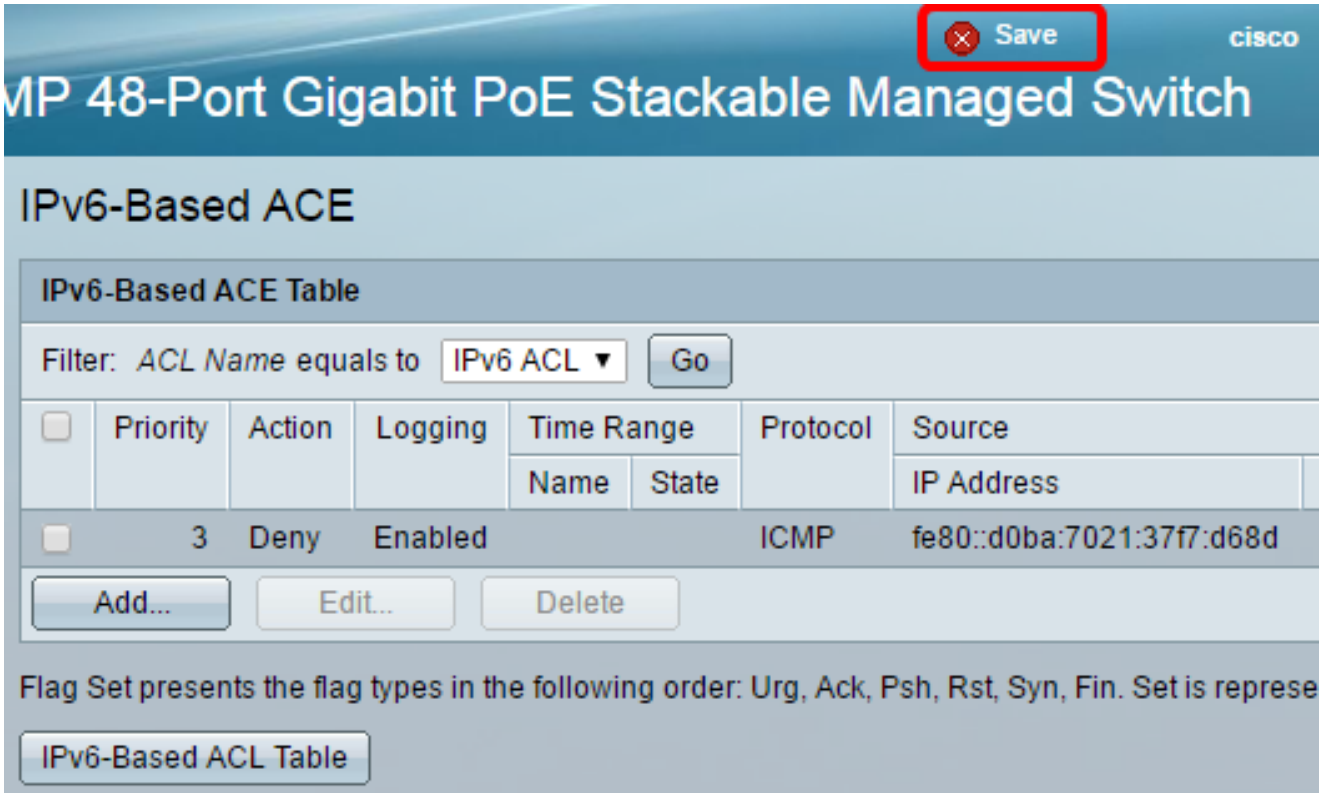


- Any (Beliebig): Akzeptieren Sie alle Codes.
- User Defined (Benutzerdefiniert): Sie können einen ICMP-Code für Filterzwecke eingeben.

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

Schritt 23: Klicken Sie auf **Übernehmen** und anschließend auf **Schließen**. Der ACE wird erstellt und dem Namen der ACL zugeordnet.

Schritt 24: Klicken Sie auf **Speichern**, um die Einstellungen in der Startkonfigurationsdatei zu speichern.



Sie sollten jetzt einen IPv6-basierten ACE auf Ihrem Switch konfiguriert haben.